

# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



**Facultad de Ingeniería en Electricidad y Computación**

**Maestría En Seguridad Informática Aplicada**

“CONFIGURACIÓN DE UN SISTEMA DE PREVENCIÓN DE  
PÉRDIDA DE INFORMACIÓN (DLP), PARA PREVENIR LA DIVULGACIÓN  
INTENCIONADA O NO INTENCIONADA DE INFORMACIÓN  
CONSIDERADA SENSIBLE DEL ÁREA DE MERCADO DE UNA EMPRESA  
COMERCIAL”

**EXAMEN DE GRADO (COMPLEXIVO)**

Previa a la obtención del grado de:

**MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA**

MARGARITA LUISA CASTILLO LOJA  
GUAYAQUIL-ECUADOR  
AÑO: 2016

## **AGRADECIMIENTO**

A Dios, en todo momento mi Padre Amado que todo lo que conviene me lo ha dado.

A mi madre por darme ejemplo de trabajo y sacrificio y haberme entregado lo más valioso que se entrega a los hijos; la educación.

A mi padre por su tierno amor, guía y apoyo.

A ambos, mi amor y corazón porque me debo a ellos.

## DEDICATORIA

Dedico este proyecto a mi bendecida familia, mi amado esposo Alan, mi preciosa hija Ana Victoria y al lindo niño que está por venir.

Para ustedes que son la alegría de mi vida.

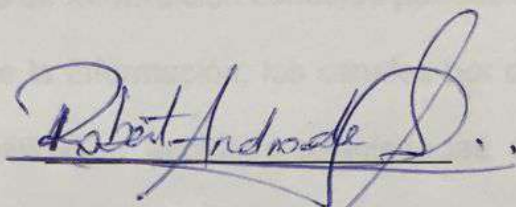
A handwritten signature in blue ink, written in a cursive style. The signature appears to be 'Luz Cortés'.

## TRIBUNAL DE SUSTENTACIÓN



ING. LENIN FREIRE COBO

DIRECTOR MSIA



MGS. ROBERT ANDRADE

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

POR LA UNIDAD ACADÉMICA



MGS. NESTOR ARREAGA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

## RESUMEN

Si revisamos el número de incidentes de fuga de información confidencial y las pérdidas económicas que estas han causado a la compañía, fácilmente determinamos la importancia de esta herramienta dentro de un marco de seguridad informática total.

Esta propuesta pretende definir dentro de una herramienta tecnológica de Prevención de Pérdida de Información conocido por sus siglas en inglés como DLP la clasificación de la información, los canales por donde se mueve esta información y las políticas o acciones relacionadas con cada rol que el empleado desempeñe dentro del departamento de mercado, todo esto permitirá minimizar la fuga de información sensible de forma intencional o no intencional. [1]

La empresa ya tiene su información clasificada en confidencial, pública y privada, con este punto de partida revisaremos el proceso del área de mercado y crearemos la matriz base especificando quien puede tener acceso a qué información y de qué modo puede tratarla.

## ÍNDICE GENERAL

AGRADECIMIENTO .....	ii
DEDICATORIA .....	iii
TRIBUNAL DE SUSTENTACIÓN .....	iv
RESUMEN.....	v
ÍNDICE GENERAL.....	vi
INDICE DE FIGURAS.....	viii
INDICE DE TABLAS .....	x
INTRODUCCIÓN .....	xi
CAPITULO 1.....	1
GENERALIDADES.....	1
1.1. DESCRIPCIÓN DEL PROBLEMA.....	1
1.2. SOLUCIÓN PROPUESTA.....	3
CAPITULO 2.....	4
METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN.....	4
2.1. LEVANTAMIENTO DE INFORMACIÓN .....	4
2.2. Elaboración de la Matriz de Patrones .....	6
2.3. Elaboración de Matriz de Canales y Acciones.....	8
2.3.2. Canales.....	9

2.3.3. Acciones de Monitoreo.....	10
2.3.4 Nivel de Monitoreo. ....	10
2.4. Creación de la política de Mercado.....	11
2.5. Clasificación de la Información. ....	17
2.5.1. Tipos de Clasificación .....	17
CAPITULO 3.....	22
ANÁLISIS DE RESULTADOS .....	22
3.1 Pruebas en escenarios programados. ....	22
CONCLUSIONES Y RECOMENDACIONES .....	31
BIBLIOGRAFÍA.....	32

## INDICE DE FIGURAS

Figura 2. 1: Dashboard general de Wave Data Protection.....	12
Figura 2. 2: Nombrando la política mercado_001 .....	12
Figura 2. 3: Elección de la OU de Mercado .....	13
Figura 2. 4: Política con integrantes de la OU .....	14
Figura 2. 5: Detalle de Canales y Acciones de Seguridad.....	15
Figura 2. 6: Pantalla para ingresar lista blanca de correo.....	16
Figura 2. 7: Creación de lista blanca Jefes Inmediatos de Mercado.....	16
Figura 2. 8: Crear nueva Clasificación de la información.....	18
Figura 2. 9: Creación de Clasificación de Pronósticos.....	19
Figura 2. 10: Elección de tipo de clasificación. ....	20
Figura 2. 11: Añadir keywords. ....	21
Figura 2. 12: Clasificaciones del área de Mercado. ....	21
Figura 3. 1: Envío de correo en escenario 1 .....	24
Figura 3. 2: Pregunta en escenario 1 .....	24
Figura 3. 3: Revisión de log en escenario 1 .....	25
Figura 3. 4: Vista del detalle del contenido del correo. ....	26
Figura 3. 5: Sitio wetransfer en escenario 2.....	27
Figura 3. 6: Mensaje de bloqueo web en escenario 2.....	27
Figura 3. 7: Muestra de log en escenario 2.....	27
Figura 3. 8: Mensaje de bloqueo en escenario 3 .....	28
Figura 3. 9: Log en escenario 3 .....	29



Figura 3. 10: Mensaje de pregunta en escenario 4.....	29
Figura 3. 11: Log en escenario 4.	30

## INDICE DE TABLAS

Tabla 1.- Organigrama de la compañía. ....	4
Tabla 2.- Información del área de mercado .....	5
Tabla 3.- Matriz de Patrones.....	7
Tabla 4.- Matriz de canales y acciones.....	11
Tabla 5.- Pruebas en escenarios programados. ....	23

## INTRODUCCIÓN

La propiedad intelectual y los secretos comerciales e industriales representan el esfuerzo, tiempo, dinero y experiencia de una compañía, si estos datos son filtrados hacia las empresas competidoras estas los podrían usar para obtener su beneficio y lucro, echándose a perder negocios y afectando la marca de la compañía.

La fuga de información puede darse de manera intencional o no intencional, por esto se debe considerar la implementación de un sistema de Prevención de Pérdida de la Información (DLP) para minimizar estos incidentes de seguridad, aunque no quiero decir que esta signifique la panacea, ya que un DLP debe ser parte de una solución de seguridad informática más amplia. Pero sin lugar a dudas esta aplicación es un punto que no debería faltar. [2]

Se protegerá la información durante su estado en movimiento usando agentes en cada una de las computadoras del área de mercado que son capaces de recolectar información a pesar de estar fuera de línea y se contará con una consola central que será usada por el personal de informática y el oficial de seguridad.

## **CAPITULO 1**

### **GENERALIDADES**

#### **1.1. DESCRIPCIÓN DEL PROBLEMA.**

Esta empresa comercial se dedica a la fabricación, importación y comercialización de electrodomésticos en el país, se esfuerza por mantener planes estratégicos como la clasificación de cartera, estrategias de mercado, desarrollo de productos, gestión de cobranzas, en fin, toda esta información es parte substancial para su negocio.

Lamentablemente se ha encontrado un historial de numerosos incidentes de fuga de información de estrategias de mercado, listados de artículos y costos que han aumentado durante los últimos años y ha provocado pérdidas económicas, porque esta información ha sido

usada por terceros para lucrarse.

Esto solo confirma las estadísticas que ya existen a nivel mundial indicando que un gran número de incidentes de seguridad son generados por empleados de las compañías [3]

En el levantamiento efectuado, se determinó que existe una solución de seguridad informática ya implementada que hace especial énfasis en proteger la salida de la información entre los que podemos mencionar: Cortafuegos, Sistema de Prevención de Intrusos, políticas y procedimientos, proxy con control web, antivirus, control de dispositivos, etc. Además, se encuentra instalado un producto DLP marca WAVE, con una suscripción de 15 licencias, pero no ha sido configurado porque el encargado de informática responsable de esta herramienta renunció hace seis meses y actualmente ninguna persona de la compañía tiene el conocimiento para implementarlo.

