Desarrollo de la Política de Seguridad de la Información: Cabrera Auto

Jennifer Sevilla Maldonado
Maestría en Ciencia de Computadoras
Jeffrey Duffany, Ph.D.
Departamento de Ingeniería Eléctrica y Computadoras y Ciencia de Computadoras
Universidad Politécnica de Puerto Rico

Abstracto — *Actualmente las empresas de venta y renta de autos enfrentan una serie de cambios que las obliga a generar nuevas estrategias para la protección de la información que custodian. El aumento en casos de fraudes bancarios como por ejemplo el robo de identidad amenazan constantemente a las empresas empujándolas a aumentar sus medidas de seguridad con el fin de salva guardar la información personal de sus clientes asumiendo una mayor responsabilidad fiduciaria. El auge en el uso de tecnología para el manejo de la información pone en un mayor panorama de riesgo a las empresas relacionadas a la industria automotriz si estas no utilizan las medidas de seguridad adecuadas. Por tales razones he desarrollado una política de seguridad de la información para la empresa en la cual actualmente trabajo, Cabrera Auto.*

Términos claves — *Amenazas, Contramedidas, Riesgos, Seguridad de la Información.*

INTRODUCCIÓN

La *política de seguridad de la información* [1] que he desarrollado pretende proteger la empresa Cabrera Auto de consecuencias legales por el mal manejo de información confidencial y personal de clientes que repercuta en gastos innecesarios para la empresa poniéndola en un posible mal estado económico. Además dicha *política de seguridad de la información* [1] también tiene como meta mantener la buena reputación de la empresa.

Para el desarrollo de esta política se realizó un *análisis de riesgos y amenazas* [2] para la implementación de contramedidas que ayudan a mitigar los riesgos existentes o futuros. Se generó un *plan de contingencia* [3] donde se delegaron un sinnúmero de responsabilidades asignadas a cada empleado del departamento de IT existente en Cabrera Auto para que puedan tener una respuesta rápida en caso de pérdida o interrupción momentánea de los sistemas de información.

TRANSFONDO

La *seguridad informática* [4] se basa en las características y condiciones de los sistemas de procesamiento de información y su almacenamiento garantizando la confidencialidad, integridad y disponibilidad de los datos.

- **Confidencialidad –** Información que solo puede ser vista o modificada por personas autorizadas al acceso y transferencia de los datos almacenados.
- **Integridad –** Datos completos sin modificación o alteración de su estado original.
- **Disponibilidad –** Se refiere a la garantía de acceso a los datos en el momento necesario.

Esta *seguridad informática* [4] ha sufrido una serie de cambios que han llevado a las empresas a la necesidad de invertir para proteger uno de los recursos más valiosos como es la información. Esta inversión va atada a un conjunto de elementos como la compra de equipos, consultoría externa o la reestructuración del departamento de "IT" existente en la empresa.

Una *política de seguridad de la información* [1] es una herramienta para la protección de la información y evitar el riesgo de la perdida de la confidencialidad, integridad y disponibilidad de los datos. Con los avances tecnológicos y el fácil acceso al internet, las *políticas de seguridad de la información* [1] se hacen cada día más un requisito vital para la salud de una empresa.

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE CABRERA AUTO

El enfoque principal de estos objetivos es encauzar una serie de problemas y guiar a la empresa a sus soluciones inmediatas mediante el uso de medidas de carácter estricto y compulsorio.

- Proteger los recursos de información y la tecnología de Cabrera Auto utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el propósito de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
- Mantener las *políticas de seguridad de la información* [1] actualizadas, con el fin de asegurar su vigencia y nivel de eficacia.

DESCRIPCIÓN DE LA EMPRESA

Cabrera Auto es una empresa netamente puertorriqueña con más de sesenta años de experiencia en la industria de venta automotriz. Cuenta con varias localidades a nivel nacional haciendo de esta una de las compañías de auto más grandes de Puerto Rico. Estas se componen por Cabrera "Car & Truck Rental" en Carolina, San Juan, Manatí, Arecibo y Aguadilla, Cabrera Usados Manatí y Arecibo, Cabrera Ford, Cabrera Chrysler, Cabrera GM y Cabrera Nissan. Además de sus áreas de servicio para todas sus marcas, cuentan con servicio Mazda, Suzuki y Mitsubishi.

Cabrera es manejado por una fuerza laboral de más de 250 empleados. Combinando los avances de tecnología, la experiencia en la industria y un equipo de excelencia Cabrera Auto es sin duda una de las marcas de ventas y renta de autos más reconocida en Puerto Rico.

