FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
ESCUELA DE AUDITORÍA

"ANÁLISIS DE LOS RIESGOS DE SEGURIDAD LÓGICA DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN EN EL COMERCIO ELECTRÓNICO (E-COMMERCE) EN CHILE".

Tesis para optar al Título de Contador Público Auditor y al Grado de Licenciado en Sistemas de Información Financiera y Control de Gestión.

Tesista: Randhit Esteban Torres Millahueque
Profesor Guía: Dante Alvarado Estay

VALPARAÍSO, DICIEMBRE 2012

TABLA DE CONTENIDO

RESUMEN

En la actualidad las compañías de todo tipo, pueden ofrecer y vender sus productos por medio de la plataforma del internet, por lo que el comercio electrónico se ha convertido en una ventaja considerable para cualquier empresa que esta insertada en este mundo globalizado. En el poco tiempo ya no será una ventaja debido a que la mayoría de las empresas se están situando a pie con la tecnología y llevara a que en unos años más este medio de comercialización absorba la mayoría de las transacciones comerciales.

Debido a la extensión de este medio se requiere de personas que manejen de forma correcta este asunto, el cual existe poco conocimiento y casi nula legislación al respecto. Siendo que este medio de comercialización entrega una gran cantidad de información en línea, pero también existe un gran riesgo debido a que esta información puede ser adulterada, por accesos no autorizados, realizando fraudes, o alteraciones al sistema lo que llevaría a perder la información. Es por ello que el rol del auditor es fundamental al momento de validar los Estados Financieros, debido a que este trabajara bajo la información entregada por analistas, bancos, gobiernos que trabajan en esta plataforma. Debido a esta tecnología de Información es a la cual se debe auditar, y verificar que la información entregada sea fidedigna, dándole al auditor un mayor riesgo.

Los resultados obtenidos del análisis de los riesgos de seguridad lógica detectados al efectuar una auditoría a los sistemas de información a una entidad que realice sus labores en comercio electrónico en el rubro Bancario, tiene como resultados que el principal riesgo que existe es el factor humano, debido a que los sistemas de seguridad informática implementadas son eficientes, y no se tiene mayor problema, pero las personas que manejan los datos, son las que generan más peligro a la entidad.

CAPITULO I

MARCO TEÓRICO

1. Antecedentes Generales

Las tecnologías de la información han cambiado la forma de operar los negocios y la manera en que las empresas compiten. Las fronteras naturales de una organización cada vez se expanden más y la infraestructura de telecomunicaciones es vital en ese proceso, de modo que surge un nuevo modelo de negocios sustentado en la comercialización de bienes y/o servicios por medios electrónico (Cohen y Asín, 2009, P.60)

Este medio se reconoce como comercio electrónico (e-commerce), la cual se define "como el intercambio telemático de información entre personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes tangibles. Este intercambio de datos o información puede ser "multimedial" o consistir en imágenes, textos y sonidos" (Asociación Iberoamericana de cámaras de comercio). Por otra parte James añade que es el "realizar negocios a través de redes interconectadas utilizando tecnologías basadas en la Web" (O´Brien James, 2001, p.322). Ahora bien, el comercio electrónico se puede entender como cualquier transacción comercial en la cual los participantes interactúan por medios electrónicos dentro de las cuales se encuentran internet, cajeros automáticos, intercambios electrónicos de datos y redes, entre otras.

2. El Comercio Electrónico

2.1. Historia del E-commerce

La historia del e-commerce comienza desde el año 1920 en los Estados Unidos aparecen las primeras ventas por catálogo, impulsado por las grandes tiendas. Este sistema reside en un catálogo con fotos ilustrativas de los productos a ofrecer, esto alcanza una aprobación dentro de los individuos, debido a que se realizaban sus compras desde el hogar. Se alcanza muchas personas que en ese tiempo residían en el campo.

A mediados de 1980, con la televisión, surge una de venta por catálogo, también llamada venta directa. De esta manera, los productos alcanzan mayor realismo, y la dinámica con la cual se exhibe resalta sus particularidades. Esta es concretada por medio de un teléfono y con pagos de tarjetas de crédito.

En la década de los 70, aparecen las originarias relaciones comerciales que se manejaban por medio de una computadora para transmitir datos. Este tipo de intercambio de información, produjo mejoras en el sector privado.

Por otra parte, en el sector público el uso de estas tecnologías para el intercambio de datos. A fines de los años 1970 el Ministerio de Defensa de Estados Unidos inicio un programa de investigación destinado a desarrollar técnicas y tecnologías que permitiesen intercambiar de manera transparente paquetes de información entre diferentes redes de computadoras, el proyecto se llamó “Internetting Project”.

En 1989 aparece un nuevo servicio, la WWW (World Wide Web, Telaraña Global), cuando un grupo de investigadores en Ginebra, Suiza, ideo un método a través del cual empleando la tecnología de Internet enlazaban documentos científicos provenientes de diferentes computadoras, a los que podían integrarse recursos multimedia (texto, gráficos, música, entre otros).

En 1995 el crecimiento de internet como un medio de comunicación es extraordinario, y este evoluciona hasta convertirse en un canal de negocios, en el cual Amazon.com y eBay.com. Lo entendieron así, y estas son las primeras empresas que sacan provecho a este nuevo medio de comunicación, siendo las pioneras en realizar comercio electrónico.

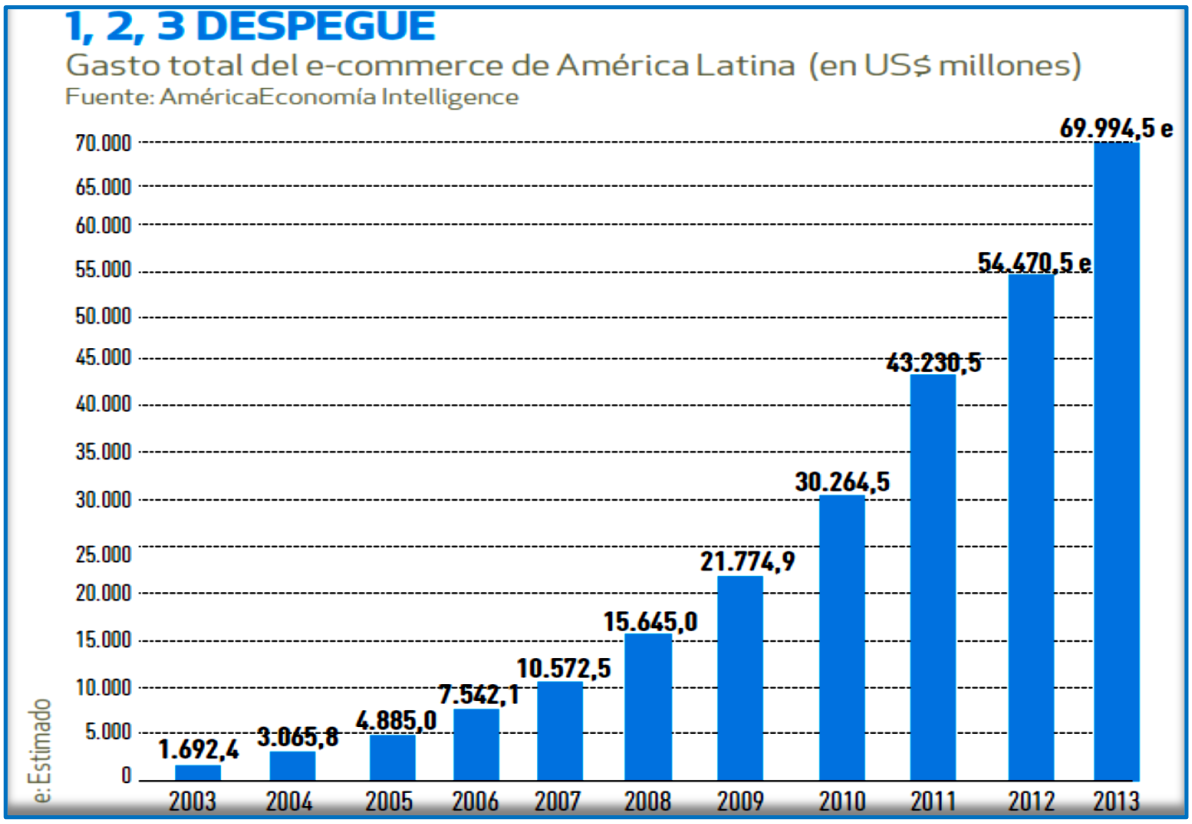
En la actualidad el comercio electrónico a nivel global es uno de los medios más utilizados por las empresas y usuarios para vender sus productos u ofrecer servicios, el cual va en aumento diariamente, además es utilizado por las empresas como un canal para conocer las necesidades de sus clientes e incrementar el rendimiento general de sus recursos.

2.2. E-commerce en Latinoamérica

Latinoamérica ha sido alcanzado por el comercio electrónico, logrando un gran auge, debido a la facilidad en los accesos a internet, existiendo un aumento considerable en el crecimiento del e-commerce en los países como Brasil, México, Argentina y Chile. Este crecimiento se puede apreciar en los gráficos Nº1 de acuerdo al estudio realizado por Visa y América Economía en mayo del año 2012.

Gráfico Nº 1:

"Gasto total del e-commerce de América Latina en los períodos 2003-2013"



Fuente: América Economía Intelligence, 2012.

De acuerdo a este gráfico se puede apreciar que existe un crecimiento de las ventas por e-commerce en más de un 100% desde el año 2009 a lo esperado en el año 2012. Y que el año 2013 se estima una venta de US $ 69.994,5 millones. Con esto se puede apreciar que efectivamente las ventas por comercio electrónico crece a pasos agigantados.

2.3. E-commerce en Chile

En Chile el mundo de los negocios aprovecho la tecnología e incursiono en el universo de internet en el año 1993 para crear un nuevo mercado conocido como comercio electrónico.

Dentro de esta década las empresas telefónicas ingresan al mercado en la cual comienza la era del internet en Chile a partir del año 1996, y las empresas lo aprovechaban para realizar sus contactos con el extranjero. Las empresas comienzan a equipar con

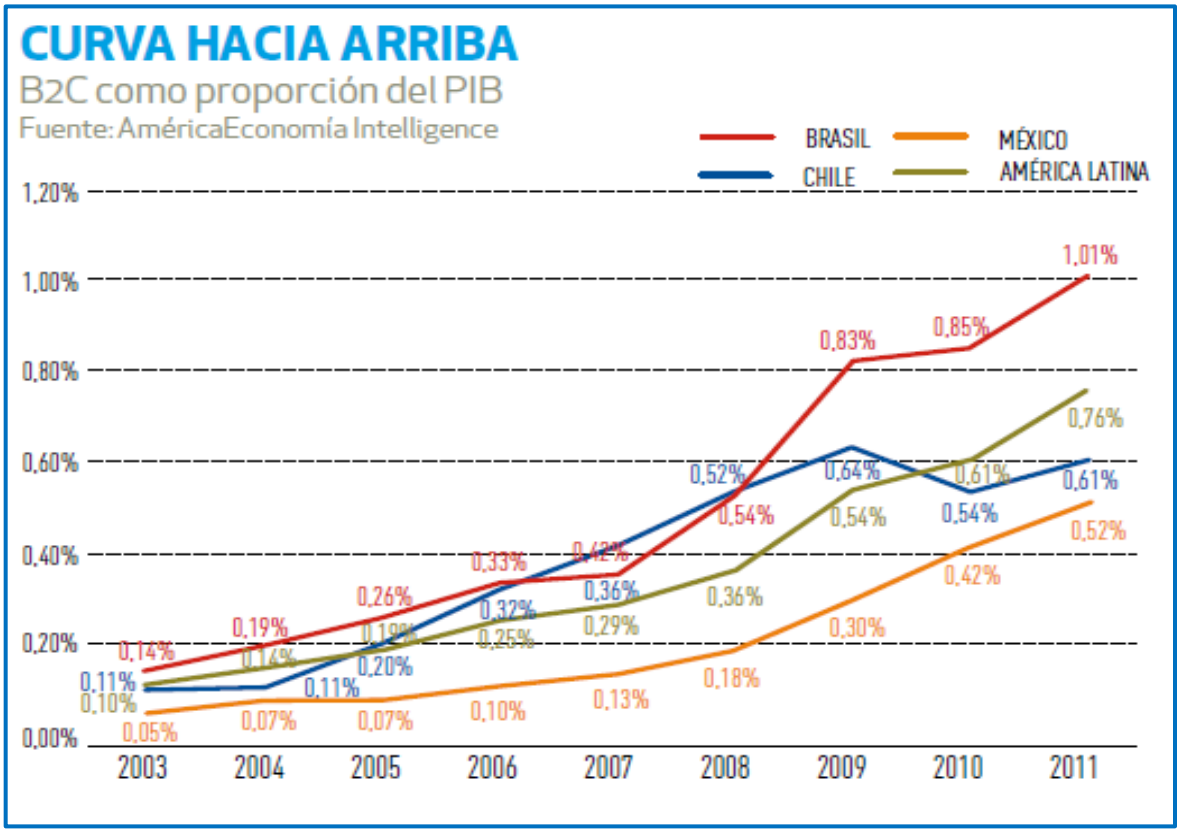
tecnología de punta para estar a la vanguardia y lograr obtener una mayor cantidad de clientes.

Ayuda mucho que el uso de internet en Chile desde el año 2000 hasta el 2010, el 41% de la población chilena utiliza el internet, y el 27% de las empresas lo utilizan para realizar ventas, el 33% tiene publicidad online y el 40% de las facturas que se emiten son electrónicas.

El crecimiento que ha tenido el e-commerce en los últimos años ha sido considerable, en Chile se puede apreciar que el porcentaje del PIB por transacciones por este tipo de comercio ha ido en aumento. En el siguiente gráfico se puede apreciar el aumento del PIB en los países de América Latina, Brasil, México y en especial de Chile.

Gráfico Nº 2:

"B2C como proporción del PIB en los períodos 2003-2011"



Fuente: América Economía Intelligence, 2012.

En este gráfico se aprecia que las ventas realizadas B2C que se refiere a las transacciones efectuadas de Negocio a Consumidor forman parte en Chile el año 2011

del 0,61% del PIB nacional que es una gran evolución relacionado con el 0,11% que correspondía al año 2003.

2.4. Evolución en Chile

Los países latinoamericanos disponen en la actualidad de una poderosa herramienta para acortar la brecha que los separa de la modernidad. Prácticamente todos, independientemente de su tamaño, están avanzando en algunas de las áreas que los especialistas identifican como críticas en su acercamiento a la economía digital que hoy se expande por el mundo.

Chile es una economía de tamaño reducido, con un grado de desarrollo intermedio y desde los años 80, con un importante nivel de integración comercial y financiera al resto del mundo. De mantener su desempeño económico de los últimos quince años, el ingreso per cápita de los chilenos debiera alcanzar el nivel de los países desarrollados en aproximadamente dos décadas.

En materia de comercio electrónico, es posible resumir sus oportunidades de desarrollo en tres determinantes claves: En primer lugar, la existencia de una moderna infraestructura técnica y grandes actores del área de las telecomunicaciones decididos a invertir en el sector.

En segundo lugar, una distribución demográfica de la población chilena propensa a las tecnologías de la información. La pirámide demográfica sigue invertida en los sectores jóvenes, para los cuales el PC es un elemento del paisaje.

Finalmente, se estima que con una adecuada cuota de creatividad y capacidad de gestión, Chile es capaz de ubicarse en el grupo de los países de avanzada en materias de tecnologías de la información e Internet.

Según estudios de la Cámara de Comercio de Santiago, Chile cuenta con un interesante potencial de absorción de nuevas tecnologías de la información (T.I.), ubicándose entre los países de desarrollo tecnológico intermedio, junto con Argentina, Croacia, República Checa, Malasia y Costa Rica, entre un total de 43 países con distintos grados de desarrollo socio-económico y tecnológico. El potencial de absorción de las tecnologías de la información viene dado por un stock importante de equipos computacionales, una amplia infraestructura de telecomunicaciones a costos razonables, y por un porcentaje de la población relevante al sistema de educación-técnico-universitaria que supera al de otros países de desarrollo económico similar.

La extraordinaria capacidad de penetración y crecimiento del comercio electrónico está asociada a su enorme potencial para ahorrar costos al ciclo de negocios y para mejorar la productividad, logística y servicio al cliente.

En el cuadro Nº1 se puede apreciar que Chile se ubica en el quinto país en Latinoamérica que más utiliza este medio de comercialización.