El oficial de seguridad tiene una bitácora con los registros de incidentes de fuga de información desde hace 18 meses donde se pueden identificar que alrededor del 70% de ellas pudieron ser mitigadas con la implementación del DLP.

## **1.2. SOLUCIÓN PROPUESTA.**

Usar el producto DLP WAVE para definir la matriz de clasificación de la información en base a la información que usa el departamento de mercado.

Usar la misma herramienta para definir controles en los diferentes canales de transmisión de la información como correo electrónico, carpetas compartidas, impresoras, entre otros, para minimizar los incidentes de fuga de información e instalar el agente WAVE en los equipos del personal del área de mercado.

Poder revisar los logs que se generan luego de cada acción que el usuario realice y analizar el detalle de los datos tratados.

## CAPITULO 2

### METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

#### 2.1. LEVANTAMIENTO DE INFORMACIÓN

En el área de mercado trabajan 13 personas, todas enroladas en la compañía, 5 de ellas tienen más de 10 años en la compañía y el resto tiene entre dos y cinco años.

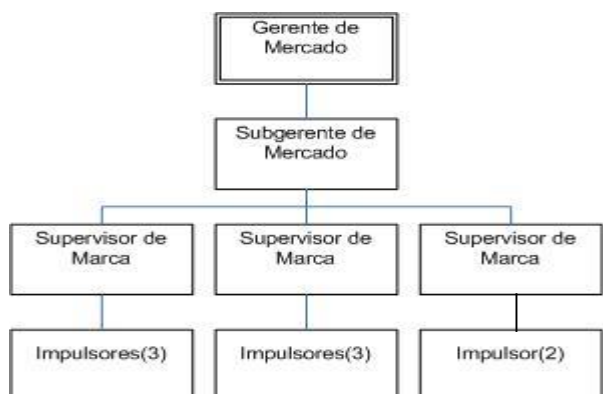


Tabla 1.- Organigrama de la compañía.

En la tabla 2 se detalla la información de tipo confidencial que se maneja en el área de mercado, a pesar de que tiene un sistema informático ERP como sistema principal, desde este sistema se descargan información para trabajarla localmente y se transforma por ese lapso de tiempo en información no estructurada y podemos encontrarlas en documentos de ofimática localizados en carpetas compartidas, discos duros, etc.

AREA: MERCADO				
INFORMACIÓN	DESCRIPCIÓN	INVOLUCRADOS	TIPO DE ARCHIVO	
Pronosticos	Cifras a vender	GERENTE DE MERCADO	XLS-DOC-TXT-PDF	
Presupuestos	Presupuesto de Venta		XLS-DOC-TXT-PDF	
Estudio de Mercado	Se revisa nicho de mercado, oportunidad, competidores y se eligen estrategias		SUGGERENTE Y JEFE DE MARCAS	XLS-DOC-TXT-PDF
	Negociaciones de costos, precios preferenciales, descuentos, etc.			XLS-DOC-TXT-PDF
Acuerdos con Proveedores				XLS-DOC-TXT-PDF
Análisis de Oportunidad	Análisis del mercado y los parametros que esta le afectan			XLS-DOC-TXT-PDF
	Características de los productos			XLS-DOC-TXT-PDF
Data maestra de artículos	Las ofertas y descuentos			XLS-DOC-TXT-PDF
Ofertas, promociones, descuentos	actuales y pasados			XLS-DOC-TXT-PDF
Precios y márgenes de ganancia	Listado de precios y/o márgenes			XLS-DOC-TXT-PDF
		XLS-DOC-TXT-PDF		

Tabla 2.- Información del área de mercado



## 2.2. Elaboración de la Matriz de Patrones

Usando el método de entrevista y observación se conversó con el personal del área de mercado exceptuando los impulsores y se recabó datos sobre cada clase de información con la que ellos trabajan, definiendo para cada documento o documentos un esquema de su contenido.

Teniendo por ejemplo que en los documentos involucrados con Precios y márgenes de ganancias (ver Tabla 1) que sabemos pueden ser de tipo XLS, DOC, TXT y PDF, existen palabras y términos que sirven para identificar el documento tales como: código, descripción de lista de precios, descripción, código, marca, margen objetivo, margen, contribución. Entonces si encontramos todo este grupo de palabras en un documento podríamos indicar que se trata de un listado de precios y márgenes.

Lo que estamos definiendo aquí es un patrón que nos permita identificar el documento Precios y Márgenes, la herramienta DLP fabricará su regla en base a este patrón, así que cuando encuentre similitud lo clasificará como confidencial y actuará según lo definido.

Existen en el mercado ya huellas digitales predefinidas, como las que usa Microsoft en su módulo DLP de Microsoft OFFICE 365 [4], o las que ya vienen incluida en WAVE acerca de tarjetas de crédito, información médica o información bancaria de diferentes países.

AREA: MERCADO	
INFORMACIÓN	PATRONES
Pronosticos	pronostico, inventario, material, descripción de división, descripción familia, peso, meses, grupo de compras, venta
Presupuestos	material, descripción lista precios, margen objetivo, precio venta, presupuesto de ventas, pronostico en unidades, cumplimiento esperado, pronostico unidades, pronostico und, costo, landed
Estudio de Mercado	plan de mercado, compras, compras y rebate de proveedores, rebate, proveedor, ventas, márgenes, margen, inventarios, precios, precio, cobertura, tipo clientes, pesos por región, tipo cliente. análisis del mercado, entorno competitivo, competencia, principales actividades, portafolio, lanzamientos, estrategias, participaciones de mercado, posicionamiento de las marcas, matriz desempeño. mercado, estrategias de mercado, marcas. objetivos y metas, objetivos generales de la marca, objetivos específicos numéricos, objetivos marcas, objetivos, metas. estrategias de mercado, estrategias de producto, estrategias de precio, estrategias de promoción, estrategias de distribución, estrategias de comunicación, marcas privadas, marcas exclusivas, marcas codistribuidas
Acuerdos con Proveedores	fob, land, description, total cost, landed, costo, descripción, marca, descuento, InStove Rocket Stoves, EverHot, CanCooker, Siemens, Oster, General Electric, Moulinex Vitae, Ufesa, Clatronic, Philips, Braun, Kenwood, York, Toshiba, Hitachi, Westinghouse, Candy, Ariston, Kenia, Daikin, BGH, PHILCO, LG, PANASONIC
Analisis de Oportunidad	Codigo, marc, marcador, descripción de material, descripción lista de precios, precio, descuento, margen
Data maestra de articulos	codigo, descripción para lista de precios, costo, margen actual, precio 60 dias, margen propuesto, precio 60 dias propuesto, precio lista anterior, precio lista nuevo, margen objetivo, producto, descripción para la lista de precios, precio, grupo compras, pronostico, venta.
Ofertas, promociones, descuentos	linea, líneas, grupo, descuento, marca, codigo de articulo, descripción material, material.
Precios y margenes de ganancia	codigo, descripción de lista de precios, descripción, codigo, marca, margen objetivo, margen, descripción, contribucion

Tabla 3.- Matriz de Patrones

## **2.3 Elaboración de Matriz de Canales y Acciones.**

En el punto anterior, se definió la matriz para determinar si la información es confidencial o no, ahora revisaremos las acciones a tomar en caso de que la comparación arroje resultado positivo.

### **2.3.1. Acciones de Seguridad**

Existen cuatro diferentes opciones en la herramienta:

- Permitir.- Permite que la información sea tratada
- Denegar.- No permite que la información sea tratada
- Preguntar.-Presenta una caja de texto donde el empleado deberá escribir una explicación del porqué de su acción y luego de Aceptar la información será enviada.
- Encriptar\*.- La información será encriptada y luego enviada.

\*No usaremos esta opción por pedido expreso de la Gerencia de Informática ya que el cifrado será cubierta por otra estrategia.

### 2.3.2. Canales

Tenemos 8 diferentes canales donde los datos pueden ser controlados o restringidos.