INFLUENCIAS PARA EL MAL USO DE LA INFORMACIÓN

El mal uso de la información es una modalidad muy común desde comienzos del año dos mil. Aunque ya era un problema existente a nivel mundial tomo gran auge con la llegada de los servicios de internet domésticos, las redes sociales y los teléfonos inteligentes. Expertos en el tema declaran que el *robo de identidad* [5] trasciende a historias bíblicas del viejo testamento donde por ejemplo un hijo le robo la identidad a su hermano usando su perfume y sus vestidos para recibir la bendición de su padre antes de fallecer.

Cada día se hace más fácil el acceso de la información personal a manos ajenas. Hoy día no solo a nivel internacional sino a nivel nacional existe un gran crecimiento en este sector criminal logrando ser una gran amenaza para ciudadanos e instituciones que manejan información sensitiva. Factores sociales como la crisis económica que atraviesa el país son precipitaderos de crímenes informáticos.

La policía de Puerto Rico en conjunto con algunas instituciones bancarias, han diseñado estrategias nuevas para dar con estos grupos de maleantes de manera más efectiva. Se ha designado un departamento de fraude bancario para manejar estos casos.

En la industria automotriz los robos de autos a través del robo de identidad [5] son la orden del día. mega empresas de autos invierten una gran tajada de su presupuesto en consultorías para minimizar los riesgos de pérdida de información. Esto con el fin de protegerse de enfrentamientos legales con las víctimas de fraude. Esta situación es sumamente delicada y hasta han ocurrido casos por los cuales las empresas se han tenido que ir a la quiebra porque sus recursos económicos no son suficientes para sobrellevar estos asuntos legales.

RIESGOS Y AMENAZAS

En este proyecto se estableció un análisis exhaustivo de *riesgos y amenaza* [2] para la implementación de contramedidas efectivas para el

desarrollo de procedimientos estrictos con el fin de garantizar la seguridad de la información custodiada por la empresa. Fueron identificados todos los activos físicos y sistemas con *vulnerabilidades* [6] los cuales requieren mayor protección. A continuación un gráfico de las posibles amenazas y su factor de riesgo.

Tabla 1
Filtración de Agua

Amenazas	**Factor de Riesgo**				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Incendios					x
Inundación				x	
Tormentas		x			
Sismo					x
Sobre carga eléctrica				x	
"Hackers"			x		
Virus o malware				x	
Robo			x		
Sabotaje			x		
"Rootkits"			x		
"Denial of Service"	x				
Pishing		x			
Leakage		x			
Keyloggers		x			
Mal manejo de contraseñas		x			

DESGLOCE DE ACTIVOS FÍSICOS Y SISTEMAS DE LA EMPRESA

Actualmente Cabrera cuenta con aproximadamente 250 computadoras, 6 servidores, 19 impresoras, 20 "routers", 325 teléfonos, 1 puerta de tele entrada y cintas magnéticas (copia de seguridad). Esta empresa utiliza varios sistemas tanto internos como externos. Los sistemas internos son: "CDK Drive", "Red Bumper", "CCM", "Bluebird", "Momentum", "Office 365" y "Menu Vantage". Los sistemas externos son: "EFirst Class", "Pada", y "Originate". Todos estos son portales bancarios para el manejo de solicitudes y contratos de préstamos de auto. A continuación un gráfico de los activos y su costo aproximado:

Tabla 2
Activos Físicos y Costo Aproximado

Activos físicos	**Costo aproximado por unidad en caso de daño o pérdida**
Computadoras	600.00
Servidores	4,000.00
Impresoras	3,000.00
Teléfonos	400.00
"Routers"	2,000.00
Cintas de copia de seguridad	20.00

CONTRAMEDIDAS

- Todos los equipos eléctricos deben tener una batería de energía (UPS). Conllevará un costo aproximado de $55.00 por unidad.
- Se necesitaran bases para la elevación de las torres de computadoras al menos 6" del suelo para la prevención de daños por elementos líquidos o inundación. Conllevará un costo aproximado de $25.00 por unidad.
- Las computadoras requieren ser apagadas durante el tiempo de inactividad mayor de 2 horas.
- Es importante que todas las computadoras tengan su antivirus activo y actualizado para la detección de virus o "malwares".
- Todo usuario deberá tener una contraseña segura para la prevención del acceso no autorizado siguiendo las reglas establecidas en la política de seguridad.
- No se colocaran objetos o papeles que obstruyan la ventilación del equipo. Para esto el personal de sistemas tendrá que buscar la manera de concientizar a los empleados sobre

los riesgos a través de charlas, comunicados, etc.

- Instalación de tormenteras para la prevención de roturas de cristales durante fenómenos atmosféricos. Conllevará un costo aproximado de $5-10k por lote.
- Instalación de cámaras de seguridad dentro de los previos. Esto servirá como evidencia en caso de un robo. Actualmente solo las sucursales de Cabrera "Car & Truck Rental" cuentan con estos equipos.
- Se instalarán láminas de privacidad en todos los monitores de las computadoras de empleados gerenciales. Conllevará un costo aproximado de $50.00 por unidad.
- Reubicación de los servidores a lugares limpios, frescos y seguros.