Cuadro Nº1:

"E-consumo en los países de Latinoamérica"

EL E-CONSUMO EN EL MAPA

Países/bloques seleccionados, B2C en millones de US$

Fuente: AméricaEconomía Intelligence

	2005	2006	2007	2008	2009	2010	2011
BRASIL	2.269,9	3.540,5	4.898,7	8.572,6	13.230,4	17.851,4	25.552,8
MÉXICO	567,1	867,6	1.377,0	2.010,0	2.624,9	4.330,5	6.137,1
EL CARIBE	731,0	949,3	1.104,9	1.244,7	1.455,9	1.895,5	2.752,0
ARGENTINA	240,9	378,1	561,5	732,8	875,0	1.797,6	2.695,3
CHILE	242,8	471,8	687,5	919,5	1.027,9	1.141,6	1.489,9
VENEZUELA	253,4	489,6	821,5	787,8	906,1	1.117,8	1.418,4
CENTROAMÉRICA	189,2	359,9	499,0	563,9	637,2	729,6	1.051,0
COLOMBIA	150,3	175,0	201,3	301,9	435,0	606,8	998,0
PERÚ	109,1	145,5	218,2	250,9	276,0	426,9	611,0
OTROS	131,3	164,8	203,0	260,9	306,5	366,9	525,0
LATAM + EL CARIBE	4.885,0	7.542,1	10.572,5	15.645,0	21.774,9	30.264,5	43.230,5

Fuente: América Economía Intelligence, 2012.

Se puede apreciar que en Chile se encuentra en el quinto lugar de Latinoamérica y que su crecimiento ha sido constante en Latinoamérica, entre las transacciones de B2C de Negocio a consumidor.

2.5. Agrupación del Negocio

EL comercio electrónico se puede agrupar de acuerdo a los tipos de entes que se relacionan entre cada transacción, en la presente se mencionan las más utilizadas y se determinan de la siguiente manera: Negocio a Negocio (B2B), Negocio a consumidor (B2C) y Negocio a Gobierno (B2G). Para esto se debe definir que es cada una de estas:

2.5.1. Negocio a Negocio (B2B)

Se refiere a una compañía que utiliza una red para hacer órdenes de compra a sus proveedores, recibir facturas y realizar los pagos correspondientes. Este tipo de operación funciona desde que existe la tecnología EDI (Intercambio electrónico de datos) para redes privadas o redes de valor agregado (VAN, value added network). En esta modalidad se considera la gama de relaciones comerciales que ocurren entre dos organizaciones. Esta modalidad representa el 80% del e-commerce de los últimos años. (Cohen y Asín, 2009)

2.5.2. Negocio a Consumidor (B2C)

Se puede comparar con la venta al detalle pero de manera electrónica. Esta categoría tiene gran aceptación y crece sobremanera gracias al WWW, ya que en internet existen diversos centros comerciales (malls) que ofrecen toda clase de bienes de consumo, desde pasteles y vinos hasta computadoras. Entre los precursores hay que mencionar a Amazon (www.amazon.com), empresa que inició con la venta de libros a través de internet y ha expandido su línea de productos. (Cohen y Asín, 2009)

2.5.3. Negocio a Gobierno (B2G)

Consiste optimizar los procesos de negociación entre empresas y el gobierno a través del uso de internet. Se aplica a sitios o portales especializados en relación con la administración pública. (Cohen y Asín, 2009)

2.6. Ventajas y Desventajas del Comercio Electrónico

En el comercio electrónico como en todo modelo de comercialización se logra encontrar tanto ventajas como desventajas, las cuales se debe analizar desde el punto de vista del usuario y de la empresa.

Cuadro N°2:

"Ventajas y desventajas del usuario al realizar las transacciones por internet"

Ventajas Usuarios	Desventajas Usuarios
Comodidad en la adquisición del producto	Se pierde cercanía con el vendedor del producto ante una eventual consulta
Encontrar un producto a menor costo	Perdida de la visualización del producto físico
Realizar una comparación inmediata en otros locales que ofrezcan el mismo producto	Al momento del pago en línea no sea seguro la transacción

Fuente: Elaboración propia a partir de trabajo de comercio electrónicos

Cuadro Nº3:

"Ventajas y desventajas de la empresa al realizar las transacciones por internet"

Ventajas Empresa	Desventajas Empresa
Elimina días muertos por cualquier circunstancia	Existe una menor comunicación con el cliente
Elimina las pérdidas de mercancía robada	Hackers y Crackers
Elimina obligaciones con trabajadores	Al momento del pago del cliente este pueda realizar una transacción fraudulenta

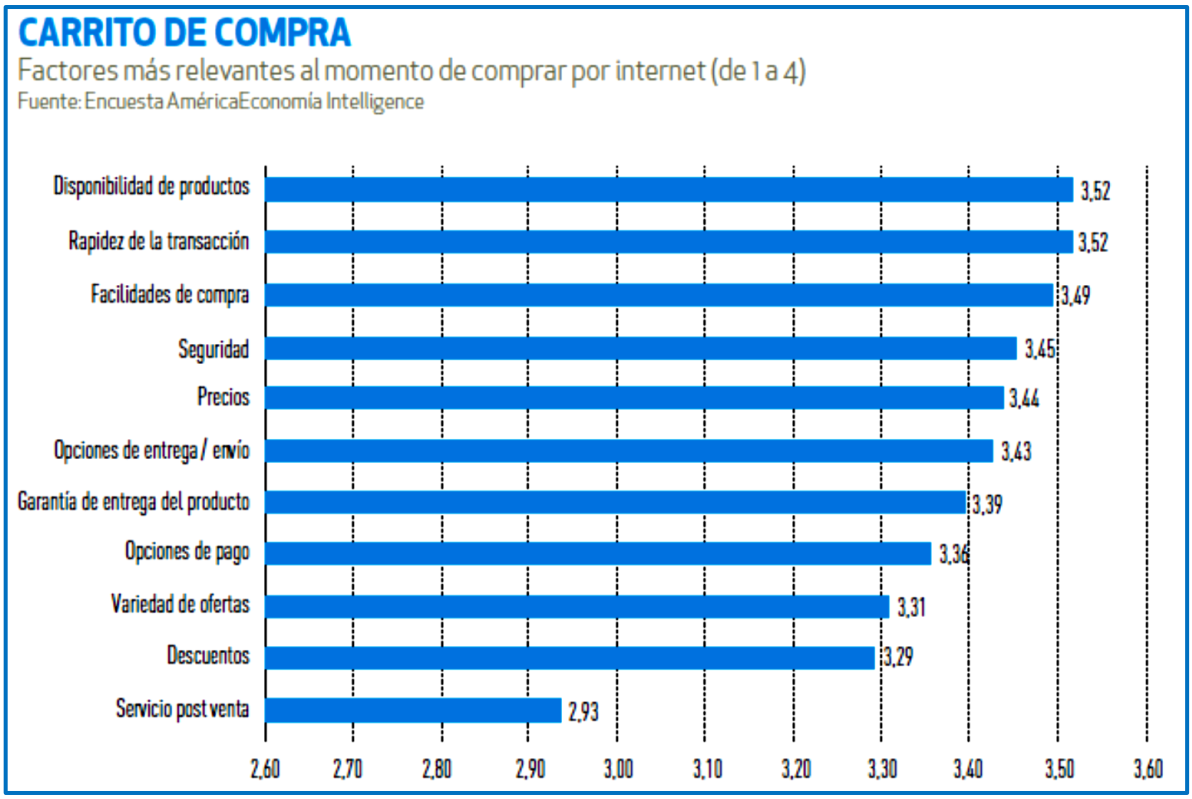
Fuente: Elaboración propia a partir de trabajo de comercio electrónicos

Se puede apreciar las ventajas y desventajas tanto para el usuario como para la empresa al realizar sus operaciones desde la plataforma del comercio electrónico, y lo más valorable para los usuarios es la comodidad de la compra del producto, y para la empresa es la eliminación de días muertos para cualquier circunstancia, estado en línea las 24 horas del día, que para cualquier empresa es excelente.

Además se agrega un gráfico con respecto a los factores más relevantes que toman en consideración los clientes al realizar sus transacciones por internet.

Gráfico Nº 3:

"Factores más relevantes al momento de comprar por internet"



Fuente: Encuesta América Economía Intelligence, 2012.

En el gráfico Nº3 se analiza que al momento de realizar la compra lo que más valora los clientes es la disponibilidad del producto y la rapidez de la transacción, en la cual se puede analizar que se busca obtener un producto de la manera más fácil y rápida.

Se puede concluir de acuerdo a los resultados en los cuadros Nº2 y 3 y gráfico Nº3 que el usuario de comercio electrónico busca realizar transacciones comerciales de una manera más sencilla, sin tener que realizar la fila para el pago de un producto, y tener que ir a un local en busca de un producto el cual puede que no se encuentre en ese momento. Además de la variedad de ofertas debido a que no existe un vendedor el cual ganara una comisión por esa venta, y la cual directamente rebaja el valor del producto a comprar, y esta forma de transacción permite comparar en línea los productos de una entidad con

respecto a su competencia lo cual le da una gran ventaja al usuario al momento de decidir la compra de un producto por este medio.

Pero como toda transacción en la cual está de por medio el dinero, siempre habrá maneras de burlar o de querer realizar transacciones no adecuadas o ilícitas en la cual busquen el perjuicio de alguna de las partes tanto cliente como entidad que proporciona el producto. Por esto en la presente trabajo se analiza el sistema bancario y las medidas que este utiliza para evitar todo los ataques a través de internet.

3. El sistema bancario

En el presente trabajo se decide utilizar el sistema bancario para tomarlo como ejemplo para el estudio.

Se debe entender por un banco como una entidad financiera que tiene el propósito de captar recursos por medio de depósitos, y proporcionar dinero a sus clientes, prestando a su vez variados servicios financieros. Por lo tanto el sistema bancario es el conjunto de instituciones que proporcionan el servicio de un banco.

Como se menciona anteriormente el comercio electrónico corresponde a las transacciones que se realizan por medios electrónicos y tiene por nombre e-commerce, pero en el sistema bancario adquiere otro nombre que es e-banking que es la banca virtual, banca en línea en la cual se tiene acceso por medio de internet o telefónicamente.

3.1. E-banking

El e-banking es una rama del comercio electrónico pero está relacionado directamente con las entidades bancarias. Se puede definir e-banking como el conjunto de las actividades bancarias realizadas con empleo de las tecnologías útiles para una ejecución más eficaz y satisfactoria para las partes directamente implicadas (banco-cliente), en cualquiera de las formas en las que se puede establecer la comunicación, el intercambio de información, el contraste de ideas, propósitos, decisiones y cualquier otra acción sobre temas bancarios o financieros que interesen al cliente y a la entidad bancaria con la que se relaciona. (BancayFinanzas, 2012)

Para esto se debe analizar la evolución que este medio ha tenido a través de los siguientes recuadros y gráficos.

En el cuadro Nº 4 se puede apreciar la evolución de las operaciones bancarias desde el año 2000 hasta el año 2011, de acuerdo a las estadísticas de la SBIF (Superintendencia de Bancos e Instituciones Financieras Chile).

Cuadro Nº4:

"Evolución de operaciones bancarias desde el año 2000 hasta el 2011"

Superintendencia de Bancos e Instituciones Financieras Chile

EVOLUCIÓN DE OPERACIONES BANCARIAS

PERÍODO	CLIENTES CONECTADOS (2)	VISITAS (3)	TRANSACCIONES (7) Saldos (4)	Transferencias (5)	Información (6)	TOTAL (4+5+6)
JUN-2000	219.619	1.753.310	2.892.897	541.282	88.950	3.523.129
DIC-2000	285.800	4.397.819	5.261.183	786.920	779.548	6.827.651
JUN-2001	411.374	4.928.186	6.869.741	2.559.857	867.264	10.296.862
DIC-2001	460.038	5.602.056	10.006.309	1.173.426	2.017.447	13.197.182
JUN-2002	591.356	5.482.679	10.924.443	1.624.842	1.634.571	14.183.856
DIC-2002	687.504	7.355.756	16.021.068	2.239.129	2.347.482	20.607.679
JUN-2003	600.888	8.743.143	17.348.171	2.367.442	10.581.232	30.296.845
DIC-2003	707.905	6.951.115	19.060.380	3.310.033	11.274.947	33.645.360
JUN-2004	776.691	12.324.977	21.729.655	3.555.393	11.175.915	36.460.963
DIC-2004	870.760	13.927.401	25.569.249	4.203.873	12.451.158	42.224.280
JUN-2005	923.327	16.191.733	29.167.428	4.197.668	17.266.466	50.631.562
DIC-2005	1.097.630	20.711.598	36.114.820	5.300.840	24.966.581	66.382.241
JUN-2006	1.225.059	21.661.315	41.579.584	6.840.784	25.406.861	73.827.229
DIC-2006	1.294.659	28.173.928	42.859.336	7.856.382	16.871.144	67.586.862
JUN-2007	1.464.311	34.724.559	47.790.897	8.066.890	21.106.900	76.964.687
DIC-2007	1.617.907	38.110.601	57.836.896	9.771.002	25.966.828	93.574.726
JUN-2008	1.810.535	41.764.144	58.085.388	10.279.129	36.840.326	105.204.843
DIC-2008	1.939.128	47.298.593	66.621.296	14.214.752	53.020.971	133.857.019
JUN-2009	2.269.605	50.760.601	73.207.138	14.387.280	48.579.772	136.174.190
DIC-2009	2.439.818	57.973.239	84.535.212	18.342.190	48.243.142	151.120.544
JUN-2010	2.779.222	58.861.233	69.038.591	18.624.323	57.814.970	145.477.884
DIC-2010	3.338.225	96.081.929	75.418.021	13.402.081	59.184.146	148.004.248
JUN-2011	3.458.270	95.358.241	74.445.575	13.523.927	63.926.737	151.896.239
DIC-2011	3.748.909	105.163.361	74.307.194	17.232.653	77.358.694	168.898.541

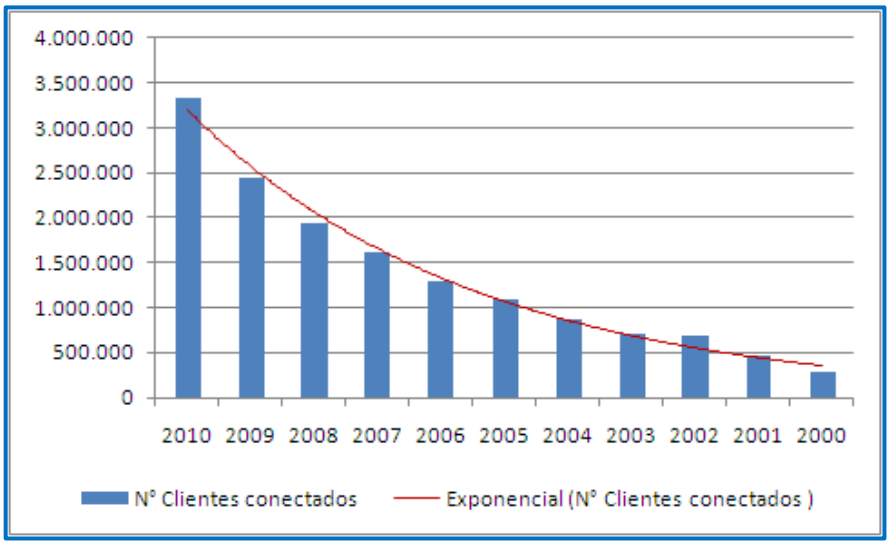
Fuente: SBIF, 2012.

En el cuadro se puede apreciar (2) número de clientes con clave de acceso al sito privado del banco y que realizan transacciones durante el período de consulta. (3) A partir de la incorporación en Julio 2010, del archivo P41, documento que recoge la información asociada a la web, se estableció que "una visita corresponde a la exploración del sitio Web durante un periodo de tiempo ininterrumpido, con independencia del número de páginas que se recorra durante la navegación". Hasta antes de esta fecha, se entendía

como vista el acceso a la página principal del sitio web. (4) Solicitud de saldos, cartolas o estados de cuentas de productos, tales como, cuentas corrientes, líneas de sobregiro y tarjetas de crédito. (5) transferencias entre cuentas. (6) solicitudes de información diferentes de saldos y cartolas (índices financieros, consultas vía e-mail, consultas legales, publicidad, etc.) y otras operaciones (bloqueos, órdenes de no pago, envíos de e-mails, etc.). (7) número de transacciones.