- Email.- Correos electrónicos, se puede definir que no acepte adjuntos y crear listas blancas de destinatarios permitidos.
- Web.- Páginas web, se puede crear listas blancas de sitios permitidos.
- External Storage.- Dispositivos externos, se puede definir una lista blanca de dispositivos permitidos.
- Cloud Storage.- Controla la subida de documentos a los siguientes aplicaciones: Dropbox, Box.net, Google Drive, and Microsoft SkyDrive
- Local Printers.- Controla la impresión en impresoras locales.
- Network Printers.- Controla la impresión en impresoras de red y permite tener una lista blanca de impresoras permitidas.
- Network Shares.- Controla la subida de documentos en carpetas compartidas, permite tener una lista blanca de carpetas.
- FTP.- Controla la subida de documentos en servicios FTP, permite tener una lista blanca de sitios.

### **2.3.3. Acciones de Monitoreo.**

- Log.- Registra el incidente sin ninguna marca adicional.
- Alert.- Registra el incidente como una alerta
- No record.- No registra el incidente.
- Not configured.- No configurado, por defecto se comporta como No record.

### **2.3.4 Nivel de Monitoreo.**

- Incident.- Se registra solo el detalle del incidente sin el contenido del archivo.
- Text & Incident.- Se registra el contenido del archivo, información general del archivo y el detalle del incidente.
- Shadow & Incident.- Envía una copia completa del archivo al servidor de WAVE, junto con los detalles del incidente.

Combinando las acciones de seguridad, los canales y los roles de los empleados según el organigrama se ha definido la siguiente matriz.

ROL	EMAIL			Web		
	Permitir	Bloquear	Preguntar	Permitir	Bloquear	Preguntar
Gerente de Mercado			x			x
Subgerente de Mercado			x			x
Jefe de Marca			x		x	
	Dispositivos Externos			Cloud Storage		
	Permitir	Bloquear	Preguntar	Permitir	Bloquear	Preguntar
Gerente de Mercado			x			x
Subgerente de Mercado			x			x
Jefe de Marca		x			x	
	Impresoras Locales			Carpetas Compartidas		
	Permitir	Bloquear	Preguntar	Permitir	Bloquear	Preguntar
Gerente de Mercado		x				x
Subgerente de Mercado		x				x
Jefe de Marca		x				x
	Impresoras de Red			Almacenamiento Virtual		
	Permitir	Bloquear	Preguntar	Permitir	Bloquear	Preguntar
Gerente de Mercado			x			x
Subgerente de Mercado			x			x
Jefe de Marca			x		x	
	FTP					
	Permitir	Bloquear				
Gerente de Mercado		x				
Subgerente de Mercado		x				
Jefe de Marca		x				

Tabla 4.- Matriz de canales y acciones

#### 2.4. Creación de la política de Mercado.

- Para comenzar a crear las políticas del área de mercado procederemos a abrir la consola de WAVE y en la pantalla principal de la consola en la pestaña Home, en el menú Políticas escoger la opción Data Control.

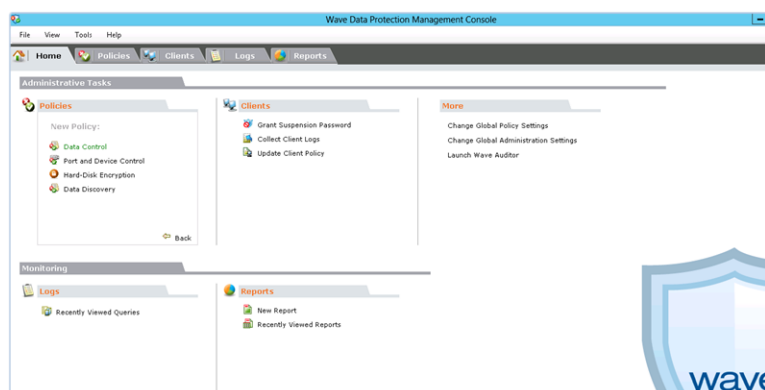


Figura 2. 1: Dashboard general de Wave Data Protection

- En el campo Policy name escribimos en este caso siguiendo la codificación estándar de la empresa: mercado\_001, si deseamos podemos colocar en el campo Descripción una frase breve, en este caso: Política de Mercado para Jefe de Marca.

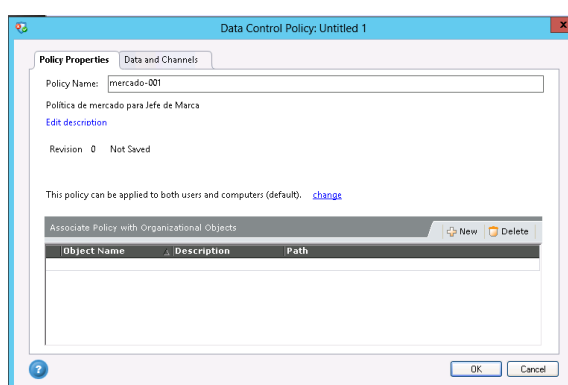


Figura 2. 2: Nombrando la política mercado\_001

- En la sección Associate Policy with organizational Objects, elegimos la opción New para poder añadir la OU que corresponda al área de

Mercado. Nos aparecerá la Figura 2.3 donde seleccionaremos la OU 1. Mercado-MKT y en la parte inferior izquierda presionaremos el botón de flecha verde a lado de la palabra GO, entonces aparecerá del lado derecho el listado de personas que trabajan en el área de mercado de la compañía, seleccionaremos a todos los que tengan el cargo de jefe de marca.

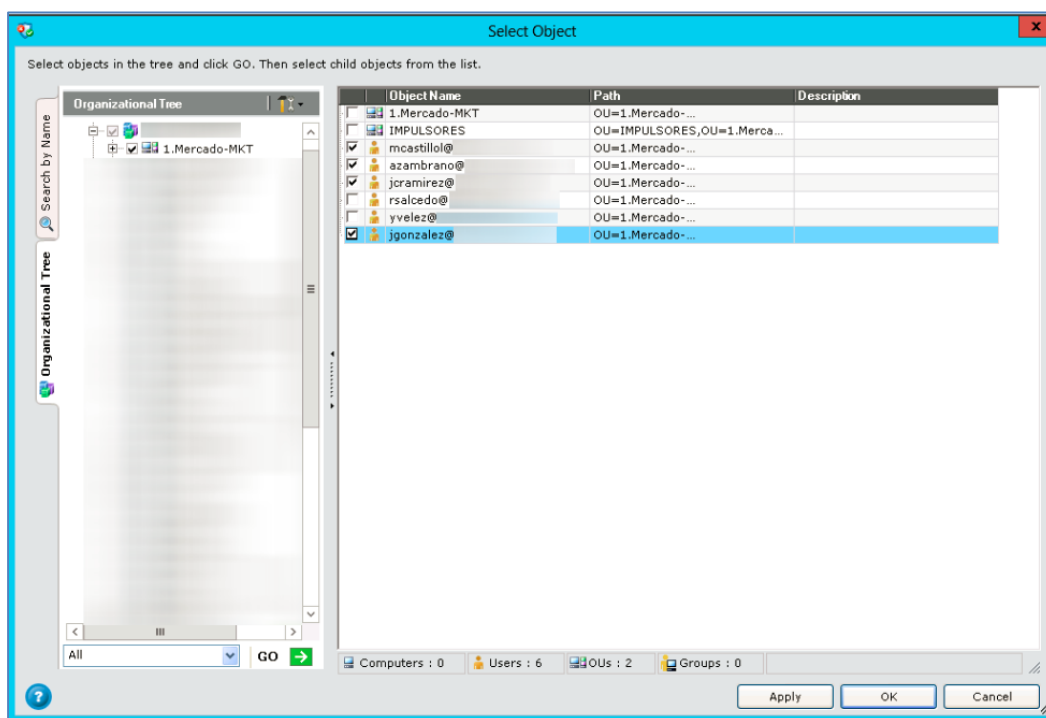


Figura 2. 3: Elección de la OU de Mercado

Al poner OK en la Figura 2.3, volveremos a la pantalla inicial, pero ya con todos los usuarios que serán parte de la política.