RECOPILACIÓN DE EVIDENCIAS

A continuación se presentan unas fotos que evidencian algunas de las amenazas que enfrenta Cabrera Auto actualmente:

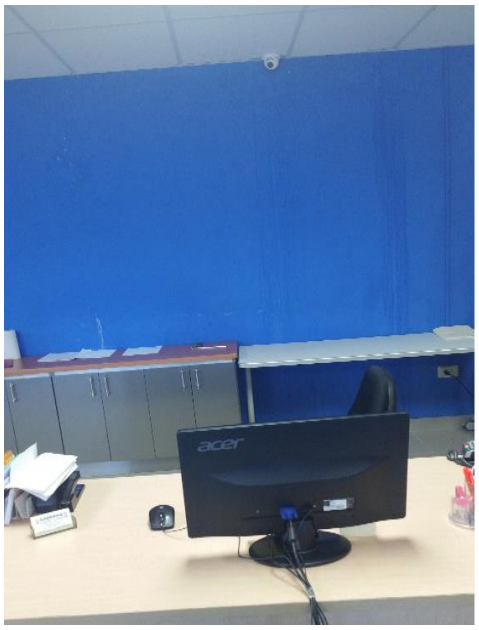

Figura 1
Filtración de Agua

Figura 2
Computadora de Gerente Descuidada con los Portales Bancarios Abiertos

Figura 3
Servidores sin Ventilación Mecánica

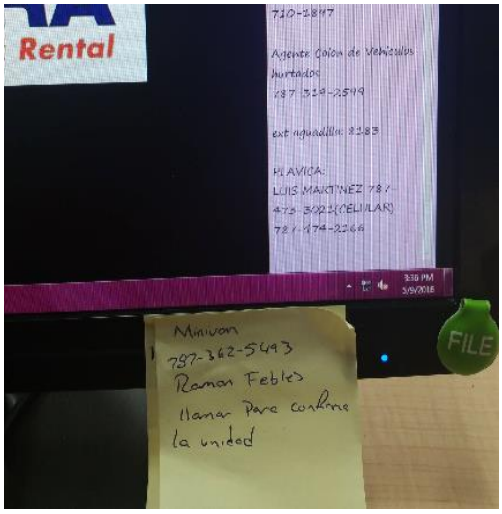

Figura 4
Contraseña en una Nota en el "Desktop"

ANÁLISIS DE IMPACTO

¿Qué es el *análisis de impacto*? [7] Este análisis es la estimación de daños que podría enfrentar una empresa como consecuencia de un incidente o desastre. El *análisis de impacto* [8] se enfoca en la identificación, análisis y valoración de amenazas en la seguridad informática de los activos críticos de la empresa y evaluando la probabilidad de ocurrencias y las consecuencias que pueda ocasionar a la empresa. Cuenta con dos objetivos principales: la identificación de funciones críticas para la operación de la empresa. Se catalogan como 'funciones no críticas" aquellas que son inaceptables a la pérdida o interrupción de las mismas durante un plazo mayor de 24 o 48 horas de acuerdo al criterio de la empresa. Tomando como medida el valor absoluto de sus ejecuciones y la imposibilidad de ser sustituidas a y la priorización del conjunto de funciones. Además este *análisis de impacto* [8] es la base para la creación del *plan de contingencia* [3].

PLAN DE CONTINGENCIA

Un *plan de contingencia* [3] es una guía para el manejo de equipos y la recuperación de las funciones más críticas luego de una interrupción no esperada por un periodo de más de 24 horas. Un *plan de contingencia* [3] fue creado paralelo a la política de seguridad de la información teniendo en mente la continuidad de los procesos más críticos de Cabrera Auto con el fin de restablecer operaciones a sus funciones normales y evitar la pérdida de información valiosa para el negocio. El plan al cual fue llamado como Cabrera Seguro fue desarrollado con un orden estricto de procedimientos asignados al personal adscrito al departamento de sistemas del departamento de "IT": Cabrera Auto. A continuación el organigrama del departamento de "IT":

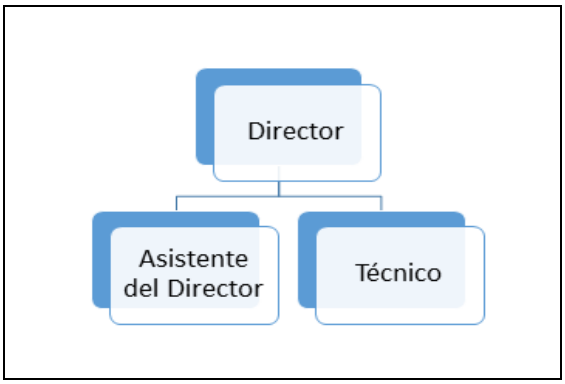

Figura 5
Departamento de "IT"