Gráfico Nº4:

"Números de clientes conectados desde el año 2000 hasta el 2010"



Fuente: ebanking.cl de acuerdo a estadística de la SBIF, 2012.

De la manera como se puede apreciar la cantidad de clientes conectados va en aumento, también se puede ver el número de clientes conectados por cada banco en el cuadro Nº5.

Cuadro Nº5:

"Evolución del número de clientes con clave de acceso que ingresaron al sitio web del banco en cada período, desde diciembre 2006 hasta diciembre 2011"

Superintendencia de Bancos e Instituciones Financieras Chile

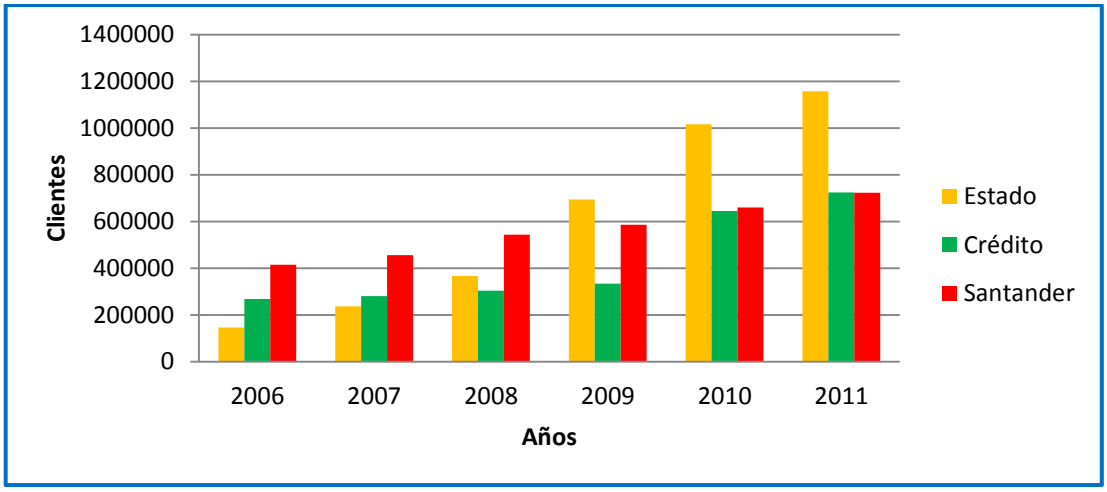
EVOLUCIÓN DEL NÚMERO DE CLIENTES CON CLAVE DE ACCESO QUE INGRESARON AL SITIO WEB PRIVADO DEL BANCO EN CADA PERIODO
(Datos correspondientes al mes informado)

BANCO	DIC-06	JUN-07	DIC-07	JUN-08	DIC-08	JUN-09	DIC-09	JUN-10	DIC-10	JUN-2011	DIC-11
Chile	238.792	260.098	288.681	335.426	362.136	379.401	388.101	400.235	509.837	532.036	540.420
Internacional	972	990	989	987	1.034	1.145	1.260	1.359	2.157	2.314	2.267
Estado	145.190	196.104	235.898	359.105	366.825	587.811	693.427	916.378	1.015.467	1.042.803	1.156.595
Scotiabank	31.770	33.794	37.683	42.254	46.398	50.095	78.410	77.545	79.807	83.334	90.015
Crédito	242.641	268.172	280.324	286.341	303.566	311.128	333.379	363.295	644.055	670.154	723.433
Do Brasil	-	-	-	-	-	-	-	6	6	8	16
Corpbanca	32.173	37.821	41.456	49.027	55.383	59.888	64.161	68.309	72.135	74.187	76.501
Bice	23.236	23.109	26.489	27.835	29.194	31.162	32.727	34.925	44.841	46.315	46.925
HSBC Bank (Chile)	-	-	-	-	-	-	-	101	940	1.097	1.464
Citibank	55.274	54.186	54.186	-	-	-	-	-	-	-	-
Santander	361.893	414.340	455.131	493.799	543.179	581.959	584.969	624.129	659.031	690.321	722.575
ITAU CHILE	52.081	56.620	61.840	67.318	63.180	65.802	81.043	85.090	81.283	55.748	94.920
The Royal Bank of Scotland	3.644	3.714	3.169	3.153	2.114	1.795	1.381	1.200	44	8	-
Security	17.163	21.504	25.165	28.597	30.594	31.536	32.666	33.023	36.569	37.462	39.307
Banco Falabella	4.681	5.818	9.327	12.876	15.049	21.545	23.337	30.451	57.546	72.141	93.732
Banco Ripley	-	407	1.221	1.832	15.120	16.935	22.862	25.766	21.267	23.136	19.457
Rabobank Chile	1.129	1.202	1.204	798	658	521	-	2.370	349	436	399
Banco Consorcio	527	-	868	658	535	419	384	285	71	110	38
Penta	952	1.305	1.303	1.261	1.046	1.179	1.107	1.702	1.080	1.106	904
Banco Paris	2.809	2.857	4.161	5.157	6.306	6.488	6.583	6.654	2.219	3.146	3.067
BBVA	51.761	56.016	60.974	64.863	67.908	79.373	94.021	106.399	109.521	122.404	136.871
Desarrollo	27.971	26.254	27.838	29.248	28.903	27.896	-	-	-	-	-
The Bank of Tokyo-Mitsubishi	-	-	-	-	-	-	-	-	-	4	3
SISTEMA	**1.294.659**	**1.464.311**	**1.617.907**	**1.810.535**	**1.939.128**	**2.256.078**	**2.439.818**	**2.779.222**	**3.338.225**	**3.458.270**	**3.748.909**

Fuente: SBIF, 2012.

Gráfico Nº5:

"Evolución de números de clientes con clave de acceso que ingresaron al sitio web privado de los 3 bancos con mayor cantidad de clientes con clave de acceso, de acuerdo a los meses informados en diciembre, desde el 2006 hasta el 2010"



Fuente: Elaboración propia de acuerdo a estadísticas de la SBIF, 2012.

La ventaja que se puede deducir que el Banco Estado tiene su aumento debido a la cantidad de cuentas Rut que este posee, debido a que es muy fácil de obtener esta cuenta. Y en el cuadro Nº6 se puede apreciar el detalle de transferencias efectuadas a través de internet.

Cuadro Nº6:

"Detalle de transferencias bancarias efectuadas a través de internet, que incluyen el 3er y 4to trimestre 2011"

DETALLE DE TRANSFERENCIAS BANCARIAS EFECTUADAS A TRAVÉS DE INTERNET

NUMERO DE OPERACIONES					
TIPO DE TRANSFERENCIAS	3er Trimestre 2011 (Acumulado para el periodo)		4to Trimestre 2011 (Acumulado para el periodo)		TOTAL OPERACIONES DEL SEMESTRE
	Empresas	Personas	Empresas	Personas	
Transferencias de fondos entre cuentas del mismo banco y del mismo RUT	186.523	2.472.071	189.000	2.722.524	5.570.118
Transferencias de fondos entre cuentas del mismo banco y distinto RUT	1.236.248	6.581.564	1.414.055	7.178.851	16.410.718
Transferencias de fondos a cuentas de otro banco y del mismo RUT	223.437	2.446.959	246.873	2.619.972	5.537.241
Transferencias de fondos a cuentas de otro banco y distinto RUT	2.234.964	10.660.088	2.531.973	11.877.779	27.304.804
Pago electrónico de cuentas de servicios	22.445	4.982.721	25.142	4.505.984	9.536.292
Pago con cargo a productos bancarios desde otros portales (Servipag, Previred, etc.)	432.386	4.783.571	448.190	4.983.262	10.647.409
Otros pagos (recarga de celulares, tarjeta BIP, etc.)	11.815	1.385.885	13.136	1.220.008	2.630.844
Pago de créditos asociados a líneas	123.345	3.770.954	131.977	3.973.160	7.999.436
Pago de otros créditos	18.881	2.085.533	20.472	2.224.412	4.349.298
TOTAL TRANSFERENCIAS	4.490.044	39.169.346	5.020.818	41.305.952	89.986.160

MONTO DE LAS TRANSFERENCIAS MM($)					
PERÍODO	Traspasos a cuentas del mismo banco y de otros bancos		Pagos asocidos a créditos y servicios		TOTAL OPERACIONES DEL SEMESTRE (MM$)
	Empresas	Personas	Empresas	Personas	
JUL-2011	33.146.321	1.452.904	1.387.047	1.481.340	37.467.612
AGO-2011	41.765.423	1.537.206	1.607.385	1.631.260	46.541.274
SEP-2011	34.392.047	1.501.895	1.786.057	1.586.255	39.266.254
OCT-2011	34.279.578	1.542.679	1.793.653	1.838.193	39.454.103
NOV-2011	34.783.160	1.599.339	1.796.592	1.732.245	39.911.336
DIC-2011	37.735.743	1.798.475	2.175.764	2.040.339	43.750.322
TOTAL DEL PERIODO	216.102.271	9.432.499	10.546.499	10.309.633	246.390.901

Fuente: SBIF, 2012.

De Acuerdo a los exhibidos cuadros y gráficos se puede concluir que cada año los clientes están realizando sus transacciones por medio del internet, debido a la comodidad que este medio entrega y la rapidez de la transacción. Además de apreciar la cantidad de nuevos clientes que se ha obtenido como en el caso del Banco Estado por medio de la cuenta Rut, debido a que no se necesita mayor documentación para obtener una cuenta corriente y esto va de la mano al aumento considerable en los clientes conectados por medio de internet. Pero a su vez representa un riesgo en el cual se apreciara más adelante.

3.2. Información Obtenida por bancos

Como consecuencia de la actividad que desempeña, la institución bancaria dispone de variada información sobre la situación económica de cada cliente. Es por eso que el banco puede adquirir información sobre sus:

a) Datos personales
b) Datos profesionales
c) Datos de servicios contratados
d) Datos de las transacciones realizadas y sus respectivos saldos
e) Datos de su vivienda
f) Datos de inversiones
g) Datos de sus gustos personales, entre otras.

El nivel de información de datos sensible (información personal de un cliente) que maneja una entidad financiera es enorme, por ello la importancia que la información se encuentre resguardada y cuente con las medidas de seguridad necesarias.

Los principales riesgos que se encuentran en la información es:

a) Difusión no autorizada a lugares que no corresponden
b) Confidencialidad es el grado de confianza que adquiere el banco de la información del cliente y no respete la institución bancaria.
c) Obtener información errónea manipulada indebidamente que sea cedidos a terceros.

Debido a este riesgo que mantiene el usuario es necesario determinar las políticas de seguridad que ofrecen cada banco y que están reguladas por la Superintendencia de Bancos e Instituciones Financieras Chile.

3.2. Políticas de seguridad

Las políticas de seguridad de las instituciones financieras se encuentran en cada una de las páginas web de cada banco, en la cual debe adquirir un compromiso tanto el cliente como la institución.

3.2.1. Recomendaciones al Cliente

a) Ingresar al respectivo banco evitando estar en cibercafés o lugares públicos.
b) Observar que la URL esté bien escrita.
c) Nunca utilizar un links para acceder a la página del banco.

d) Nunca aceptar a entrar al sitio por medio de correos electrónicos.
e) Cambiar frecuentemente la clave
f) Instalación de antivirus en el caso de computador portátil.

3.2.2. Políticas del banco

a) Contar con un proceso de identificación y autenticación confiable.
b) Manejar la información de los clientes en base de datos encriptados y custodiadas.
c) Bloqueo de claves ingresadas erróneamente más de 3 veces.
d) Encriptación, la comunicación entre el equipo portátil y el banco debe estar libre de cualquier intromisión. Esto se logra encriptado los datos mientras viajan por internet, quedando ilegibles para quien intente interceptarlos y leerlos.
e) Servidores certificados, todos los bancos deben adquirir estos certificados para actuar como tal.
f) Contar con procesos rápidos tanto informativos como bloqueos de tarjetas.
g) Monitorear permanentemente la actividad de las Tarjetas de Crédito para identificar a tiempo posibles fraudes o clonaciones.
h) El Banco jamás compartirá estos datos con empresas u organizaciones sin tu consentimiento (a excepción que la ley o el gobierno lo requiera.
i) Cualquier dato demográfico entregado por el Banco siempre representará información agregada y nunca en relación a un cliente específico.(Banco Internacional, 2012)

Es necesario mencionar que los bancos son instituciones que están en constante supervisión, y que además por el nivel de información que manejan, todos los sitios que estos mantengan por internet deben estar certificados por sellos de firma electrónica.

4. Certificados de sitios Web

Un certificado de sitio web es una tecnología que permite proteger la información confidencial de sus clientes, por ejemplo Rut, password o número de tarjeta de crédito. De otra forma estos datos, de gran valor, pueden ser mal usados causando daño tanto a sus clientes como al patrimonio de la empresa. (Certificado de firma electrónica, Acepta.com)
Los certificados de sitio web permiten asegurar a los clientes que el servicio es realmente administrado por la entidad y no se trata de una página simulada. Además, se habilitan comunicaciones privadas en Internet gracias a que se establece una comunicación

encriptado (cifrado) utilizando llaves de 40, 56 o hasta 128 bits, lo que es un indicador del nivel de seguridad implementado.
Internacionalmente se conoce el certificado de sitios web llamado “Web Trust” y que opera en el extranjero.

4.1. Web Trust

Es el sello de confianza, calidad y seguridad que se concede a la “página Web” de la empresa que, previamente ha obtenido un Informe Favorable de Auditoría Independiente, por una Firma de Auditoría Habilitada para la Prestación de Servicios Web Trust al cumplir, durante un cierto periodo de tiempo, los Criterios y Principios Web Trust, establecidos por las entidades promotoras y licenciatarias del sello. (Web Trust, 2011).

O sea es un servicio proporcionado por Contables colegiados (CPA, Certified Public Accountant) para determinar si un servidor Web sigue ciertos principios exigidos. Los servidores Web que cumplan estos requisitos reciben un logotipo y diploma que pueden exhibir en su página web y que tienen una validez de 90 días por lo que deben pasar frecuentes auditorias. Solo los CPA que sean miembros de AICPA (Instituto Americano de Contadores Públicos Certificados), hayan cursado un seminario especial, tengan una licencia y permitan inspecciones de calidad pueden proporcionar este servicio. El logotipo que podrán exhibir es proporcionado por VeriSign, que es la empresa que proporciona el soporte técnico. (Web Trust, 2011)

El pedido de este sello de seguridad en el extranjero cada vez es más utilizado por las empresas sobre todo en España, la cual ofrece una gran ventaja para las empresas que operan sus comercialización por internet por que entrega esa seguridad al usuario de que la pagina visitada donde se realiza la compra entrega confianza y logra que sus productos sean elegidos por sobre páginas que en este caso no obtenga este sello de seguridad, creciendo en la venta de sus bienes o servicios. En Chile existe el sello secure site seal que traducido es sello de sitio seguro que tiene la misma función que cumple el Web Trust en el extranjero que es entregar confianza a los usuarios que utilizan dicha página. El sello se obtiene demostrando que se es una empresa confiable y cancelando un “X” monto de dinero. Es necesario mencionar que en Chile todos los bancos se deben encontrar acreditados con estos sellos, porque la normativa se los exige por ser entidades

que manejan información muy sensible y relevante, por lo tanto todos los bancos deben tener el sello VeriSign.

4.2. Firma Electrónica

La Firma Electrónica nace en Chile de la Ley Sobre Documentos Electrónicos, Firma Electrónica Y Servicios De Certificación De Dicha Firma Nº 19.799 del 12 de Abril de 2002.

Para esto se debe entender por:

a) Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;
b) Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica;
c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas;
d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior;
e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción.
f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;
g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.
h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica. (Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma Nº19.799)

Este certificado proporciona mayor seguridad garantizada, el certificado de firma electrónica avanzada permite firmar documentos de acuerdo a la ley 19.799. Este certificado contiene información que identifica al emisor y le permite firmar digitalmente documentos, de modo que el destinatario esté seguro del origen del mensaje o archivo.

Los Certificados de Firma Electrónica Avanzada, además de contar con las características básicas de un certificado digital, cumplen con los requisitos establecidos por la ley 19.799 en materia de verificación de identidad. Están acreditados por la Subsecretaría de Economía del gobierno de Chile, por lo que posibilitan que electrónicamente se autentique la identidad del solicitante, se asegure la integridad de los documentos firmados y se evite la repudiación de los mismos. Toda firma que pueda ser validada con este tipo de certificados obtiene el respaldo de plena prueba legal para los documentos electrónicos. Las personas pueden firmar electrónicamente documentos tanto privados como públicos.