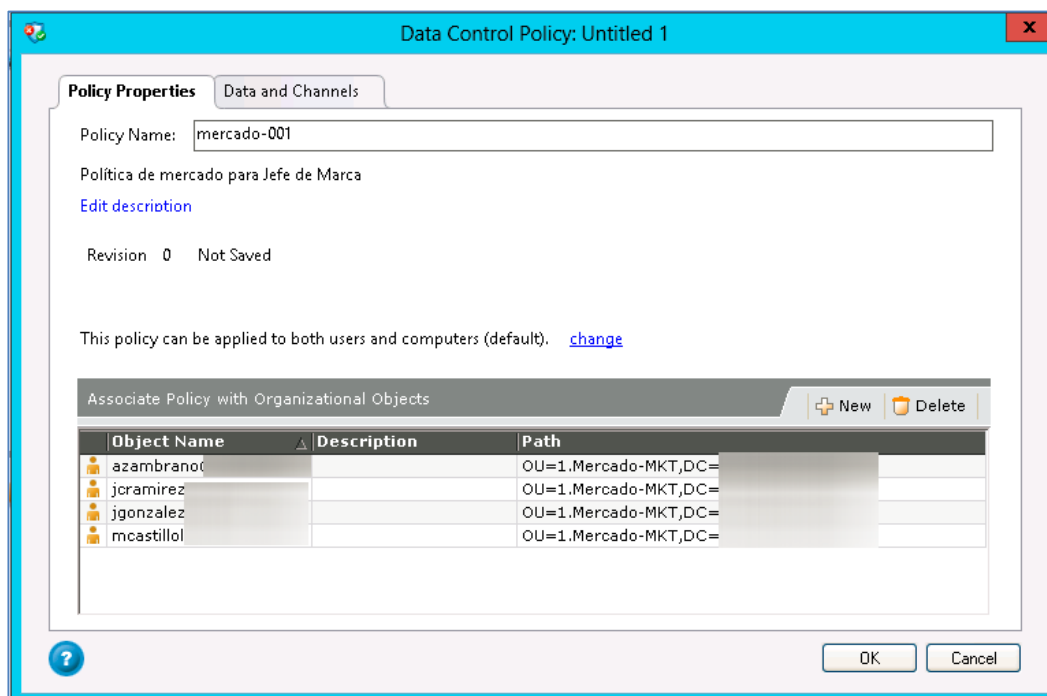


Figura 2. 4: Política con integrantes de la OU

- Ahora en la pestaña Data and Channels especificamos cada uno de los canales con sus respectivas acciones como lo detalla la Tabla 4 donde se detalla el canal de comunicación a usar y la acción de seguridad a seguir. Además de esto se configuran tres parámetros más: Acción de monitoreo, nivel de monitoreo y el mensaje que este caso hemos elegido el mensaje estándar, que puede ser modificado

al dar doble click sobre la palabra Global.

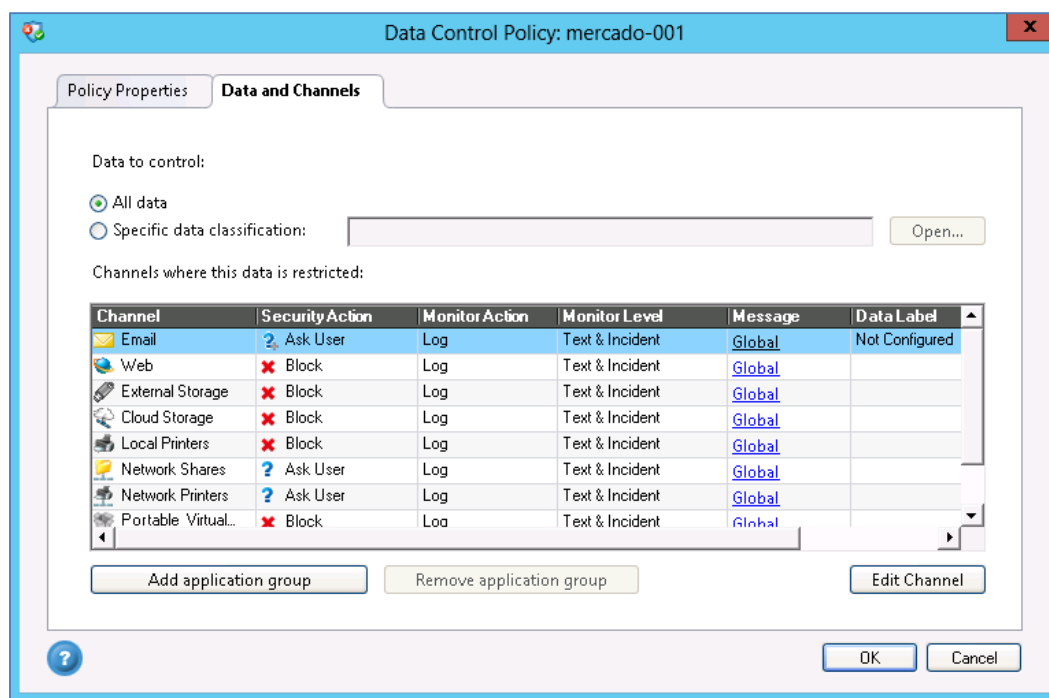


Figura 2. 5: Detalle de Canales y Acciones de Seguridad

Además, vamos a configurar ciertos parámetros en alguno de los canales:

**Email.-** Seleccionaremos esta línea y daremos click en el botón Edit Channel y nos posicionaremos en la pestaña Destination Exceptions List y daremos click en el botón ADD, para añadir una lista blanca, en este caso queremos conseguir que a pesar de que tiene este canal “EMAIL” restringido esto no aplique cuando se envíe email a sus jefes inmediatos como el gerente y subgerente del área.

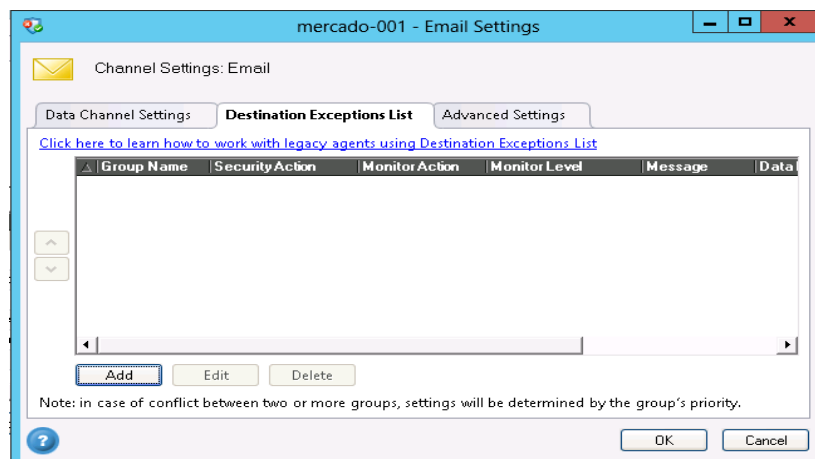


Figura 2. 6: Pantalla para ingresar lista blanca de correo.

Ingresamos uno a uno el correo del gerente y subgerente del área, y damos click en OK:

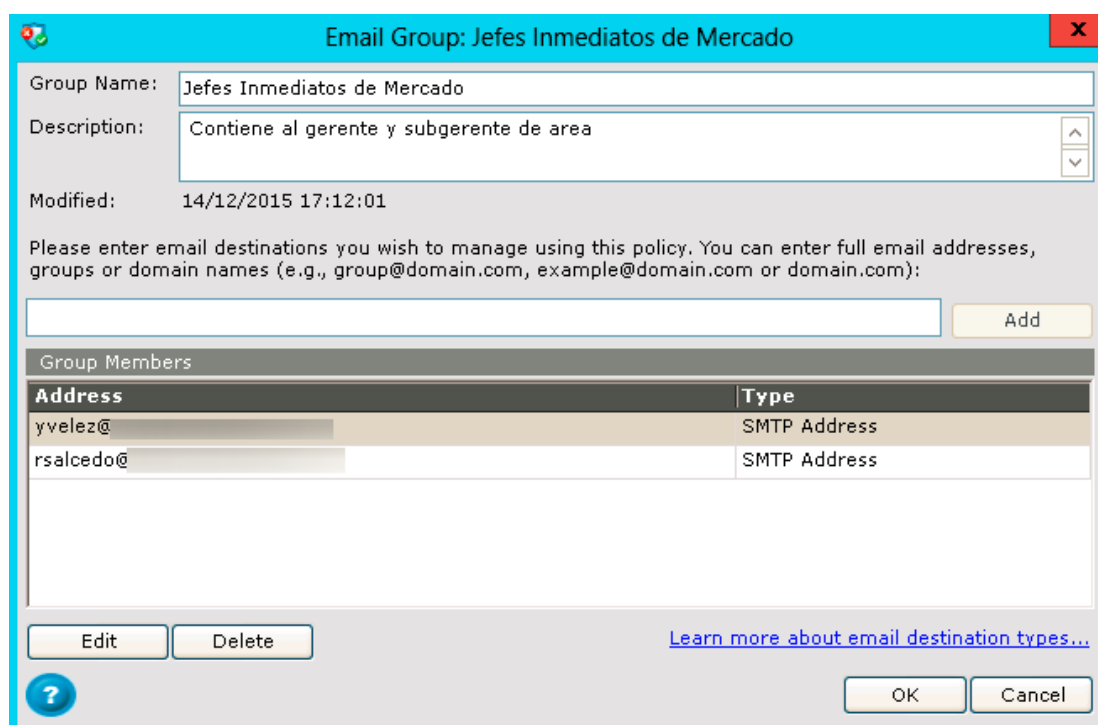


Figura 2. 7: Creación de lista blanca Jefes Inmediatos de Mercado.