Los siguientes objetivos se han establecido para este plan:

- Maximizar la eficacia de las operaciones de contingencia a través de un plan establecido que se compone de las siguientes fases: 1) fase de notificación / activación para detectar, evaluar los daños y activar el plan, 2) fase de recuperación para restaurar las operaciones de "IT" temporales y recuperar el daño realizado al sistema original y 3) fase de reconstitución para restaurar el sistema de "IT" procesando capacidades a las operaciones normales.
- Identificar las actividades, los recursos y procedimientos necesarios para llevar a cabo los requisitos de procesamiento de Cabrera Auto durante las interrupciones prolongadas a las operaciones normales.
- Asignar responsabilidades al personal de Cabrera Auto y proporcionar orientación para recuperar los sistemas durante períodos prolongados de interrupción de las operaciones normales.
- Asegurar la coordinación con otros del personal de Cabrera Auto que va a participar en las estrategias de planificación de contingencia. Asegurar la coordinación con puntos externos de contacto y proveedores que van a participar en las estrategias de plan de contingencia.

FUENTES DE APOYO INTERNAS

- Carmelo Rodriguez – Asistente de director IT.
- José Laó De La Cruz – Gerente de financeamiento.
- José Gonzalez Antonmarchi – Especialista de ventas digitales.
- Pedro Polanco – Director Centro de desarrollo del negocio.

CONCLUSIÓN

Definitivamente la *seguridad informática* [4] hoy día es un aspecto crítico en las empresas que manejan información sensitiva de terceros. La evolución de la tecnología y el aumento en los crímenes cibernéticos han sido factores influyentes que han obligado a las empresas a tomar medidas estrictas para proteger los datos almacenados. Cabrera Auto no es la excepción. La implementación de una nueva política de seguridad es sumamente vital para la salud y continuidad del negocio. La inversión en nuevas medidas y equipos para salva guardar la información es una cantidad mínima comparado con los gastos que la empresa podría enfrentar por conceptos legales relacionados al mal manejo de la información.

Es importante destacar que para que una política de seguridad funcione eficazmente las empresas deben concientizar a sus empleados acerca de sus responsabilidades dentro de la empresa y las consecuencias que tomaría su incumplimiento. Además es crucial para la administración hacer auditorias periódicamente para asegurar que los empleados estén siguiendo los procedimientos ya establecidos en dicha política o para identificar posibles cambios que incurran en la actualización de la política según las necesidades de seguridad de la empresa.

Luego de haber realizado este proyecto y de visualizar todas las *vulnerabilidades* [6] existentes que amenazan a la empresa en la seguridad de la información le presentaré a la compañía una propuesta para la implementación de una nueva política de seguridad de la información. Esta política sin duda será una gran oportunidad y ayuda para la empresa ya que actualmente no cuenta con una *politica de seguridad de la información* [1] lo cual en la actualidad ha puesto a Cabrera Auto en peligro enfrentando fraudes y situaciones de indole legal inecesarias que pudieron haber sido evitadas.

REFERENCIAS

[1] A. Diego. (2016). "Políticas de seguridad", [Online]. *Es.slideshare.net*. Available: http://es.slideshare.net/bellaroagui/politicas-deseguridad-13610538.

[2] U. de México. (2016) *Seguridad Informática Redyseguridad.fi-p.unam.mx*. [Online]. Available: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/AnalisisRiesgos.php.

[3] S. Marinao. (2016). *Plan de Contingencia de Informática de Empresa_X* [Online]. *Monografias.Com*. Available: http://www.monografias.com/trabajos90/seguridad-informatica-empresa/seguridad-informatica-empresa.shtml.

[4] M. Erb. (2016). *1. Definición de Seguridad Informática, Gestión de Riesgo en la Seguridad Informática* [Online]. Available:https://protejete.wordpress.com/gdr_principal/definicion_si/.

[5] E. Gonzalez. (2016). *Génesis 27 ¿Robo De Qué En El Concesionario? R20.rs6.net*. N.p. [Online]. Available: http://files.ctctcdn.com/3103b173301/69d55130-7453-47b2-ad98-4fa5f95620f1.pdf.

[6] P. Antón, *Finding and fixing vulnerabilities in information systems*, Santa Monica, CA: Rand, 2003.

[7] M. Rouse. (2016). *What is business impact analysis (BIA)? - Definition from WhatIs.com* [Online]. *SearchStorage*. Available: http://searchstorage.techtarget.com/definition/business-impact-analysis.

[8] M. Mendoza. (2016). *Business Impact Analysis (BIA) y la importancia de priorizar procesos* [Online]. *Welivesecurity.com*. Available: http://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/.