La firma electrónica avanzada es el instrumento que permite dotar de seguridad jurídica a la nueva economía, debido a que la Ley reconoce pleno valor jurídico a las actuaciones realizadas bajo el soporte electrónico. Los certificados de Firma Electrónica Avanzada requieren de un dispositivo criptográfico FIPS140-2 para poder ser generados y utilizados. (Firma electrónica avanzada, CertiSur).

Hace posible la verificación de la afirmación de alguien que dice tener el derecho de utilizar una clave dada. Con esto se asegura a los socios comerciales, amigos y a los servicios en línea que la información electrónica enviada es auténtica, proporcionando una solución de seguridad más completa, asegurando la identidad de todas las partes involucradas en una transacción, las cuales se pueden comparar con las licencias de conducir, pasaportes y tarjetas de socios.

En resumen Chile se tuvo que adoptar y aprobar una ley que tuviese relación directa con la seguridad lógica que se debe entregar a una empresa o a un usuario que navega por la web para que al realizar sus operaciones comerciales no sufra algún fraude a través de phishing, robo de identidad u otros esquemas delictivos que pudiesen llevar al usuario a tener sospecha de usar este medio de comercialización. Como se mencionó anteriormente estos certificados de firma electrónica simple, firma electrónica avanzada y sitios web les brinda a los usuarios, tanto empresa como cliente individuales, como particulares, una seguridad y confianza para que puedan seguir usando estos medios cómodamente sin mayor preocupación e inseguridad debido a que este es el instrumento que permite dotar de seguridad jurídica a este tipo de transacciones, porque la ley reconoce de pleno valor jurídico a las actuaciones realizadas bajo este soporte electrónico.

5. La Auditoría y el Comercio Electrónico

Con el arribo de esta nueva manera de operar que es el comercio electrónico ha dificultado al auditor. Debido a que todas las transacciones que se realicen por internet llevan un riesgo extra que una transacción que no fuese por este medio, porque el auditor se encuentra estructurado a que las auditorías realizadas a las transacciones debe existir documentación como la factura, boletas, entre otros. ¿Pero qué ocurre cuando estos documentos no existen? Muchas de las transacciones son electrónicas y el auditor debe dar fe de que efectivamente esas transacciones son correctas. Por eso se debe determinar un buen esquema de trabajo para comenzar a trabajar en esta área.

La auditoría en el comercio electrónico se rige por la Declaración de Prácticas de Auditoría Internacional (IAPS) 1013, (Internacionales de Auditoría, Declaración de prácticas de 1013) “Comercio Electrónico- Efecto en la auditoría de estados financieros”, estas son entendidas en el contexto del “Prólogo a las Normas Internacionales de Control de Calidad, Auditoría, Revisión, Otros Aseguramiento y Servicios Conexos”, que establece la aplicación y autoridad de IAPS.

Esta declaración establece lo siguiente:

A) Orientación sobre la aplicación de las NIA cuando una entidad utiliza un público de red tales como Internet, para el comercio electrónico, y
B) Los materiales para aumentar la conciencia de los problemas financieros de auditoría declaración en esta dinámica zona.

En esta sección se verá las prácticas más relevantes que debe utilizar el auditor y que están contenidas en la “Declaración de Prácticas de Auditoría Internacional”.

5.1. Prácticas de Auditoría

En esta declaración se puede encontrar el ISA 400, “Evaluación de riesgos y control interno” y “La comprensión de la entidad y su entorno y evaluación de los riesgos de errores materiales” e ISA 330, “Procedimientos del auditor en respuesta a los riesgos evaluados”. Se debe estar al tanto de:

5.1.1. Conocimiento y habilidades

El nivel de habilidades y conocimientos necesarios para comprender el efecto del e-commerce sobre la auditoría variará con la complejidad de la entidad,

actividades de comercio electrónico. El auditor considera si el personal asignado a la contratación es el apropiado para TI (tecnología de información) y de negocio en Internet conocimiento para realizar la auditoría. Cuando el comercio electrónico tiene un efecto significativo en los negocios de la entidad, los niveles adecuados de ambas tecnologías de la información y conocimiento del negocio de internet puede ser necesario para:

- Entender, en la medida en que puedan afectar los estados financieros:
  - La entidad de comercio electrónico y estrategia de las actividades;
  - La tecnología utilizada para facilitar la entidad, las actividades de comercio electrónico y las habilidades en TI y el conocimiento de personal de la entidad, y
  - Los riesgos de la entidad de utilizar el comercio electrónico y el enfoque de la entidad a la gestión de los riesgos, en particular la adecuación del sistema de control interno, incluida la seguridad la infraestructura y los controles relacionados, ya que afecta a los estados financieros en la presentación del informes;
- Determinar la naturaleza, oportunidad y alcance de los procedimientos de auditoría y evaluar las pruebas de auditoría, y
- Considerar el efecto de la dependencia de la entidad sobre el comercio actividades de su capacidad para continuar como empresa en marcha.

En el caso que el auditor no cumpla con estas exigencias para auditar una entidad que trabaja en e-commerce puede recurrir al trabajo de un experto en sistemas de información y reduciendo el riesgo que este podría correr, y dicho trabajo realizado por el experto se utiliza como una evidencia apropiada.

5.1.2. Conocimiento del Negocio

El conocimiento del auditor de la empresa es fundamental para evaluar la importancia del e-commerce para negocios de las actividades de la entidad y cualquier efecto en el riesgo de la auditoría. El auditor considera los cambios en los negocios de la entidad medio ambiente imputables al comercio electrónico, como riesgos identificando la medida en que afectan a los estados financieros. Aunque el auditor obtiene mucha información de las

investigaciones de los responsables financieros presentación de informes, hacer las investigaciones del personal directamente involucrado con la entidad, actividades de comercio electrónico, como el director de informática o equivalente, puede también ser útil. En la obtención o actualización de conocimientos de la entidad, negocio, el auditor considera, en la medida en que afecten los estados financieros:

- La entidad de las actividades comerciales y la industria.
- La entidad de comercio electrónico, estrategia.
- El alcance de la entidad, las actividades de comercio electrónico y
- Los acuerdos de subcontratación de la entidad.

En este caso se verá:

- La entidad de comercio electrónico, estrategia: incluye la forma en que lo utiliza para comercio electrónico y su evaluación de los niveles de riesgo aceptables, que pueden afectar a la seguridad de los registros financieros y de la integridad y fiabilidad de la información financiera producida.
- El alcance de la entidad, las actividades de comercio electrónico: esto se debe al grado de utilización del comercio electrónico que afecta a la naturaleza de los riesgos que se abordarán en la entidad.

5.1.3. Identificación del Riesgo

Gestión de negocios se enfrenta a muchos riesgos relacionados con la entidad de e-commerce actividades, incluyendo:

- La pérdida de la integridad de la transacción, cuyos efectos pueden ser agravados por la falta de una pista de auditoría adecuada, ya sea en papel o en formato electrónico;
- Generalizando el comercio electrónico los riesgos de seguridad, incluyendo ataques de virus y la potencial de la entidad de sufrir el fraude por los clientes, empleados y otros a través de accesos no autorizados; en la cual se enfoca este trabajo.
- Las políticas contables inadecuados relacionados como por ejemplo, la capitalización de gastos como los costes de desarrollo de sitios web, la incomprensión de complejos arreglos contractuales, la transferencia de

riesgos de título, la traducción de moneda extranjera, los subsidios para las garantías o devoluciones, y los ingresos cuestiones de reconocimiento, tales como:

- Si la entidad está actuando como director o agente y si las ventas son brutas o la comisión sólo se reconoce.
- Si otras entidades se les da espacio publicitario en la página web de la entidad, cómo los ingresos se determinaran y si se instalaron.

- El incumplimiento de la fiscalía y otros instrumentos jurídicos y normativos necesarios, sobre todo cuando la transacción por internet se llevo a cabo a través de fronteras internacionales;
- Si no se garantiza que los contratos se evidencien solo por medios electrónicos vinculantes;
- Más confianza en el comercio electrónico al hacer negocios importantes sistemas o negocio otras transacciones en internet, y
- Sistemas e infraestructura de fallos o accidentes.

El auditor además usa el conocimiento de la empresa para identificar los eventos, transacciones y prácticas relacionadas con los riesgos del negocio derivados de las actividades del comercio electrónico.

5.1.4. Cuestiones Jurídicas y Reglamentarias

Un amplio marco jurídico internacional para el comercio electrónico y un eficiente para apoyar ese marco (la firma electrónica, registros de documentos, los mecanismos de controversias, protección de los consumidores, entre otras) en el caso chileno la firma electrónica ya existe. Los marcos jurídicos en las distintas jurisdicciones varían en su reconocimiento del comercio electrónico. Los factores que pueden dar lugar a los impuestos sobre las transacciones de e-commerce hará constar el lugar donde:

- La entidad está legalmente registrada;
- Sus operaciones se basan físicamente;
- Su servidor web se encuentra;
- Los bienes y servicios son suministrados, y

- Entre sus clientes se encuentran bienes y servicios prestados.

5.1.5. Seguridad

Entidad de seguridad de la infraestructura y los controles relacionados son una particular característica importante de su sistema de control interno en las partes externas son poder tener acceso a la entidad la información del sistema utilizando una red pública como el Internet. La información es segura en la medida en que los requisitos para su autorización, la autenticidad, confidencialidad, integridad, no repudio y disponibilidad se han cumplidos. La entidad normalmente se ocupará de los riesgos de seguridad relacionados con el registro y el procesamiento de transacciones de e-commerce a través de su infraestructura de seguridad y los controles relacionados.

La infraestructura de seguridad y los controles relacionados pueden incluir una política de seguridad de la información, un riesgo para la seguridad de información evaluación, y las normas, medidas, prácticas y procedimientos dentro de los sistemas individuales se introducen y mantienen, tanto medidas físicas y lógicas y otras garantías técnicas como usuario identificadores, contraseñas y firewalls. En la medida en que sean pertinentes para la declaración afirmaciones financieros que el auditor considera aspectos tales como:

- El uso eficaz de los firewalls y software antivirus para proteger sus sistemas de la introducción de software no autorizado o perjudicial, datos u otro material en formato electrónico.
- El uso eficaz de la encriptación, incluyendo:
  - Mantener la privacidad y seguridad de las transmisiones a través, por ejemplo, autorización de claves de descifrado, y
  - Prevenir la utilización indebida de la tecnología de encriptación, por ejemplo, el control y la protección de descifrado las claves privadas.
- Los controles sobre el desarrollo e implementación de sistemas utilizados para apoyo a actividades de comercio electrónico;
- Si los controles de seguridad en el lugar siguen siendo eficaces como nuevas tecnologías que se pueden utilizar para atacar a la seguridad en Internet disponible, y
- Si el ambiente de control compatible con los procedimientos de control implementado. Por ejemplo, mientras que algunos procedimientos de control, tales como digital de

cifrado de sistemas basados en el certificado, puede ser técnicamente avanzada, no puede ser eficaz si operan dentro de un ambiente de control inadecuados.

5.2. Prácticas de Auditoria en los Sistemas de Información

También existen las prácticas de los sistemas de seguridad que se encuentran en la serie 27000 de las Iso, en el siguiente extracto se menciona algunas de estas Iso que son utilizadas por el auditor, según lo menciona Wikipedia.

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación e incluyen:

- ISO/IEC 27000 - es un vocabulario estandard para el SGSI. Se encuentra en desarrollo actualmente.
- ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estandar internacional en octubre de 2005.
- ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
- ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010.
- ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
- ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos

de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3.

- ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
- ISO/IEC 27007 - Es una guía para auditar al SGSI.
- ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.
- ISO/IEC 27035:2011 - Seguridad de la información- Técnicas de Seguridad- Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. (Wikipedia, 2012)

5.3. Riesgos de Auditoria en el Comercio Electrónico

Si se realiza un esquema cuales son los grandes riesgos que puede tener el comercio electrónico se puede mencionar:

- ❖ Entorno empresarial y tecnológico cambiante.
- ❖ Privacidad y seguridad.
- ❖ Asunto legales, políticas y sociales.

De acuerdo al presente trabajo se enfoca en el riesgo de la privacidad y seguridad por la falta de veracidad de los datos enviados, en la cual se debe ver desde un punto de vista de una auditoría informática y dentro de esta en una seguridad lógica.

5.3.1. Seguridad Informática

Según el autor Mario G. Piattini la define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (Piattini, Mario, 2001, p.4) Y se puede definir como “aquellas prácticas que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la

información en el contenida". (definicionabc.com, 2011). Por lo tanto se puede definir como la disciplina de proteger la integridad y la privacidad de los datos entregados impidiendo todo anomalía que pueda alterar los sistemas almacenados en el sistema informático.

Los objetivos de la seguridad informática son:

- Garantizar la adecuada utilización de los recursos y de todas las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación de los sistemas en el caso de eventuales incidentes que puedan ocurrir dentro de la entidad.
- Reducir y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad a través de diferentes controles. Este objetivo divide los controles en 3 categorías:
  - Controles preventivos: que tratan de evitar el hecho, como un software de seguridad que impida todos los accesos no autorizados al sistema vigente, evitando pérdidas millonarias en el daño de los sistemas a los datos poseídos.
  - Controles detectivos: es cuando fallan los preventivos para tratar de conocer cuanto antes el evento que altera el sistema, como es en el caso del registro de actividades para detectar errores u omisiones del acceso de personas no autorizadas, la cual se realiza dentro de los bancos ya que una persona que está sacando dinero en Chile, no puede a la hora después estar ocupando la misma tarjeta para sacar dinero en Estados Unidos, entonces ahí se encuentra una anomalía la cual es detectada y avisada al usuario.
  - Controles Correctivos: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un archivo dañado a partir de las copias de seguridad, esto ocurrió directamente en los atentados de 11 de Septiembre 2001, cuando muchas de las empresas internacionales tenían sus oficinas centrales en World Trade Center, y aun cuando hubo un incidente a escala mayor, a los días después ya estas empresas estaban funcionando con sus sistemas operativos adecuadamente.
- Cumplir con el marco legal y con todos los requisitos impuestos por los clientes en los contratos firmados.

Para alcanzar estos objetivos se debe ver de 4 planos que son:

- Técnico: nivel físico como a nivel lógico.
- Legal: las medidas de seguridad implantada por el país de origen de la entidad, para cumplirlas cabalmente.
- Humano: formación de los empleados y directivos, definiendo cuales son cada una de sus funciones y la obligación que le corresponde a cada una de estos.
- Organizativo: definir e implementar las políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación que lleve a la organización a ser una entidad segura.

Por lo tanto es necesario ver la seguridad informática como un proceso dentro de la organización y no como un producto a instalar, la cual tiene mucha importancia dentro de esta.

5.4. Que ocurre en Chile

Porque es tan necesaria la seguridad informática dentro de una empresa, debido a lo mencionado anteriormente y a los nuevos delitos relacionados en estos últimos años es uno de los mayores problemas de seguridad a nivel global que está sufriendo las entidades. Como es lo que ocurre en Chile según un informe de radio cooperativa el año 2009 donde se menciona “En Chile los delitos cometidos por internet han ascendido numerosamente, porque durante el año 2009 se registraron 396 denuncias y en lo que va de este año, ya se han registrado más de 500, según la Brigada de Ciber Crimen de la Policía de Investigaciones” (Cooperativa.cl, 2011). Esto da a entender que los delitos realizados por internet es algo que va en aumento y uno de los métodos más usados por los delincuentes informáticos se conoce como phishing, nombre que reciben correos electrónicos pidiendo una supuesta actualización de los antecedentes bancarios o alertas de bloqueos o intervención en las cuentas de los mismos, estos correos fraudulentos contienen un link, que deriva a los usuarios de sitios web con formularios falsos, que imitan el formato de los bancos, y en donde solicitan la información para actualizarla y en la cual los usuarios realizan y se comete el robo de los datos. En Chile las penas para quienes son descubiertos realizando estos delitos son bajas y a lo que pueda interpretar el juez en cuestión lo que lleva a que se sigan realizando tantos delitos informáticos sin temor a que estos puedan ser castigados por la ley vigente.