Se pueden configurar excepciones para otros canales como web, ftp, impresoras y external storage, pero en este caso el cliente nos ha solicitado que las reglas sean bastante restrictivas.

## **2.5. Clasificación de la Información.**

El sistema usará estas definiciones para identificar la información y poder aplicar la acción de seguridad apropiada. Estas clasificaciones consisten en reglas booleanas (and, or, not)

La empresa ya tiene clasificada su información en Confidencial, Privada y Pública, teniendo que el tipo confidencial implica que su divulgación accidental o intencional el impacto sería incuantificable o crearía un impacto muy grande, privada crea un impacto económico no significativo y el público que no necesita ningún etiquetamiento. Existen otros tipos de niveles de clasificación que dependerá de la aplicabilidad en la empresa [5]

### **2.5.1. Tipos de Clasificación**

- **Keywords.-** Se identifica la información si contiene palabras específicas (palabras claves) , tiene un mecanismo de “pesos” que

facilita la identificación de los datos indicando cuantas veces debe aparecer esta palabra en un archivo para considerarlo como confidencial o restringido.

- **File Type.-** Tipos de archivos individuales son reconocidos de acuerdo a un análisis total del archivo,
- **File Properties.-** Algunos parámetros de metadata pueden ser usados para identificar contenido sensible.
- **Pattern.-** Reconocimiento de patrones de texto identifica incidentes que contienen un patrón predeterminado, tales como un correo electrónico, número telefónico, numero serial o números de tarjeta de crédito.
- **Data Fingerprints.-** Es usado para identificar contenido conocido aun si los datos han sido modificados parcialmente.

Se creará en base a la Tabla 3 una clasificación de la información sobre cada uno de los procesos que se manejan en el área de mercado.

En el menú principal, en la pestaña Políticas,(Figura 2.8) elegimos la opción Data Classifications y damos click en el botón NEW.

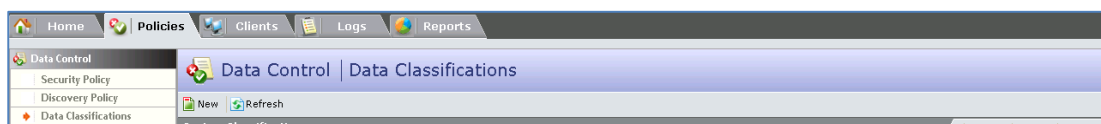
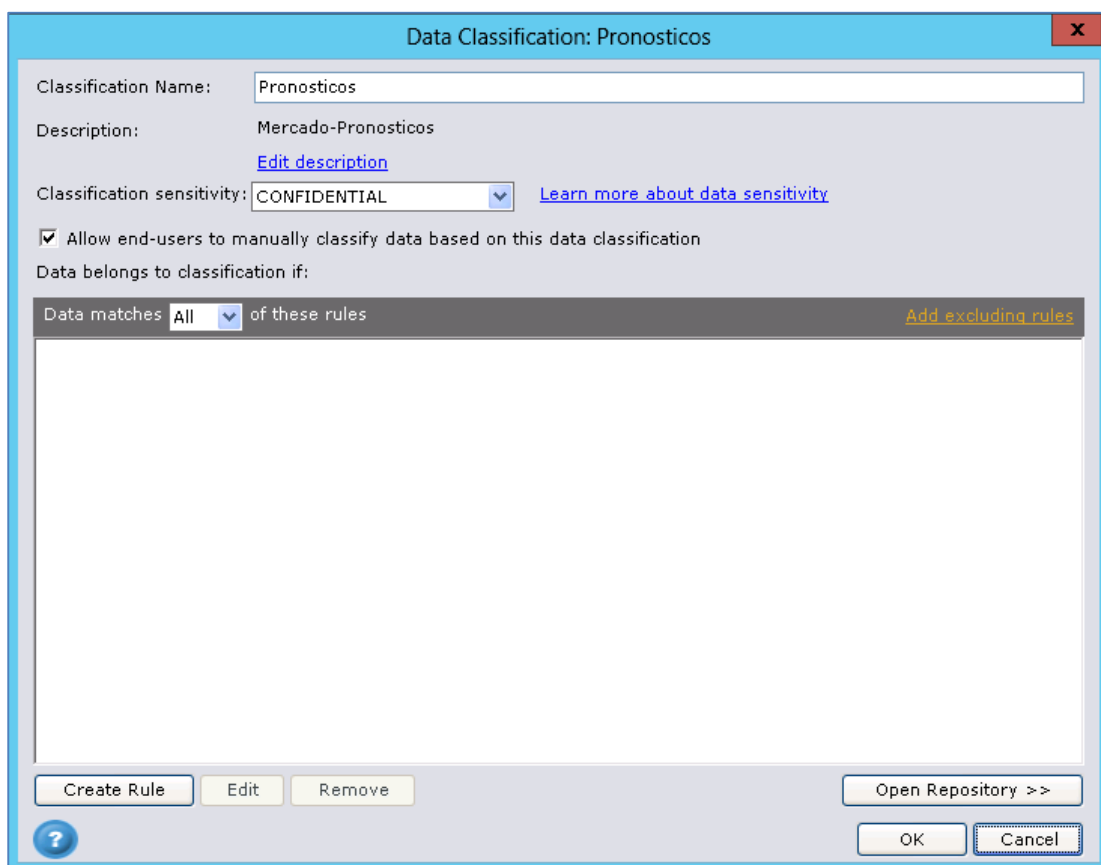


Figura 2. 8: Crear nueva Clasificación de la información

Comenzaremos por Pronósticos, en la sensibilidad de la información escogeremos confidencial y damos click en el botón Create new rule.



The screenshot shows a dialog box titled "Data Classification: Pronosticos". The fields are filled with the following information:

- Classification Name: Pronosticos
- Description: Mercado-Pronosticos
- Classification sensitivity: CONFIDENTIAL
- Allow end-users to manually classify data based on this data classification
- Data belongs to classification if: Data matches All of these rules

At the bottom of the dialog, there are several buttons: "Create Rule", "Edit", "Remove", "Open Repository >>", "OK", and "Cancel".

Figura 2. 9: Creación de Clasificación de Pronósticos

Nos preguntará que tipo de clasificación deseamos realizar, hemos decidido escoger la opción keyword, que se ajusta a nuestras necesidades y damos click en OK.

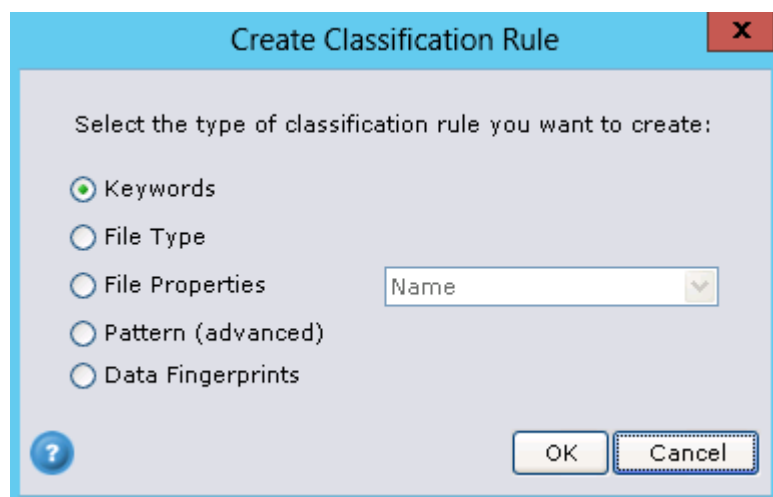


Figura 2. 10: Elección de tipo de clasificación.