Por lo tanto es necesario conocer los riesgos que puede tener toda empresa que comercializa sus productos electrónicamente, como también ocurre en las entidades bancarias.

5.5. Riesgos de seguridad y privacidad

Se encuentra 3 tipos de amenazas a la seguridad informática que son:

5.5.1. Criminalidad

Son todas las acciones causadas por la intervención humana, que violan directa o indirectamente la ley y que están penadas por estas. En la cual se encuentra los fraudes, y toda operación realizada por alguien con el fin de engañar al sistema logrando el objetivo planeado por estos delincuentes, que en su gran mayoría son estafas efectuadas para obtener la información el de algún cliente para después robarle el dinero que este posee. Dentro de estas se encuentras:

- Delitos dirigidos a la computadora como método, medio en la comisión del ilícito:
  - Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, entre otras.
  - Variación de la situación contable.
  - Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
  - Alteración del funcionamiento normal de los sistemas mediante la introducción de código extraño al mismo: virus, bombas lógicas, entre otras.
  - Intervención de líneas de comunicación de datos o teleprocesos.
- Y delitos dirigidos en contra de la computadora, pero en sus accesorios o programas como una entidad física:
  - Instrucciones que producen un bloqueo parcial o total del sistema
  - Atentado físico contra la computadora, sus accesorios o sus medios de comunicación
  - Secuestro de soportes magnéticos con información valiosa para ser utilizada con fines delictivos
  - Destrucción de programas por cualquier método.

5.5.2. Sucesos de origen físico

Son los eventos naturales, técnicos y además eventos indirectamente causados por la intervención humana. Dentro de esta categoría se encuentran los incendios, inundación, sismos, sobrecarga eléctrica, entre otras, esta se controla bajo una Seguridad Física.

5.5.3. Negligencia y decisiones institucionales

Que corresponden a las acciones, decisiones u omisiones por parte de las personas que tienen la influencia de poder ingresar a estos sistemas. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano. Por eso recae la importancia de que no cualquier persona pueda estar a cargo de estos sistemas debido a que una mala decisión o alguna negligencia pueda llevar incluso a la quiebra a la entidad, y además la confianza que se debe tener al personal, la cual en este caso quisiera recalcar, aunque no es el objeto puramente de este estudio, debido a que a veces los mismos empleados son los que pueden aprovechar sus influencias dentro del sistema y sacar provecho de esto, como es lo que ocurrió en Chile con el caso de un joven ingeniero en informática que pretendía aprovecharse de su posición y vender una base de datos de una conocida tienda del retail chileno, la cual le reportaría millonarias sumas de dinero a su bolsillos, como lo indica la noticia a través de radio cooperativa “Un egresado de Ingeniería en Informática que se desempeñaba como analista en una empresa de cobranza intentó vender por internet la base de datos de la tarjeta Presto, del supermercado Líder, por lo cual fue detenido por la PDI. Los datos de 400 mil personas estaban evaluados en 800 millones de pesos”. (Cooperativa.cl, 2011). Esta noticia podría caer en el riesgo de criminalidad pero se ha puesto en este punto porque se deben realizar constantes capacitaciones al personal no solamente porque la tecnología va avanzando continuamente sino que además para que estos hechos no ocurran dentro del personal de la entidad, siendo un fuerte golpe a la ética de las personas que trabajan en estos sistemas. Esta área se puede controlar bajo una Seguridad en las Comunicaciones.

En este caso se enfoca en la criminalidad debido a que en esta área donde ocurren los fraudes y engaños en el comercio electrónico. Ahora se verá la seguridad lógica como las

medidas de proteger a los sistemas de informáticos que poseen las empresas efectuadas en el comercio electrónico.

6. Seguridad Lógica

Como se menciona anteriormente existen diversos riesgos a las entidades, pero el contador auditor debe anticiparse al delito que pueda ocurrir y necesita realizar procedimientos y tareas en la cual debe evitar los fraudes, y realizar los controles pertinentes los cuales estos controles los deben realizar auditores expertos en estos sistemas de información. Para esto se debe definir que es seguridad lógica.

Seguridad lógica según una página web de seguridad informática la define como la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo" (Seguridad Informática, 2011). Entonces se puede definir a la seguridad lógica como la barrera de mecanismos para mantener el resguardo y la integridad de la información de un sistema informático. Desde esta plataforma esta tiene el objetivo de:

a) Restringir el acceso a los programas y archivos que puedan tener información valiosa.
b) Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
c) Asegurar que se estén utilizados los datos, archivos y programas correctos en los procedimientos correctos.
d) Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
e) Que la información recibida sea la misma que ha sido transmitida.
f) Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
g) Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Para lograr estos objetivos de seguridad se debe ofrecer los mecanismos correspondientes como lo describe Mario Piattini los cuales son:

a) Identificación de usuarios y políticas de contraseñas

b) Control lógico de acceso a los recursos
c) Copias de seguridad
d) Centros de respaldos
e) Encriptación de las transmisiones
f) Huella digital de mensajes
g) Sellado temporal de mensajes
h) Utilización de la firma electrónica
i) Protocolos criptográficos
j) Análisis y filtrado del tráfico (cortafuegos)
k) Servidores proxy
l) Sistema de detección de intrusiones (IDS)
m) Antivirus, entre otras. (Piattini, Mario, 2001, p.14)

Por esto es necesario verificar que cada usuario solo pueda acceder a los recursos a los que le autorizo el propietario, aunque sea de forma genérica, según su función y con la posibilidad de que en este caso el propietario haya fijado, si esta autorización se realizara de lectura, con modificación, borrado, ejecución trasladando a los sistemas lo que representaríamos en una matriz de accesos en la que figuran los sujetos grupos de usuarios o sistemas, los objetos que puedan ser accedidos con mayor o menor regularidad al disco, una aplicación, una base de datos, un programa, con las posibilidades que a esta se le otorgan si es de lectura, borrado o ejecución. O sea dependiendo de la autorización que obtenga el usuario va a adquirir el nivel si puede leer o trabajar en el sistema.

6.1. Procedimientos de Auditoria

Desde el punto de vista de la auditoria se han señalados pautas de lo que se debe conocer, que es lo que se debe hacer en la “auditoria y el comercio electrónico”.
La auditoría debe necesariamente revisar cómo se identifican y sobre todo autentican los usuarios, como han sido autorizados y por quién, y que ocurre cuando se producen transgresiones o intentos: quién se entera y cuando y que se hace, en los debidos casos.

Algunos aspectos a evaluar respecto de las contraseñas según Piattini es:
a) Quien asigna la contraseña: inicial y sucesivas
b) Longitud mínima y composición de caracteres

c) Vigencia, incluso puede haberlas de un solo uso o dependientes de una función tiempo
d) Control para no asignar las “x” ultimas
e) Numero de intentos que se permiten al usuario, e investigación posterior de los fallidos: pueden ser errores del usuario o intentos de suplantación
f) Si las contraseñas están cifradas y bajo qué sistema, y sobre todo que no aparezcan en claro en las pantallas, listados, mensajes de comunicaciones o corrientes de trabajos (JCL en algunos sistemas)
g) Protección o cambio de las contraseñas iníciales que llegan en los sistemas y que a menudo aparecen en los propios manuales
h) Controles existentes para evitar y detectar caballos de Troya: en este contexto se trata de un programa residente en un PC que emulando un terminal simule el contenido de la pantalla que recoge la identificación y contraseña del usuario, grabe la contraseña y devuelva control al sistema verdadero después de algún mensaje simulado de error que normalmente no despertara las sospechas del usuario.
i) La no-cesión, y el uso individual y responsable de cada usuario, a partir de la normativa. (Piattini, Mario, 2001, p.403).

Otra posible debilidad que debe considerarse en la auditoría es si pueden crear situaciones de bloqueo porque solo exista un administrador, que puede estar ausente de forma no prevista, por ejemplo por haber sufrido un accidente, e impedir la creación nuevos usuarios en un sistema de administración centralizada y única.

Además se debe desarrollar procedimientos realizados por el auditor en la seguridad lógica en los siguientes puntos:

- Monitorizar los archivos:
  - Comprobar propietarios y permisos de los archivos importantes de configuración del sistema.
  - Comprobar propietarios y permisos de los directorios importantes del sistema.
  - Verificar la integridad de archivos binarios del sistema
  - Verificar la presencia o ausencia de ciertos archivos
  - Verificar la integridad interna de los sistemas de archivos

- Monitorizar la actividad del sistema:

- Procesos
- Intentos fallidos de entrada
- Intentos de entrada del superusuario
- Tareas realizadas por el superusuario
- Lo hacen los usuarios
- Auditar los eventos importantes del sistema

Otra protección que se debe tomar en cuenta y debe ser vista por el auditor es la protección de los programas, que estos sean de la propiedad de la entidad y no de terceros y que tengan licencia para usar estos programas.

Ahora cabe la interrogante ¿Cómo se puede realizar todo esto?

Para esto se debe tener en cuenta que frecuentemente el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Las Trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo. (*Herramientas y técnicas para la auditoría informática*, (s.f.))

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

El auditor informático debe emplear preferentemente la amplia información que proporciona el propio Sistema: Así, los ficheros de <Accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <Log*> de dicho Sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.

El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la Aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log permite analizar cronológicamente que es lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos. (*Auditoría Informática*, (s.f.))

Otro punto que debe realizar el auditor informático es el tunning que es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

- Cuando existe sospecha de deterioro del comportamiento parcial o general del Sistema
- De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano. (*La Auditoría (Definiciones, métodos, tipos y ejemplos)*, (s.f.))

El auditor deberá conocer el número de tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

También es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condicione el Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

En general el auditor deberá realizar controles relativos a la seguridad lógica:

- Verificación de controles de acceso a los archivos y base de datos, que impida el acceso libremente, evitando que sean leídos, copiados o alterados.
- Verificación que la entidad tiene definido un registro de usuarios autorizados a acceder a cada uno de los archivos pero con la especificación correspondiente si es solo lectura, si se puede trabajar en él, debe estar registrado.
- Comprobación de un registro de los accesos al sistema no autorizados, y para aquellos archivos más críticos, un registro de los accesos producidos en el que indique la fecha y hora, tipo de operación realizada sobre los datos y el usuario que inicio el acceso.

6.2. Conductas del Auditor

Pauta de las conductas que debe tener un auditor informático según el autor Mario Piattini:

Qué pueden/deben hacer Los auditores	Qué no deben hacer los auditores
Ser independientes y objetivos	Actuar en beneficio propio por encima del interés del cliente
Recomendar	Obligar, forzar, amenazar
Ser competentes en la materia (seguridad)	Asumir encargos para los que no esten preparados
Basar sus informes en verificaciones y evidencias	Basarlos en suposiciones
Verificar que se evaluan periodicamente riesgos o bien evaluarlos	Revisar la seguridad "día a día" o administrada (son fuaciones de otros)
Conocer perfiles de usuarios	Realizar gestión perfiles de usuarios
Conocer criterios y prácticas sobre contraseñas	Gestión/asignación contraseñas o conocerlas
Verificar que las aplicaciones se desarrollan y mantienen según normas y se incorporan controles	Realizar funciones de análisis o gestionar proyectos
Revisar codificacion de programas (seguridad y calidad) y las pruebas realizadas, o bien probarlos	Codificar programas
Revisar la documentación (aplicaciones, programas)	Realizar la documentación
Verificar que siguen los procedimientos	Escribir procedimientos
Responsabilizarse del contenido de sus informes	Aceptar presiones de sus jefes o clientes y que el informe no sea veraz
Evaluar riesgos e informes	Garantizar que no se puedan realizar/haber realizado delitos, fraudes o errores
Sustentar los informes con papeles de trabajo	Enzarzarse en discusiones de diferencias de opiniones
Estar al día en cuanto a avances, riesgos, metodologias	Auditar con técnicas, métodos o recomendaciones obsoletos

Fuente: Pautas de conducta de los auditores, Auditoría Informática un enfoque práctico

7. La auditoría en el sistema bancario

En el sistema bancario existen constantes auditorias y controles por agentes externos como internos del Banco, para garantizar que cumple con los procedimientos y tiene los mecanismos de control adecuados para prevenir y detectar el correcto funcionamiento de los sistemas informáticos, garantizando seguridad y confianza al sistema bancario como a los clientes que son usuarios de los servicios emitidos por el banco.

Se debe tener presente que los bancos además de prestar servicios financieros son un ente que constituyen una gran fuente de datos para agentes externos. Cabe mencionar que entre los mismos bancos se traspasan información el uno hacia el otro. (Oscar Vallarin, Sub gerente de medios de pago, Banco Internacional).

Por la funciones que el banco realiza este maneja información sensible de cada uno de sus clientes, como lo es su situación patrimonial, saber las aficiones y gustos personales de cada uno de sus clientes, si tiene endeudamiento, cuál es su profesión, el valor tasado de su viviendo, e incluso el tener un patrón de dinero que retira con cuanta periodicidad lo realiza, entre otras.

Es por ello que se puede analizar que los mayores riesgos que existe en el sistema de información bancario de acuerdo a lo establecido por Piattini corresponde a:

a) Difusión no autorizada, intencionada o no, hacia destinos improcedentes. Esto se debe que la información de los clientes puede representar para empresas comerciales y otro tipo de organizaciones un valor incuestionable, como se le menciona anteriormente en la página 34 del presente trabajo de la persona que iba a vender la base de datos de 400 mil personas en 800 millones de pesos.

   Es por ello que la confidencialidad es un tema especial preocupación en cualquier entidad financiera, porque el negocio bancario tiene como una de sus características la de ser una actividad en mayor o menor grado intervenir en la confianza depositada por los clientes.

b) Obtención de información errónea, por accidente o manipulación indebida. (Piattini, Mario, 2001)

Lo cual es lo medular de esta presente análisis de tesis, debido a que los sistemas de información en general están muy bien resguardados a través de programas, y controles constante que realizan los bancos a sus sistemas informáticos en lo cual las entidades

bancarias invierten en millones de pesos para tener la última tecnología en seguridad, pero esto no va a tener efecto alguno si las personas que están a cargo, de esta información privilegiada de los clientes los utiliza con un fin perjudicial o venderlos para obtener un beneficio de dicha operación.

8. El Informe de Auditoria

Para conocer que es lo que después se realiza, se debe explicar brevemente lo que ocurre una vez hechos todos los procedimientos de auditoría.

El Informe de Auditoría es la comunicación del Auditor Informático al cliente de una manera solemne y formal, tanto del alcance de la auditoría realizada en sus objetivos, período de cobertura, naturaleza y extensión del trabajo realizado, además de los resultados y conclusiones elaboradas por el auditor. Este informe debe ser necesariamente revisado por las personas que realizaron la auditoría y discutido entre ellos según todas las aristas importantes obtenidas en los papeles de trabajo, para finalmente emitir el informe definitivo. En cada punto expuesto en el informe se debe explicar porque se cree que existe un incumplimiento o una debilidad, además de alguna recomendación que ellos darían, eso si nunca ligando su recomendación a que esta debe ser lo definitivo a realizar. La entidad auditada siempre busca un informe lo más benigno posible, mientras que los auditores se deben proponer llegar a un informe veraz y útil; estos diferentes puntos de vista a veces crean algunos problemas en el transcurso de la auditoría y en la discusión del informe.

Algunos puntos importantes que pueden llegar a estar dentro de los informes respecto a la seguridad, por la ausencia de estos son:

- Copias de activos críticos en cuanto a su continuidad
- Cumplimiento de la legislación aplicable así como de las políticas y normas internas
- Diferenciación de entornos de desarrollo y producción
- Involucración de la alta Dirección
- Evaluación periódica y adecuada de riesgos
- Segregación de funciones.

Estos son los puntos que más podrían referirse en el informe de auditoría.

La evidencia son la base que tiene el auditor para poder formular sus propias conclusiones, se pueden generalmente encontrar 4 tipos de evidencias las cuales son:

- Evidencia relevante: esta tiene una relación lógica con los objetivos de la auditoría.

- Evidencia suficiente: esta es de tipo cuantitativo, es la evidencia suficiente, objetiva y convincente que basta para sustentar los hallazgos, las conclusiones y recomendaciones expresadas en el Informe.
- Evidencia adecuada: Es de tipo cualitativo para afectar a las conclusiones del auditor.
- Evidencia fiable: es válida y objetiva, aunque con un nivel de confianza.

Las pruebas de cumplimiento consisten en comprobar que se están cumpliendo las normas establecidas. En caso de que no existan manuales o no se puedan hacer las pruebas de cumplimiento se debe pasar a las pruebas sustantivas

Las pruebas sustantivas consisten en revisar las aplicaciones, si son pocas aplicaciones se revisan todas, si son muchas se elige una muestra representativa que se han pasado de desarrollo a explotación y revisar que antes de pasarlas han sido sometidas a un lote de pruebas y las han superado satisfactoriamente, debido a que cumplen los requisitos y estándares del sector.

Después de todo se realizara el Informe de Auditoría final el cual debe contener los siguientes puntos esenciales y mínimos de un informe.

1) Identificación del informe (titulo)
2) Identificación del cliente (destinatarios)
3) Identificación de la entidad auditada (objeto de la auditoria)
4) Objetivos de la auditoria (propósito)
5) Normativa aplicada y excepciones (normas legales)
6) Alcance de la auditoria (naturaleza y extensión, señalando sus limitaciones al alcance y restricciones del auditado)
7) Conclusiones
8) Fecha del informe
9) Identificación y firma del auditor
10) Distribución del informe

Con esto se terminaría el proceso de auditoría a la entidad controlada.

CAPITULO II

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

El entorno competitivo que desarrollan las empresas ha experimentado varios cambios dentro de los cuales existe la incorporación de las tecnologías de información y comunicación como una de las técnicas que más rentabilidad genera a sus dueños. Utilizando esta plataforma se ha desarrollado el comercio electrónico. En la actualidad las compañías en su gran mayoría tienen áreas especializadas en este tema, para brindar al consumidor un mayor servicio.

Hoy existe poco conocimiento del comercio electrónico y su manera de operar, esto se refleja en el Auditor, que debe recurrir a especialistas en tecnologías de información para validar los sistemas computacionales utilizados por las instituciones, al cual se le debe entregar el conocimiento para que comience a prepararse en este tipo de comercio. Debido a que el auditor trabaja en base a información entregada por las entidades que este audita, esta información debe ser confiable, existiendo siempre un riesgo en toda auditoría pero la cual aumenta cuando se habla de transacciones que se realizan a través de internet a la cual pueden acceder todo tipo de individuo que pueden burlar los sistemas de seguridad informáticos implantados por la entidad y cometer un ilícito informático el cual en cierta medida deberían ser detectados por la auditoría. Además se debe conocer los instrumentos utilizados por las entidades para dar seguridad a las transacciones realizadas por las redes de internet.

De esta perspectiva el comercio electrónico necesita ser conocido, a través de la investigación, informando el aumento obtenido y la relevancia que obtendrá en el pronto tiempo. Además el auditor debe descubrir los riesgos adherentes al realizar procedimientos bajo comercio electrónico, que se conoce que son las personas internas de la misma entidad el mayor peligro lo cual se descubre por medio de las entrevistas realizadas a firmas auditoras de los procedimientos utilizados para controlar estos sistemas y entrevistas realizadas a sociedades bancarias y sus medidas de seguridad para evitar ilícitos bancarios.

OBJETIVOS DE LA INVESTIGACION

OBJETIVO GENERAL

Analizar los riesgos de seguridad lógica en la auditoria de sistemas de información del comercio electrónico en Chile. En una entidad Bancaria.

OBJETIVOS ESPECIFICOS

1. Identificar las políticas de seguridad que proporciona las entidades bancarias a sus clientes e internamente.

2. Revelar las medidas de seguridad en el sistema bancario, mediante de fuentes internas de la institución financiera.

3. Descubrir los riesgos existentes en él sistemas de información en sus procesos y la relevancia del factor humano en estos procesos, mediante interpretación de fuentes externas.

PROPUESTA METODOLÓGICA

El presente estudio es de tipo cualitativo con un enfoque de sintetización. Se basa principalmente en los riesgos existentes en las transacciones que existen en el comercio electrónico. En el cual se realizó por medio de las siguientes fases, en cada una de las cuales se establecieron actividades que se indican a continuación:

Fase I Recopilación de antecedentes bibliográficos

- Recopilar información de las entidades bancarias.
- Recopilar antecedentes de la auditoria informática.
- Revisión de páginas de internet de políticas de seguridad bancarias.
- Consultas a expertos del tema.

Fase II Sistematización de la información recopilada

- Ordenamiento de la información encontrada, dependiendo de su importancia y relevancia dentro de la tesis.
- Digitalización de la información recopilada.
- Realización de cuadros comparativos.

Fase III Elección de sujeto de investigación

- La elaboración de entrevistas.
- Entrevistas a experto en el área de bancario y auditores en informática.

- Aplicación de la entrevista a las personas encargadas del área de sistema de información que puedan proporcionar datos relevantes para la investigación.

Fase IV Aplicación de la técnica de Recogida de datos.

Ruta de la Entrevista

- Contacto inicial con la empresa, para la autorización de la entrevista la que se realizará a un encargado del área de administración que opere con los sistemas de información.

- Se procederá a efectuar la entrevista en profundidad sobre la información requerida.

- Transcripción de la entrevista

- Informe entrevista final.

Fase V Criterios de Calidad

La propuesta metodológica para la entrevista incorpora los criterios de credibilidad, confirmabilidad, fiabilidad y transferencia.

- La credibilidad se realizará en cada una de las técnicas de recolección de datos, en el caso de las entrevistas en profundidad la credibilidad es la revisión por parte del entrevistado y la aprobación de la entrevista final.

- La confirmabilidad se presentará al incorporar a los distintos actores que forman parte de la investigación.

- La fiabilidad se entregará a partir de la presentación de la ideología del investigador.

- Tranferibilidad estará dada al describir el contexto y cada una de las situaciones en particular en conjunto con las características de los sujetos.

Fase VI Categorización

- Categorización de las entrevistas realizadas considerando el problema de investigación y los objetivos que busca este estudio.

CATEGORIZACIÓN

1) **Seguridad en el sistema bancario**
   a) Normativa, que rigen al sistema bancario.
   b) Enfrentamiento de virus, lograr combatir los ataques externos.
   c) Respaldo de información, donde se guardan la información en caso de eventual ataque.
2) **Seguridad al cliente**
   a) Estrategias, efectuadas por el banco entregar seguridad a sus clientes.
3) **Políticas internas para trabajar en el sistema bancario**
   a) Asignación de perfiles, para trabajar en el sistema.
   b) Limitaciones a usuarios internos, para solo trabajar en lo requerido.
4) **Controles al sistema bancario**
   a) Interno, personas del mismo banco.
   b) Externo, personas que no tengan relación con el banco.
5) **Factor humano**
   a) Orientación, como se educa al personal.
   b) Riesgo, de que una o pocas personas manejen información tan importante.

Fase VII Análisis de Resultados

- Análisis de la información en función de las categorías de análisis de las entrevistas aplicadas a cada experto.

Fase VIII Discusión de resultados

- Discusión de la Información Recopilada en base a lo establecido por la teoría y lo que resultados de acuerdo a los expertos.

Fase IX Conclusiones

- Identificar conclusiones luego de finalizado la etapa de discusión de resultado.

CAPITULO III

ELECCION DE LAS ENTIDADES EN ESTUDIO

Se eligieron a la entidad bancaria Banco Internacional y el Banco de Chile porque son entidades que cubren todo tipo de cliente, tanto como el Banco Internacional que apunta a una clase social alta, y el Banco Chile que es en general para toda clase social. Los auditores entrevistados son expertos en informática, como los entrevistados en el Banco que son muy entendidos en el tema de seguridad dentro del Banco.

Por esto se eligieron a estas personas porque son aquellas que proporcionan la información necesaria para poder determinar las conclusiones de la presente investigación.

ANÁLISIS DE RESULTADOS

1. Enfoque del Sistema Bancario

a) Políticas de seguridad: Las políticas de seguridad son vista de dos aristas, las políticas de seguridad que tiene que adquirir el cliente con la institución bancaria y la otra es la Institución bancaria internamente. Las políticas de seguridad se encuentran disponibles libremente en las páginas de cada institución bancaria en lo que respecta a la seguridad, y entrega información educativa para que los clientes ingresen al sistema de la manera más segura y óptima. Esto conlleva a que las instituciones bancarias sean entidades que estén cumpliendo con diferentes normativas de seguridad constantemente y que sus sistemas no se vean vulnerados con ataques externos e internos.

i) Con el cliente: El banco maneja políticas de seguridad internas, que en si son entregarle la seguridad correspondiente al cliente que todas las transacciones realizadas entre ambos es segura y confiable, y que nadie intervendrá en esta transacción.

ii) Internas: siempre existe contingencia para que nada de lo que está en producción se pierda y siempre quede guardado en algún lugar del sistema.

b) Medidas de seguridad: Las medidas de seguridad son variadas, desde el momento para entrar al sistema en la identificación y autenticación hasta cuando este realiza una transacción, todo se encuentra normado por los sistemas de seguridad de la entidad bancaria. Agregando además que internamente no cualquier persona puede ingresar a la data sensible, sino que se realiza bajo ciertos perfiles que los entrega el oficial de seguridad, entregando la confianza necesaria en estos sistema, de lo cual es poco lo que se puede atacar.

i) Con el cliente: existen dos tipos de medidas de seguridad, una es entregándole al cliente el mayor grado de comunicación en su sistema para que él no caiga en algún trampa, y medida de seguridad cuando exista una anomalía dentro del lugar donde se encuentra el cliente y la transaccionalidad que está realizando, ya que esto se rige por patrones de los clientes.

ii) Internas: el sistema bancario crea toda una operación para que nadie dentro de la empresa acceda a toda la información manejada.

c) Ataques: Los ataques son de malware que van dirigidos a los clientes, los cuales son detectados a través de los controles internos que realiza la entidad bancaria.

i) Principales ataques: malware, phishing, pharming en si son ataques que van dirigidos a los clientes, ya que al sistema bancario es complicado

ii) ¿Cómo me percato de ataques?: uno se percata por los controles internos que según patrones de comportamiento de los clientes detectas anomalías dentro de un cliente y la alertan

d) Control: La información es controlada por oficiales de seguridad que son los encargados de entregar permisos, y dar las autorizaciones correspondientes para cada trabajo realizado por los funcionarios.

i) Encargados y función: en el banco existen los oficiales de seguridad que son personas que entregan todos los permisos para que los usuarios internos del banco puedan trabajar en ellos, en base de perfiles, esto está muy normado dentro de los bancos, y siempre tiene restricciones y todo es con sus respectivas autorizaciones

ii) Factor humano: Primeramente se debe educar a los usuarios internos dentro de la entidad bancaria de que todo lo que realizan debe pedir sus autorizaciones, a través de compromisos en los cuales ellos realizan, y además que el mismo oficial de seguridad no te permite acceder a información por más que la necesites puedas utilizar porque es información más sensible

2. Enfoque de Auditoria

a) Normativa: La seguridad de información que se rigen los auditores son las normativas ISO 27000 y sus correspondientes secciones es una guía para el auditor y en instituciones del Estado por el decreto 83. Esto es un tema poco abordado en Chile y por lo tanto no existe demasiada normativa

b) Procedimientos: Los procedimientos realizados por el auditor siempre son los mismos, y además pueden a veces variar de acuerdo a la experiencia del auditor, pero siempre se debe comenzar con lecturas de políticas para que según esa lectura es como irán actuando.

i) ¿Qué se busca?: Siempre se busca la seguridad, que empresa como cliente al momento de realizar una transacción sea de la manera más segura, que viaje toda la información sin percance de manera óptima y segura. Y que solo acceda a esto solo las personas autorizadas y ninguna otra más

ii) ¿Qué se analiza?: Existen dos tipos de revisión, análisis uno es la lectura de los procedimientos con sus políticas, y la forma como trabaja la empresa, y el otro está relacionado a la seguridad lógica pura, en la cual se realizan controles para detectar programas maliciosos que pueden afectar a la confidencialidad de la información

c) Riesgos: Siempre existirán riesgo en toda auditoria, pero el mayor riesgo en este ámbito viene internamente, que son las personas internas las cuales vulneran el sistema el cual ha sido implantado.

i) Procesos: en el proceso existen sistemas para poder darse cuenta de cuando se está haciendo algo que no corresponde debido a que toda la información siempre queda registrada en algún lugar y por ello es la evidencia comprobatoria en el caso que allá algo que no corresponda.

ii) Factor humano: este es el punto más crítico debido a que por regla son pocas las personas que manejan demasiada información, en las cuales debe haber confianza en ellos y no se vean tentados por su cargo a realizar maniobras que le generen beneficios pero a la empresa afecten. Como el auditor lo menciono en la entrevista puede ser que la empresa gaste el máximo de dinero en sistemas de seguridad para su empresa pero si no existe los debidos controles de esto, de nada va a funcionar por eso los mayores ataques a los sistemas de información se dan dentro de la misma entidad en vez de un externo

iii) Recomendaciones: En las entidades primero se debe revisar los privilegios de los usuarios que puedan trabajar con cierta información, solo la necesaria, y además que se modifiquen contratos imponiendo clausulas en las cuales el informático no pueda traspasar nada, o tomar privilegios que no le corresponde y de lo contrario tiene que pagar una penalización por aquello.

CAPITULO IV

DISCUSIÓN DE RESULTADOS

Cuando se habla de normativa los auditores se rigen por las ISO 27000 y sus series las cuales dan una extensa guía de los puntos que se deben revisar en una auditoria en seguridad de sistemas, y a esto agregado la experiencia que el auditor adquiere con el paso del tiempo, mientras tantos que en el marco teórico se regían por las IAPS 1013 que habla de la auditoria en el comercio electrónico.

En esta seguridad siempre se busca que la información que viaja entre la empresa y el cliente, sea de manera óptima y segura, solo accediendo a esta las personas debidamente autorizadas dentro del control interno, mientras que en el marco teórico esta expresado que es garantizar la adecuada utilización de los recursos y de todas las aplicaciones del sistema, Limitar las pérdidas y conseguir la adecuada recuperación de los sistemas en el caso de eventuales incidentes que puedan ocurrir dentro de la entidad y por último reducir y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad a través de diferentes controles.

En la categorización se percibe que existen dos tipos de revisión, análisis uno es la lectura de los procedimientos con sus políticas, y la forma como trabaja la empresa, y el otro está relacionado a la seguridad lógica pura, en la cual se realizan controles para detectar programas maliciosos que pueden afectar a la confidencialidad de la información. Además a través de la entrevista se puede percibir que las personas que manejan demasiada información es poca, en las cuales debe haber confianza en ellos y no se vean tentados por su cargo a realizar maniobras que le generen beneficios pero a la empresa afecten. Como el auditor lo menciono en la entrevista puede ser que la empresa gaste el máximo de dinero en sistemas de seguridad para su empresa pero si no existe los debidos controles de esto, de nada va a funcionar por eso los mayores ataques a los sistemas de información se dan dentro de la misma entidad en vez de un externo. Tema que en el marco teórico es mencionado que corresponden a las acciones, decisiones u omisiones por parte de las personas que tienen la influencia de poder ingresar a estos sistemas. Al mismo tiempo son las amenazas menos predecibles porque están

directamente relacionados con el comportamiento humano. Por eso recae la importancia de que no cualquier persona pueda estar a cargo de estos sistemas, y esto es en general lo más importante de los riesgos que se pueden encontrar dentro de la seguridad informática, porque se puede invertir mucho dinero en sistemas de seguridad pero si las personas no las saben implementar, o es un ataque interno, la gravedad del asunto aumenta. Don Carlos González menciono: El factor humano es el más crítico, puede existir un respaldo de todas las cosas y estar bien encriptados se puede gastar mucho en un software y programas pero si esta persona no hay control, no sirve de nada porque este se lleva la información en el pendrive. Y Don Luis Flores: Personas no autorizadas (empleados o terceros) pueden tener acceso directo a los archivos de datos o programas de aplicación utilizados para procesar transacciones permitiéndoles realizar cambios no autorizados a los mismos.

Entonces los mayores ataques a estos sistemas son ataques internos, los que lamentablemente el auditor no puede descubrir a través de una auditoria debido a que esto es natural en cada persona, el hombre no sigue un patrón de conducta como los computadores, sino que simplemente si se ve en la necesidad de hacer algo, lo realiza. Por eso este es el punto y el riesgo mayor que puede tener una auditoria de seguridad de la información.