Detallamos la primera regla con nombre Pronosticos\_001 y añadimos una a una las palabras claves junto a su peso, es decir las veces que debe aparecer esta palabra en el documento para considerarlo sensible. (Figura 2.11)

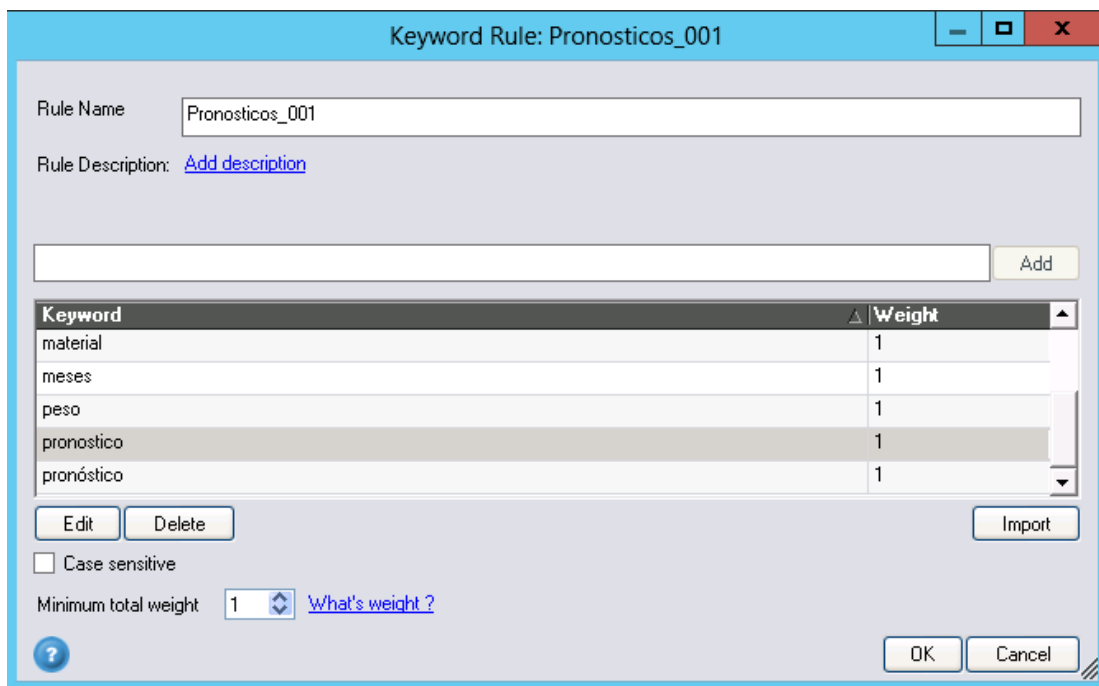


Figura 2. 11: Añadir keywords.

Así creamos en base a la Tabla 3, todas las clasificaciones.

Name	Description	Data Sensitivity Level
1.Pronosticos	Mercado-Pronosticos	CONFIDENTIAL
2.Presupuestos	Mercado-Presupuestos	CONFIDENTIAL
3.Estudio de mercado	Mercado-Estudio de mercado	CONFIDENTIAL
4.Acuerdo con proveedores	Mercado-Acuerdo con proveedores	CONFIDENTIAL
5.Analisis de oportunidad	Mercado-Analisis de Oportunidad	CONFIDENTIAL
6.Data maestra de articulos	Mercado-Data maestra de articulos	CONFIDENTIAL
7.Oferta promociones y descuentos	Mercado-Ofertas promociones y descuentos	CONFIDENTIAL
8.Precios y margenes de ganancia	Mercado-Precios y margenes de ganancia	CONFIDENTIAL

Figura 2. 12: Clasificaciones del área de Mercado.



## CAPITULO 3

### ANÁLISIS DE RESULTADOS

#### 3.1 Pruebas en escenarios programados.

Todas las pruebas las realizaremos con el usuario mcastillol con perfil de jefe de marca porque es el perfil que más restricciones tiene. Hemos creado una plantilla de pruebas para poder evaluar cada uno de los canales de comunicación relacionado con la clasificación confidencial que el departamento de Mercado realiza.

Se utilizarán tres tipos de clasificación de la información: 1. Pronósticos, 3. Estudio de Mercado y 5. Analisis de Oportunidad y los probaremos con algunos de los nueve canales que se han controlado. En la siguiente tabla resumimos el total de las pruebas, aunque luego hemos detallado el proceso de prueba en cuatro escenarios

#	Canal	Escenario	Expectativa	Detalle de Datos de Prueba	Mensaje presentado al usuario.	¿Cumplio expectativa?
1	Correo Electrónico	Se enviará un correo electrónico y se copiará dentro del cuerpo un reporte de pronósticos teniendo como destinatario un correo personal del usuario.	La regla definida en 1. Pronosticos y la restricción del canal email debe exigir que el usuario escriba una explicación antes de poder enviar el correo y esto quedará registrado en los logs de la consola.	Muestra de un reporte de Pronosticos real de la compañía dentro del cuerpo del correo	Pregunta si esta seguro de enviarlo	Si
2	Web	Se subirá un archivo con información confidencial sobre pronósticos en una página para compartir archivos www.wetransfer.com, adjuntaremos un documento en Excel con la misma información del escenario 1.	No debe permitir subir el archivo al portal ya que está controlada por la clasificación de información 1.Pronosticos y el canal WEB.	Muestra de un reporte de Pronosticos real de la compañía en formato excel	Mensaje de bloqueo	Si
3	Almacenamiento Externo	Se copiará un archivo de word con información confidencial sobre pronósticos en un dispositivo externo, en este caso un pen drive.	No debe permitir copiar el archivo al pen drive ya que está controlada por la clasificación de información 1.Pronosticos y el canal External Storage..	Muestra de un reporte de Pronosticos real de la compañía en formato word	Mensaje de bloqueo	Si
4	Carpeta Compartida	Se copiará un archivo de Word con información confidencial sobre pronósticos en la carpeta compartida de mercado	Antes de poder copiar el archivo a la ubicación compartido, se le presentará una pantalla preguntando si está seguro de realizar la acción y que justifique su acción	Muestra de un reporte de Pronosticos real de la compañía en formato word	Mensaje de bloqueo	Si
5	Cloud Storage	Se copiará un archivo de excel con información confidencial en el cliente de google drive	No debe permitir la copia del archivo al aplicativo (cliente) google drive porque esta controlada por la clasificación de la información 3. Estudio de Mercado y el canal Cloud Storage	Archivo excel con datos reales de estudios de mercado de la compañía	Mensaje de bloqueo	Si
6	Impresora Local	Se enviará a imprimir información de un archivo txt con información confidencial a una impresora conectada via usb	No debe permitir la impresión del contenido del archivo porque esta controlada por la clasificación de la información 3. Estudio de Mercado y el canal Impresora Local	Archivo txt con datos reales de estudios de mercado de la compañía	Mensaje de bloqueo	Si
7	Impresora en Red	Se enviará a imprimir información de un archivo word con información confidencial a una impresora del servidor de cota de impresión de la compañía.	Antes de permitir la impresión del contenido del archivo se preguntará al usuario si esta seguro de su decisión y se pedirá justificación porque esta controlada por la clasificación de la información 5. Analisis de la oportunidad y el canal Impresora en Red	Archivo word con datos reales de un reporte de Analisis de oportunidad de la compañía	Pregunta si esta seguro de enviarlo	Si
8	Almacenamiento Virtual Portable	Se copiará un archivo pdf con información confidencial en un celular marca SAMSUNG con S.O. Anroid 5.0 que no es reconocido en el computador como Almacenamiento externo.	No debe permitir la copia del archivo porque esta controlada por la clasificación de la información 5. Analisis de la oportunidad y el canal Almacenamiento Virtual Portable	Archivo pdf con datos reales de un reporte de Analisis de oportunidad de la compañía	Mensaje de bloqueo	Si
9	FTP	Se copiará un archivo pdf con información confidencial en un servidor FTP de la compañía FTP://empresarial/uploads	No debe permitir la copia del archivo porque esta controlada por la clasificación de la información 5. Analisis de la oportunidad y el canal FTP	Archivo pdf con datos reales de un reporte de Analisis de oportunidad de la compañía	Mensaje de bloqueo	Si

Tabla 5.- Pruebas en escenarios programados.

- Escenario 1.- Se enviará un correo electrónico y se copiará dentro del cuerpo un reporte de pronósticos teniendo como destinatario un correo personal del usuario.