CONCLUSIONES

A continuación se exponen las conclusiones que se han logrado determinar luego del proceso de investigación llevado a cabo y de acuerdo al análisis de la información recopilada, obtenidas de diferentes fuentes consultadas:

1. Las políticas de seguridad que poseen las entidades financieras son muy similares entre ellas, y tiene el objetivo de dar seguridad a cada transacción comercial que suceda. Estas políticas se encuentran normadas en cada página web de la institución financiera y es de acceso público.

    a. Es necesario dejar en claro para que las políticas de seguridad son iguales para todos los bancos y para que sean efectivas debe existir un compromiso mutuo entre la institución y el cliente, debido a que este recibe recomendaciones de lo que no debe hacer, para que no sea atacado con malware, phishing o similares que son los mayores ataques que reciben los clientes.

2. A través de la educación a cada cliente, la entidades aseguran que las transacciones que se estarán realizando serán de la manera más segura posible, debido a que a través de cibercafé, computadores públicos es donde se encuentran mayores ataques que en vez se realice la transacción de un computador personal y que además se encuentra registrado su IP.

3. Las medidas de seguridad que utilizan los bancos es enorme debido a que estos se encuentran normados por diferentes entes como son la SBFI, SVS, Banco Central, entre otros. Por lo tanto deben cumplir con ciertas normas y parámetros que otras entidades no es necesario cumplir.

4. Debido a lo anterior, y lo recopilado por las entrevistas en el banco deben existir diferentes controles tantos diarios, mensuales que estén constantemente revisando datos de las operaciones que ocurren dentro del banco este trabajo en general lo hace un oficial de cumplimiento, en este contexto es muy difícil que se realicen fraudes a las instituciones financieras debido que ante cualquier anomalía

en el sistema, este entrega una alerta para evitar de esta manera un posible fraude.

5. También cabe destacar las medidas de seguridad interna que proporciona estas instituciones, que teóricamente es a través de perfiles controlan el acceso a los usuarios internos de acuerdo a la base de datos en producción, este encargado llamado oficial de seguridad solo entregara la información requerida a los usuarios de acuerdo a lo que se quiere trabajar, por lo tanto no cualquier persona accede a esta información, por eso es necesario destacar que también este personaje determina la data sensible, que es la información de datos personales, domicilio, que a esta información es difícil de acceder a menos que sea algo muy necesario.

6. Desde el punto de la auditoria uno de sus objetivos principal es la verificación de cada uno de los usuarios de una organización sólo pueda acceder a los recursos que hayan sido autorizados por el propietario de la información impidiendo que personal no autorizado tenga acceso a estos datos. Que los datos sean confidenciales.

7. En conclusión personal se puede determinar que los sistemas utilizados por las instituciones financieras son óptimas para ataques externos porque cuenta con diferentes medidas de seguridad que evita una vulneración en su sistema.
    a. Internamente se protegen a través de perfiles, para que solo algunas personas puedan acceder a la información, siempre cuando estén debidamente autorizadas. Y debido a que la información que viaja entre el cliente y el Banco de a través de un túnel seguro es difícil que se ataque al Banco y ocurra una alteración, es más fácil que se ataque al cliente independientemente. Personalmente el gran problema está en las personas internas las cuales pueden tener acceso a información la cual ellos podrían vender a otros, o sacar provecho de esa información.

8. De acuerdo a las entrevistas realizadas podemos interpretar que uno de los mayores riesgos y que no se consideran dentro de las posibilidades de fraude, son los empleados. El ingreso de datos confidenciales al sistema computacional puede provocar que esta información este concentrada en pocas personas, por lo

que existe una considerable dependencia de estas personas en caso de pérdidas de registros. Por ende se puede hacer un gasto muy significativo en programas de seguridad, pero si no existe las personas adecuadas para instalar estos productos, o una constante vigilancia a que los usuarios no vayan a vender la información a otras empresas de nada servirá. Por eso es necesario que este tema sea tratado con mayor profundidad en las auditorias, porque puede andar todo bien con los sistemas, por eso la conclusión de la tesis quiere hacer hincapié en este tema que la dependencia de ciertos individuos clave, colocan a las organizaciones en una pared donde el informático se puede enojar con los empleadores y puede llegar y borrar toda las transacciones que realizo la empresa durante años, y esto ha ocurrido, y no existe legislación al respecto de que si alguien roba la información o la venda tenga que ser penalizado, no está normado en Chile, es por esto que a los empleados de informática se le deben dar capacitación y actualización que requiere, así como proporcionarle las retribuciones e incentivos justos, para que esto no se vea tentado en querer perjudicar a la entidad.

9. Se podría recomendar que el área informática en una auditoria se le tome mayor importancia porque en estos sistemas se guarda toda la información de una entidad, y que estén las personas indicadas a cargo de esto a través de test psicológicos, conocimiento de trabajos anteriores y buenos salarios. Porque siempre el factor humano es el eslabón más débil. Y para esto debería existir más independencia de los departamentos y no tener una sola persona que tenga el poder absoluto de todo el sistema de información, además de hacer contratos que sean muy explícitos en castigo en la medida de si alguien entrega información a una institución para que pueda saber que le ocurrirá si trata de hacer algo con la información de los clientes. Por eso es fundamental educar mejor a las personas de esta área en la identidad internamente.

GLOSARIO

- Base de datos: (DataBase). Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos. Entre las más conocidas pueden citarse dBase, Paradox, Access y Aproach, para entornos PC, y Oracle, ADABAS, DB/2, Informix o Ingres, para sistemas medios y grandes. (diccionario informático, 2012)
- Bits: (Color Bits). Número de bits asociado con cada pixel que representa su color. Para 16 colores, se utilizan cuatro bits; para 256, ocho bits. (diccionario informático, 2012)
- Encriptar: Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor. Se usa para evitar el robo de información sensible, como números de tarjetas de crédito. Las últimas generaciones de navegadores, como Netscape Navigator 2.0, incluyen sistemas automáticos de encriptación. (diccionario informático, 2012)
- Firewall: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. (diccionario informático, 2012)
- Hacker: Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta. (diccionario informático, 2012)
- Hacking: Es la penetración directa a un sistema informático. El hacking está basado en la escalada de privilegios en un sistema como tal, se puede hacer tanto remota como localmente. (diccionario informático, 2012)
- Https: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Híper Texto, es decir, es la versión segura de HTTP. (Wikipedia, 2012)
- Información sensible: Información sensible es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y

bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. (Wikipedia, 2012)

- Loguin: En el ámbito de seguridad informática, login o logon (en español ingresar o entrar) es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario. (Wikipedia, 2012)
- Malware: Programa maligno. Son todos aquellos programas diseñados para causar daños al hardware, software, redes, como los virus, troyanos, gusanos, nukes. Es un término común que se utiliza al referirse a cualquier programa malicioso. (diccionario informático, 2012)
- Oficial de seguridad de la información: Dentro de una organización, el oficial de seguridad de la información o director de seguridad de la información —en inglés, CISO (chief information security officer: 'oficial principal de seguridad de la información') es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad. (Wikipedia, 2012)
- Pharming: es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. (Wikipedia, 2012)
- Phishing: Es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. Normalmente, se utiliza con fines delictivos enviando SPAM e invitando acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios. (diccionario informático, 2012)

BIBLIOGRAFIA

- ✓ América Economía Intelligence. Obtenida el 20 de diciembre 2012. http://www.einstituto.org/site/novedades/estudio-2012-ecommerce-america-latina/
- ✓ Asociación Iberoamericana de cámaras de comercio. Obtenida el 02 de Junio 2011, de http://www.aico.org/aico/Default.aspx?tabid=1689.
- ✓ Auditoría Informática. Obtenida el 14 de Junio 2012. http://www.eaprende.com/blog/2009/08/11/trabajo-practico-sobre-auditoria-informatica/
- ✓ Banco Internacional. Obtenido el 14 de junio 2012 https://www.bancointernacional.cl/politicas_de_seguridad.html.
- ✓ Cohen y Asín (2009). Tecnologías de información en los negocios (5º edición). México: Mc Graw Hill.
- ✓ Definición de seguridad informática, definicionabc.com. Obtenida el 30 de junio del 2011. http://www.definicionabc.com/tecnologia/seguridad-informatica.php
- ✓ Delitos informáticos en Chile, radio cooperativa. Obtenida el 30 de junio del 2011. http://www.cooperativa.cl/en-2010-chile-acumula-mas-de-500-denuncias-de-delitos-informaticos/prontus_nots/2010-09-26/161036.html
- ✓ Delitos informáticos en Chile, radio cooperativa. Obtenida el 30 de junio del 2011. http://www.cooperativa.cl/individuo-intento-vender-base-de-datos-de-tarjeta-presto/prontus_nots/2011-03-29/102316.html.
- ✓ Diccionario Informático. Obtenida el 26 de Diciembre 2012. http://www.lawebdelprogramador.com/diccionario/
- ✓ Firma electrónica Avanzada, Certisur. Obtenida el 21 de Abril 2011. http://www.certisur.cl/firma-electronica-avanzada.
- ✓ Herramientas y técnicas para la auditoría informática, Obtenida el 14 de Junio 2012. http://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf
- ✓ http://www.acepta.com/Productos/Certificados/SitioWeb.html. Obtenida el 30 de Junio 2011.
- ✓ http://www.finanzasybanca.com/index.php/Guia-de-Banca/concepto-de-banca-electronica.html
- ✓ Internacionales de Auditoría, Declaración de Prácticas de 1013. Obtenida el 02 de Junio 2011 http://web.ifac.org/download/2008_Auditing_Handbook_A250_IAPS_1013.p

- ✓ La Auditoría Obtenida el 14 de junio del 2012 http://www.monografias.com/trabajos34/auditoria-informatica/auditoria-informatica.shtml
- ✓ Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma Nº 19.799. Obtenida 02 Junio 2011. http://www.leychile.cl/Navegar?idNorma=196640
- ✓ O´brien, James (2001, 322) Sistemas de información gerencial (4º edición). Bogotá, Colombia: Mc Graw Hilla.
- ✓ Piattini, Mario (2001). Auditoría informática un enfoque práctico. Pitágoras 1139, Col. Del Valle, 03100 México, DF: Alfaomega grupo editor, S.A. de C.V
- ✓ Seguridad lógica, seguridad informática. Obtenida el 30 de junio del 2011. http://www.segu-info.com.ar/logica/seguridadlogica.htm
- ✓ Superintendencia de bancos e instituciones financieras Chile. Obtenida el 21 de diciembre 2012. http://www.sbif.cl/sbifweb/servlet/Portada?indice=0.0
- ✓ Web Trust. Obtenida el 21 de Abril 2011 http://webtrust.es/webtrust/
- ✓ Wikipedia, Serie 27000. Obtenida el 26 de diciembre 2012. http://es.wikipedia.org/wiki/ISO/IEC_27000-series.

ANEXOS

ENTREVISTAS

NOMBRE: CARLOS GONZÁLEZ
CARGO: INGENIERO INFORMÁTICO, AUDITORA BAKER TILLY CHILE

1) ¿Porque normas se rige el auditor para realizar estos procedimientos?

Respuesta: Dentro de los ISO que son de informática en distintos niveles y enfocados en distintas cosas, hay algunos que son más para administración otros que son más para la parte técnica pero los ISO de la seria 27000 1,2,3,4 así dan una guía bien completa respecto a lo que uno debe revisar para considerar algo tanto un proceso informático general como en particular seguro, (eso se complementa con las IAPS) no sé, (lo que pasa e-commenrce) estas son las reglas que son válidas en todos lados, manejándola y tu equipo de auditores internos o externos que están revisando los sistemas se guían por lo general detectan muchas brecha que en la realidad son y lo que deberían ser. E instituciones públicas que se rigen por el decreto 83 o tratan de el decreto 83 es una resumida de la ISO 27000 2 o 3 es un resumen de 3 o 4 hojas de lo básico que deberían cumplir y no cumplen. (Hay súper poca normativa con respecto a eso) en seguridad y confiabilidad de la información acá es de poca o nula o sea el mismo ejemplo, o sea que tu información sea regalada o vendida, en España son pioneros en eso de crear leyes. Ahora si tú no quieres recibir información tú ahora le colocas que no quieres recibir más correo pero igual ellos pueden saber de qué existe un correo tuyo. Los tipos que manejan el área de informática que por lo general no se toman en cuenta como un área de negocios fundamental, para una empresa lo más importante son sus clientes, que pasa si la información de tus clientes cautivos y tú puedes hacer un historial de eso tú debes cuidarlo, y alguien que hace esto que son los de informática y ellos por querer ganar más plata y no tiene ninguna política en la cual digan que no te puede robar la información, por lo tanto todo lo que pase por los servidores y las personas que están a cargo de esto deberían ser personas que deberían estar más controladas porque ahora nadie te controla son pocas las personas que tienen un auditoria de planta que este controlando,(o sea cada empresa debería tener las políticas de cada una de las brechas que existe) todo lo que te digan que no puedes hacer lo puedes hacer, el informática lo maneja todo, y eso es lo poco valorado acá en Chile, en los países primer mundista igual está más avanzado el tema, (¿Pero igual es peligroso que la información este concentrada en pocas personas?) es mejor pocas que muchas pero esas pocas tienen que ser de

confianza en la empresa, entonces la confianza se la vas dando a través de un sueldo, haciéndole firmar unas cláusulas de que no pueden sacar información y lo demandas si lo está haciendo, y que también allá un auditoria informático, o un ingeniero informático con los conocimientos que trabaje de forma independiente. También lo que he visto mucho en muchas empresas que erróneamente dentro del área informática está el jefe de informática y por al lado tiran al auditor o sea su jefe es el jefe del resto, o sea si algo esta malo su jefe le va a decir que va a estar malo, o sea este debe estar aislados del resto de los informáticos. Lo ideal que alguien que revise.

2) ¿Cuáles son los objetivos principales que busca la seguridad lógica?

Respuesta: Que no se filtre información confidencial, tratar que la información viaje solamente entre las dos entidades, a veces pasa en el caso de wifi y estas en un café y puede haber alguien que este escuchando tu información, que esta informáticamente en modo promiscuo y puede captar todo tu tráfico de internet, entonces su información no está certificado digital https hay varias opciones entre tu persona y el banco, y tu información no viajan encriptados el tipo que está escuchando tu información va a tener toda la información después va a hacer lo que quiera con tu cuenta. La forma es hacer un tipo de túnel de un punto a otro y eso se hace encriptandolo, y esto sería más difícil, hasta el momento nada es totalmente seguro, hay seguridad norteamericana, nada es 100% seguro pero para el normal de la gente certificado http, siempre hay forma de engañar, nada es 100% seguro (la persona de los bancos es imposible que engañen) pero es fácil con phishing de partida, la seguridad pero la gente cae, (es difícil los del banco), se reconocen entre sucursales, tienen líneas dedicadas un cable o una línea óptica de una sucursal a otra, además ya no hay nadie metido ahí y además encriptando la información, entonces tratar de inyectar algo ahí es difícil, los sistemas lo hacen de forma cerrada, sería difícil porque no se puede acceder solamente desde el mismo banco puede acceder al sistema, y ciertos computadores con las autorizaciones correspondientes, a menos que allá un ataque interno eso es peligroso, mas menos el 70%, 80% de los incidentes que trabajan dentro de las mismas instituciones, (o sea por eso necesitan capacitación las personas) hay que informarle que todos están vigilados, acá en Chile no ocurre eso. También hay procedimientos que despiden a alguien y la cuenta sigue activa, y me echan a alguien y me fui enojado, y entre al banco y mi cuenta sigue activa, y los procedimientos deberían ser diferentes, y borrar todas las cuentas, todos sus accesos a todas las cuentas, y de ahí le notifica que te tienes que ir, en el

banco de Chile lo hacen así. Que primero te bloquean y después te echan. Está en las reglas ISO 27003 creó la que me consta, pero en si lugar donde se va aun no le dan de baja a las personas a las cuales ya se despidieron en el sistema informática o muchas veces, de recursos humanos no le informan a informática que alguien se ha ido y por lo tanto no le dan de baja al perfil correspondiente y por lo tanto de sus casas pueden tratar de hacerles la maldad.