Expectativa.- La regla debe exigir que el usuario escriba una explicación antes de poder enviar el correo y esto quedará registrado en los logs de la consola.

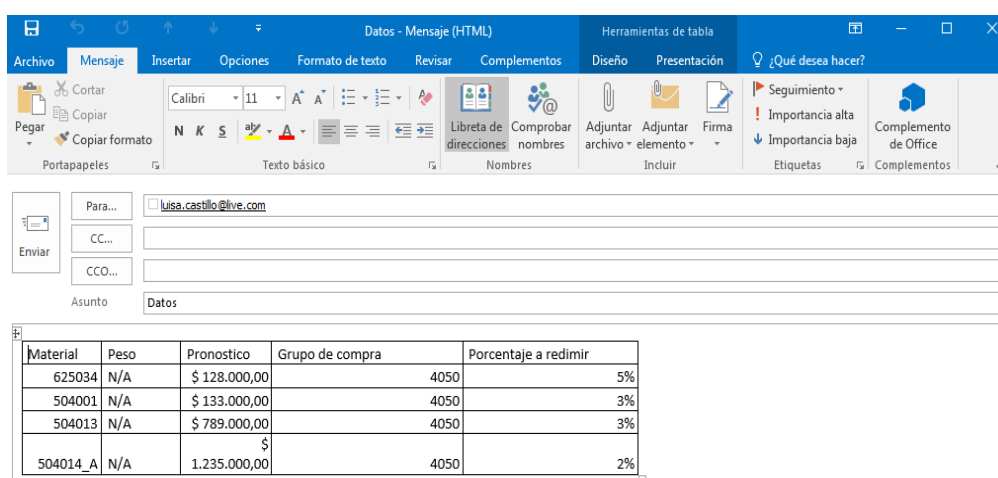


Figura 3. 1: Envío de correo en escenario 1

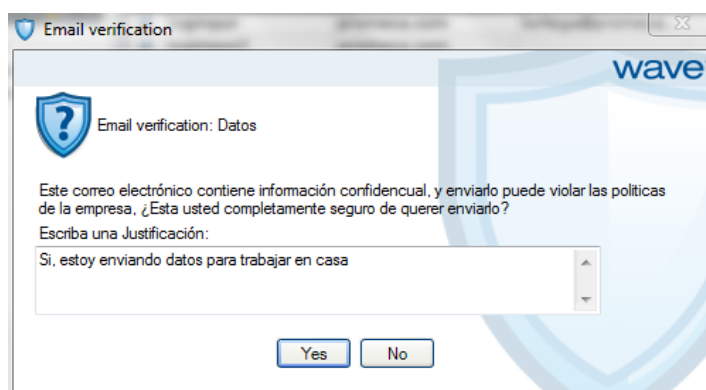


Figura 3. 2: Pregunta en escenario 1

Luego en el dashboard de la consola del servidor en la pestaña LOGS, el administrador puede revisar el detalle de la acción realizada por el usuario.

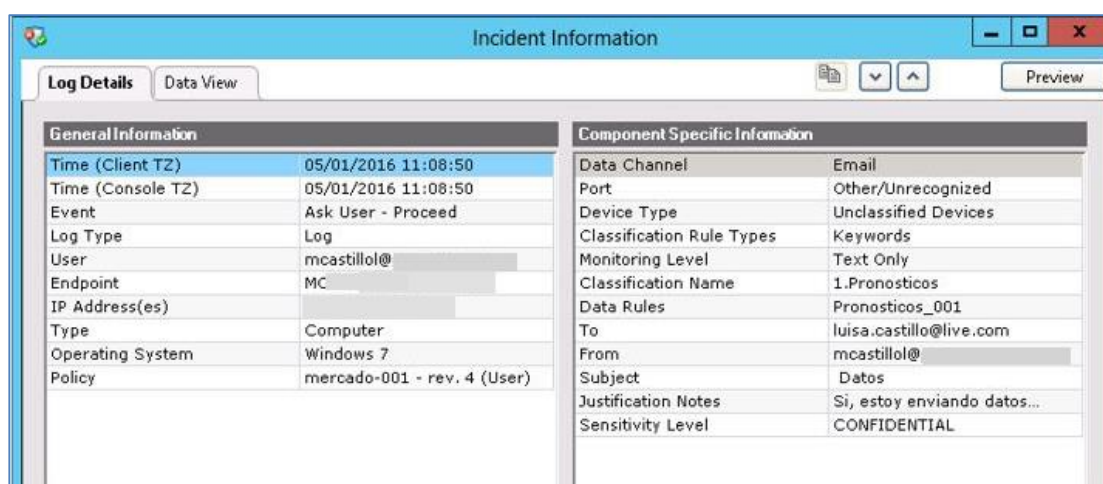


Figura 3. 3: Revisión de log en escenario 1

En la pestaña Data View podemos observar el contenido del correo

The screenshot shows a window titled "Incident Information" with a "Data View" tab. The main area contains a table with the following data:

Material	Peso	Pronostico	Grupo de compra	Porcentaje a redimir
625034	N/A	\$ 128.000,00	4050	5%
504001	N/A	\$ 133.000,00	4050	3%
504013	N/A	\$ 789.000,00	4050	3%
504014 A	N/A	\$ 1.235.000,00	4050	2%

Below the table is a file list with columns: Name, File Size, Date Modified, Time Modified. One entry is visible:

Name	File Size	Date Modified	Time Modified
Email		05/01/2016	11:08

On the right side, there is a "Classification Details" panel with a table:

Classification Rule	Rule Name
Keywords	Pronosticos
Keywords	Pronosticos
Keywords	Pronosticos
Keywords	Pronosticos

Figura 3. 4: Vista del detalle del contenido del correo.

- Escenario 2.- Se subirá un archivo con información confidencial sobre pronósticos en una página para compartir archivos [www.wetransfer.com](http://www.wetransfer.com), adjuntaremos un documento en Excel con la misma información del escenario 1.

Expectativa. - No debe permitir subir el archivo al portal ya que está controlada por la clasificación de Información 1.Pronosticos y el canal WEB.

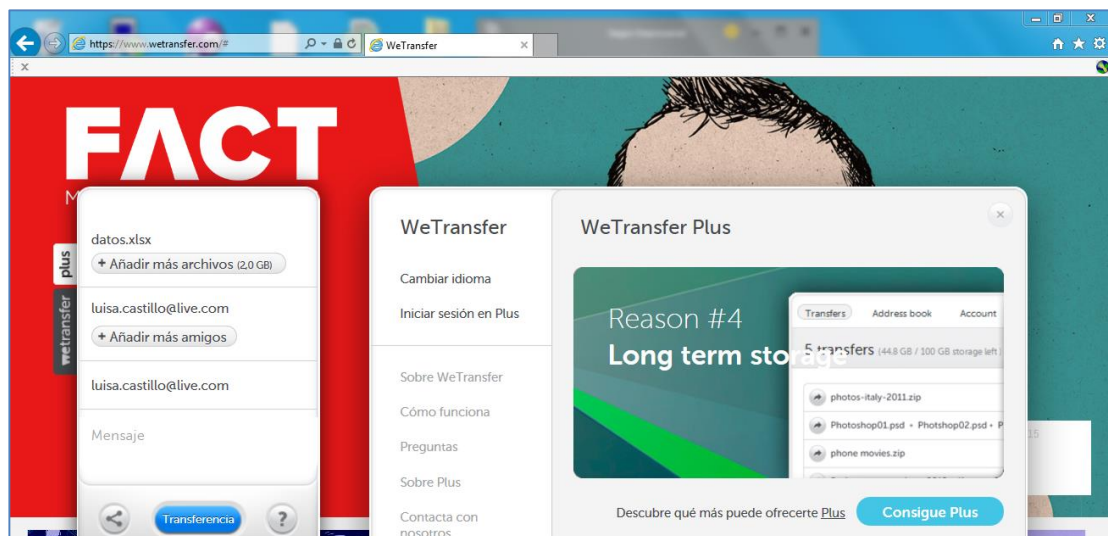


Figura 3. 5: Sitio wetransfer en escenario 2

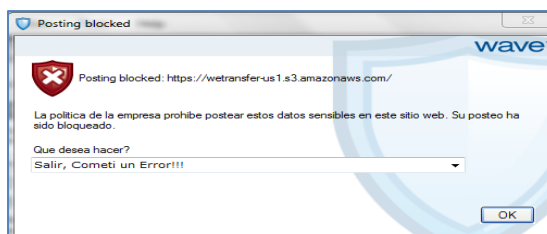


Figura 3. 6: Mensaje de bloqueo web en escenario 2

General Information		Component Specific Information	
Time (Client TZ)	05/01/2016 12:13:20	Data Channel	Web
Time (Console TZ)	05/01/2016 12:13:20	Port	Other/Unrecognized
Event	Blocked	Device Type	Unclassified Devices
Log Type	Log	File Name	Web...
User	mcastillo@...	Extension	.txt;.bin;.xlsx
Endpoint	MC	File Size	12941
IP Address(es)		Classification Rule Types	Keywords
Type	Computer	Monitoring Level	Text Only
Operating System	Windows 7	Classification Name	1.Pronosticos
Policy	mercado-001 - rev. 4 (User)	Data Rules	Pronosticos_001
		URL	https://wettransfer-...
		Referrer URL	https://www.wetransfer.com...
		User Justification	Salir, Cometi un Error!!!
		Sensitivity Level	CONFIDENTIAL

Figura 3. 7: Muestra de log en escenario 2

Resultado: Se ha conseguido superar este escenario de manera exitosa.

- Escenario 3.- Se copiará un archivo de word con información confidencial sobre pronósticos en un dispositivo externo, en este caso un pen drive.

Expectativa. - No debe permitir copiar el archivo al pen drive ya que está controlada por la clasificación de Información 1.Pronosticos y el canal External Storage.

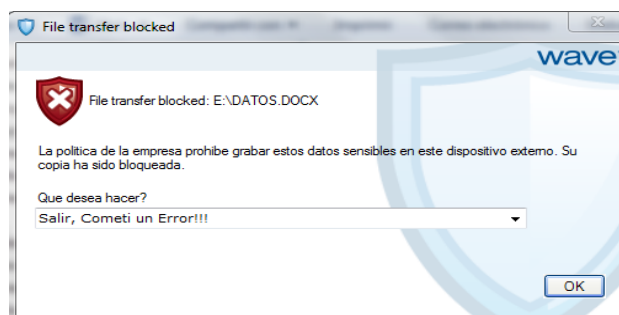


Figura 3. 8: Mensaje de bloqueo en escenario 3

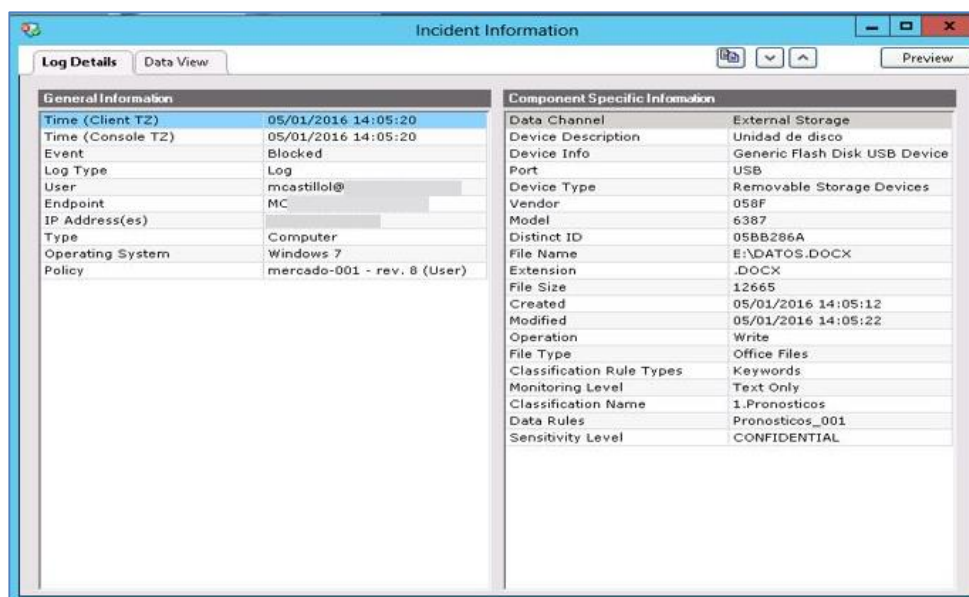


Figura 3. 9: Log en escenario 3

- Escenario 4.- Se copiará un archivo de Word con información confidencial sobre pronósticos en la carpeta compartida de mercado.

Expectativa. – Antes de poder copiar el archivo a la ubicación compartido, se le presentará una pantalla preguntando si está seguro de realizar la acción y que justifique su acción.

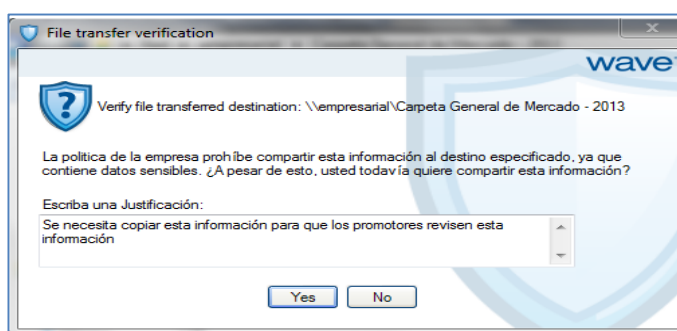


Figura 3. 10: Mensaje de pregunta en escenario 4



The screenshot shows a window titled "Incident Information" with two tabs: "Log Details" (selected) and "Data View". The "Log Details" tab contains two tables. The first table, "General Information", lists event details. The second table, "Component Specific Information", lists technical details about the data channel and classification.

General Information	
Time (Client TZ)	05/01/2016 15:51:01
Time (Console TZ)	05/01/2016 15:51:01
Event	Ask User - Proceed
Log Type	Log
User	mcastillo@
Endpoint	MC
IP Address(es)	
Type	Computer
Operating System	Windows 7
Policy	mercado-001 - rev. 19 (User)

Component Specific Information	
Data Channel	Network Share
Port	Other/Unrecognized
Device Type	Unclassified Devices
File Name	datos.xlsx
Extension	.xlsx
File Size	12402
Classification Rule Types	Keywords
Monitoring Level	Text Only
Classification Name	1.Pronosticos
Data Rules	Pronosticos_001
Destination	\\empresarial\Carpeta...
Destination Display Name	\\empresarial\Carpeta...
Justification Notes	Se necesita copiar esta...
Sensitivity Level	CONFIDENTIAL

Figura 3. 11: Log en escenario 4.

## CONCLUSIONES Y RECOMENDACIONES

1. La herramienta tecnológica WAVE nos da el soporte para evitar fuga de información sensible ya sea de forma voluntaria o involuntaria a través de la clasificación de la información y las diferentes acciones de permisión o bloqueo en los diferentes canales de comunicación existentes, además permite que personal administrativo monitoree a través de su consola los registros. WAVE es de gran ayuda cuando los empleados tienen malos hábitos que ponen en riesgo la información de la empresa.
2. A pesar de que la empresa tiene un robusto sistema de seguridad de la información, un sistema DLP les ha permitido tener mayor control a nivel granular sobre las acciones de sus usuarios sobre la información que es considerada sensible.
3. Ampliar la implementación del sistema DLP a todas las áreas de la empresa que manejen información sensible.
4. Definir una persona neutral dentro de la organización responsable de la revisión de logs y de las acciones a tomar según se necesite.
5. Definir tipos de canales necesarios donde se incluyan clientes FTP, aplicaciones de smartphones con S.O. IOS.

## BIBLIOGRAFÍA

- [1] Winkler Mike, 10 things that I used to be good ideas in data security, Brayne Babe Micro Pub, 2014
- [2] Asaft Shaftai, Yuval Elovici, Lior Rokach, A survey of data leakage detection and prevention solutions, Springer, 2012.
- [3] Cisco Systems, Fuga de datos a nivel mundial: El elevado costo de las amenazas internas, [http://www.cisco.com/web/offer/em/pdfs\\_innovators/LATAM/data\\_threat\\_sp.pdf?sid=177824\\_11](http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_threat_sp.pdf?sid=177824_11), fecha de consulta Noviembre del 2015
- [4] Microsoft, Creación de huella digital de documento, [https://technet.microsoft.com/es-s/library/dn635176\(v=exchq.150\).aspx](https://technet.microsoft.com/es-s/library/dn635176(v=exchq.150).aspx), fecha de consulta Noviembre 2015.
- [5] Gutierrez Camilo, Cómo clasificar la información corporativa, <http://www.welivesecurity.com>, fecha de consulta Noviembre 2015.