3) **El auditor en la seguridad lógica, ¿Qué es lo primero que debemos analizar en esta área?**

Respuesta: Lo normal, o sea revisamos procedimientos, hacemos dos cosas una es revisar procedimientos auditoria y la otra es entregar seguridad para empresas. Primero se debe hacer un levantamientos de los procesos ver cómo influyen y de allí verificarlos, y después te metes en la seguridad lógica, siempre que vas a auditar es lectura de procedimientos y entrevista de personal. O sea a los encargados de cada área, hoy en día se ocupan todas las áreas de negocio de cada empresa y siempre uno solicita hablar con el jefe del área, bueno soy tal persona y vengo a revisar el sistema o la seguridad, pero si tú le dices que vas a hacer una auditoria, e inmediatamente toman resguardo por eso tienes que decirle que tú vas a revisar el sistema y no a las personas. Siempre es la parte teórica antes, piden todos los procedimientos, las políticas de redes políticas de creación de cuenta, respaldo, como son las transacciones entre sistema, depende de la empresa si te dan los contratos de los informáticos, por el mismo tema que te decía de confiabilidad, tiene que haber de los informáticos. (ellos entregan la información) las privadas por lo general son más abiertas en entregarte la información siempre que no le digas que sea plata, y en las públicas es difícil que te entreguen la información (en lo público siempre hay cosas raras) es que en lo público queriendo o no siempre hacen las cosas más lentas, tu les dices en un informe que el servidor tanto tiene tal riesgo y uno le da los pasos a seguir pero ellos no lo toman en cuenta la información entregada, una inercia bien grande en no hacer nada. (De que te echen es difícil como que ellos están confiados) es complicado porque gastan plata en cómo mejorar pero no todos lo implementan.

4) **¿Qué procedimientos realiza el auditor para conocer el riesgo que existe?, y ¿cuáles son sus mayores riesgos al que se ve afectado generalmente?, y ¿Qué recomendaciones se entregan en ese caso?**

Respuesta: Depende de la metodología que se usa, usamos una exposición del riesgo, con una matriz interna, que no compartimos dependiendo del grado de compromiso, la severidad, la frecuencia que ocurren los errores que es más menos algo estándar, se da un cálculo numérico a ciertos riesgos que ya tenemos identificados la base de datos de nosotros es gigante entonces dependiendo el tipo de empresa de las áreas más críticas hacemos un listado y después en base a eso hacemos una las pruebas de verdad, o sea supongamos una revisión en la parte lógica que diga la conexión web en el sistema web de pago no tiene nada encriptado esto es crítico para el negocio ¿Si, es riesgoso para el negocio? sí.

El mayor riesgo es el tema que no hay control dentro de la empresa del informático, y esto conlleva que pueda haber infiltración de la información, modificación de la información. Supongamos a mí no me ha tocado en forma directa pero sé que en lados si ha pasado que el informático veía todos los sistemas incluidos el de remuneración y de a poco él se subía los sueldos todos los meses e iba pasando piola y después estaba ganando casi el doble y como no había nadie que lo controlara, no había nadie de auditoría que se diera cuenta. Si es de a poquitito no se da cuenta, por eso debe existir un control, El factor humano es el más crítico, puede existir un respaldo de todas las cosas y estar bien encriptados se puede gastar mucho en un software y programas pero si esta persona no hay control, no sirve de nada porque este se lleva la información en el pendrive. Los riesgos mayores son internos, pero en el área de lógica, de hacker son pocos, pero lo que tiene más existo y por lo tanto más riesgosos son los ataques internos.

Se dan recomendaciones se modifiquen los contratos, o análisis sicológicos, se debe hacer un análisis de lenguaje corporal ayuda mucho ese tema. Si ves que la persona está muy nerviosa es porque algo debe estar ocultando, o la mano tapando la boca puede que está ocultando algo, y de ahí uno da las recomendaciones al caso y decimos que verifiquen que la personalidad se está acorde al cargo, hacer contratos donde se deje estipulado que esta persona no puede llevarse información para el hogar, y de lo contrario serán penalizados.

5) **¿Cómo se da cuenta de que esta en un sistema o software que no cumplen con las medidas de seguridad necesarias para la entidad?**

Respuesta: se debe tener cierto conocimiento del negocio que está abordando. Si es de comercio electrónico tienes que saber que tiene que haber información entre el cliente tu empresa de la forma más segura posible, que además si tienen algún contrato de servicio

externo de pago que en el fondo tú le dices el cliente quiere comprar esto tú ya ok, comprar con tarjeta de crédito y tú lo mandas a la página del banco y le sale y después internamente el banco te envía la plata a ti, tiene que estar el conocimiento debe estar seguro de que ambas partes de tu empresa al banco, del banco al cliente tiene que haber cierto conocimiento o sino no tienes como revisar, los procedimientos por ejemplo que los certificados debe ser de 120 bits, o 156 bits emitidos por alguna empresa de tal calificación que el servidor va a estar en algún lado con cierta seguridad, uno va a la parte papel, entrevista después la parte lógica lo que vemos que se encuentra riesgoso. Esto va a depender netamente del tipo de negocio.

6) **¿Qué pruebas utiliza la auditoria para comprobar la veracidad de los datos?, y ¿Qué parámetros toman en cuenta para determinar una muestra?**

Respuesta: Normalmente por ejemplo tiene que haber un respaldo semanal, o uno mensual total, se van a guardar en cinta eso es lo que dice el procedimiento, si no hay procedimiento y el tipo hace respaldo cuando se le ocurre tú ya tienes el respaldo tiene que existir esto, es algo bien especifico. Yo tengo que revisar donde se están revisando los archivos, ejemplo el semanal que se halla hecho el ultimo día que corresponde y lo toma como prueba debe haber una comprobación del respaldo se debe analizar que esto sea real y te dicen que están abierto solo algunos tipos de puertos 80, 443 tú tienes que hacer un escaneo de esos puertos estén abiertos. Dependiendo de lo que me entregan y tu detectan de acuerdo a mi experiencia sabes lo que es común que pase uno igual tiene que verificar que lo que se supone que está viendo este bien, este correcto. No sirve un respaldo que no funciona o que quedo hasta la mitad. Por eso tienes que tener las herramientas necesarias, ingeniería social, ejemplo una firma auditoria inglesa coloco a una mujer linda, y comenzar a pedir información a la persona, donde me pueden sacar información, o en facebook uno babea por una persona y tú te haces el lindo y te comienza a sacar información el tipo está jugando con lo que yo pienso que es. O también te doy un chocolate y tú me das tu contraseña y todo esto ha salido aprobado, y donde te pueden sacar información, esa es ingeniería social. Es fundamental ante cualquier sistema. Es aprovecharse de las apariencias. Pueden invertir millones de dólares en sistema y una tipa encachada y te saca la clave. Siempre tiene que haber un control de distintos tipos. Es lo más utilizado en tipo de hacking.

Informática solo va a ver el área de informática, el auditor es quien toma la muestra.

7) **¿Cómo compruebo que solo ciertas personas tengan acceso a la base de datos?, y ¿Cómo reviso esos perfiles y su grado de acceso?**

Respuesta: dependiendo de qué tipo de sistemas de base de datos se esté utilizando. Ver dentro de la lista de usuario y dentro de eso que usuarios tienen acceso a qué base datos, y que estas personas sean reales y que una persona no tiene 3 usuarios y ese usuario a las distintas base de datos acorde a lo que le corresponde, solo el que está a cargo de la base datos es quien tiene toda la claves, y una cosa que mucho pasa es que se comparten las claves los usuarios y eso es lo más complicado porque si tú dices ¿usted comparte su clave? No la tengo yo nomas es algo que se sabe que tiene que decir que no nomas y como se comprueba eso no se puede, es imposible. En los procedimientos debe aparecer que no te puedes meter con otro usuario.

(Como lo haces con los perfiles) Crediticias al área, hablar con el jefe del área, preguntar a su equipo de personas que pueden ser 10 no se, necesito un listado con todos los usuarios o del módulo, ir a recursos humanos necesito un listado de nombres que están trabajando actualmente están trabajando en esa área, por lo general sobran más usuarios de personas que hay, un usuario tenga varios perfiles, o gente que se fue tenga perfiles, que perfil y que acceso tiene cada usuario. Revisando los que tenga más importancia el tema de las claves es imposible. Los perfiles se debe comprobar que es lo que tiene cada uno que hacer. El tema de las claves es imposible, para loguearte en un sistema debe colocar tu dedo, y te logueas y otro hace el servicio. Es normal pero no se debería hacer. En el momento que haya errores puede que tú intencionalmente cometiste un error para que al otro lo reten o lo echen. En el historial me aparece toda la información de las personas que entraron al sistema con el fin de poder ver todo lo que ocurrió.

8) **¿Qué una entidad este acreditada como página segura, en qué medida favorece la auditoria?**

Respuesta: En la auditoria en realidad que hay alguien que ya reviso el tema de seguridad no le da una confianza absoluta, porque alguien hizo una revisión y te dice que es segura, pero como paso en la polar es una cosa que muestran nomas, porque ellos no te iban a revisar a la fuente de la información y no existe una certeza absoluta de que la cosa esta bien ya que te pueden mostrar lo que ellos quieren mostrar, pero por detrás no es así y depende mucho del prestigio que tenga esta acreditadora. (A mí en el banco. me explicaba que siempre tiene que estar acreditadas, independiente de eso ustedes que este o no acreditada ustedes harán el mismo procedimiento) Pero siempre se realizaran

los procedimientos, independiente si está calificado por algún ISO, por lo que hacemos nosotros que hacemos la auditoria algo que se usa es que yo hago reviso un procedimiento y después otro compañero me revisa lo que yo mismo hice (cuando viene que otra firma auditora como lo hacen con la información) es reacción entregarle la información es complicado porque tú ya has trabajado y no le entregaras tu trabajo, pero en los informes tu igual le mandas los resultados que tu encontraste pero tú no entregas toda la metodología, haciendo ingeniería inversa uno igual puede ver cómo trabajan. La empresa auditora termina y uno se lo pide a la institución. No existe contacto entre empresas auditoras. Quien me contrata es quien me pasa la información de años anteriores. También puede ser que ellos te van a querer pasar lo que les conviene. Ejemplo el director de una institución dijo que este año debemos estar cumpliendo con el decreto supremo 83 porque es una institución del 2005 y todos deberían tenerlo pero algunos nomas lo tienen, y el informático debería tenerlo todo listo pero ocurre solo lo bonito es lo que muestra, tú no puedes revisar solo lo que te pasa, y eso también lo que le paso a la polar va en ti que esos resultados estén correctos.

9) **¿Cómo se da cuenta que está ante un fraude?, o ¿Ante una anomalía en el sistema informático?**

Respuesta: Se debe tener conocimiento del negocio, existen cosas lógicas, si entra plata y después hay menos es porque alguien la está sacando pero fraudes económico eso lo vemos en el área de auditoría, pero el área de información que una persona se lleva la información para otro medio, no se sabe que esté haciendo el tipo en su casa, que lo lleve en un pendrive y haga movimientos, pero se debe ver en la base de datos, a través del respaldo me aparecerá la información del historial, el por qué hizo una transacción en la tarde hora que ya no se trabajaba a esa hora. Esto normalmente no se hace, el que está a cargo de este sistema es amo y señor de toda la información. Tiene que haber un administrador pero también alguien que este controlando para saber que se está haciendo. Y normalmente esto no se hace. Una vez la firma tuvo que ser intermediario en una empresa por este lado. Ya que el tipo les dejo la información de hace un año atrás y lo tuvieron que demandar y lo tuvimos que asesorar. Más que fraude es para mal uso. Se tuvieron que juntar todos viendo para que entregara la información de la empresa. En este caso la información de la empresa pierde más. Si tú no tienes beneficios económicos las penas son menores.

10) **En el caso de que exista un fraude que no ha sido detectado por la auditoria, y es detectado posteriormente por diferentes motivos ¿Qué grado de responsabilidad tiene en esos casos la auditoría?**

Respuesta: No es una responsabilidad total, sino que compartida en realidad, al final siempre el socio firma y entrega información con certificado de responsabilidad razonable, cubriéndose en esa área, y no dando una fe absoluta de todo lo que ocurre, diciendo que no la información no es 100% verdadera. Ninguna empresa auditora es a prueba de balas.

NOMBRE: LUIS FLORES
CARGO: GERENTE DE INFORMÁTICA, AUDITORA FORTUNATO Y ASOCIADOS

1) **¿Porque normas se rige el auditor para realizar estos procedimientos?**

Respuesta: Normas de auditoría generalmente aceptadas, incorporando la experiencia del auditor y tomando como referencia las mejores prácticas en seguridad de la información. (Ej. ISO27001)

2) **¿Cuáles son los objetivos principales que busca en la seguridad lógica?**

Respuesta: Uno de los objetivos que busca la seguridad lógica es verificar que cada uno de los usuarios de una organización sólo pueda acceder a los recursos que hayan sido autorizados por el propietario de la información impidiendo que personal no autorizado tenga acceso a éstos.

3) **El auditor en la seguridad lógica, ¿Qué es lo primero que debemos analizar en esta área?**

Respuesta: Uno de los aspectos a evaluar es el procedimiento y políticas de seguridad asociadas principalmente a las altas de usuarios y a los controles existentes para detectar programas maliciosos (Malware) que pudieran afectar la disponibilidad, integridad y confidencialidad de la información manejada por la organización.

4) **¿Qué procedimientos realiza el auditor para conocer el riesgo que existe?, y**

Respuesta: Las principales herramientas que tiene un auditor informático para identificar riesgos existentes en una empresa son, entre otros: la observación directa, cuestionarios, entrevistas, muestreos estadísticos, listas de comprobación o de cumplimiento, etc.
Lo anterior sumado a la utilización de herramientas CAT’s que permiten analizar la información contenida en las bases de datos de los sistemas en evaluación.
Ejemplo de procedimientos de análisis de datos es la revisión utilizando datos de prueba. Se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.

¿Cuáles son sus mayores riesgos al que se ve afectado generalmente?,

Respuesta: Personas no autorizadas (empleados o terceros) pueden tener acceso directo a los archivos de datos o programas de aplicación utilizados para procesar transacciones permitiéndoles realizar cambios no autorizados a los mismos.

Y ¿Qué medidas tomo en ese caso? ¿Influye el factor humano en este riesgo?

Respuesta: Generalmente se recomienda revisar los privilegios de los usuarios vigentes existentes en el (los) sistema(s) y validar que las atribuciones que les han sido asignados para el normal desempeño de sus tareas dentro de la empresa concuerden con las actividades que realizan en la actualidad a objeto de corregir eventuales privilegios que pudieran afectar la integridad y confidencialidad de las transacciones del sistema.

5) **¿Cómo se da cuenta de que esta en un sistema o software que no cumplen con las medidas de seguridad necesarias para la entidad?**

Respuesta: Cuando el sistema en evaluación no cuenta con los controles apropiados, seguimientos de auditoría o registros de actividad (log de transacciones), no cuenta con suficientes validaciones en los datos de entrada, procesamiento interno y datos de salida.

6) **¿Qué pruebas utiliza la auditoria para comprobar la veracidad de los datos?,**

Respuesta: Se pueden realizar pruebas de cumplimiento o de conformidad para comprobar que determinadas normas, procedimientos y/o controles se cumplan. Para este caso si se detectan inconsistencias en los controles, o bien si los controles no existen, se procede a la realización de pruebas sustantivas que permiten dimensionar de mayor forma el impacto de las deficiencias detectadas.

Y ¿Qué parámetros toman en cuenta para determinar una muestra?

Respuestas: En el caso de seleccionar muestras para la revisión informática, en general, se utilizan mecanismos estadísticos que permiten inferir una conclusión en base a una muestra tomada.

No obstante lo anterior, existen muestras no estadísticas que están orientadas principalmente a las operaciones que tienen una probabilidad mayor de error o riesgo.(se basa en muchas ocasiones en la experiencia del auditor)

7) **¿Cómo compruebo que solo ciertas personas tengan acceso a la base de datos?, y ¿Cómo reviso esos perfiles y su grado de acceso?**

Respuesta: Se revisan los privilegios y perfiles existentes en el sistema en evaluación.

Se deben verificar las altas y bajas, contrastando la base de datos de los usuarios vigentes (activos) v/s los empleados con contrato vigente a la fecha de la revisión informática. (Listado entregado generalmente por el departamento de personal).

8) **¿Qué una entidad este acreditada como página segura, en qué medida favorece la auditoria?**

Respuesta: La acreditación o certificados digitales entregan a los usuarios seguridad y confianza en la realización de transacciones electrónicas, permitiéndoles interactuar de manera segura y privada con un sitio web. No obstante lo anterior, esta característica no es una medida que favorezca la auditoría si no que favorece la seguridad de las transacciones de los usuarios de la respectiva página minimizando la probabilidad de incidentes que afecten la seguridad de los sistemas de una organización.

9) **¿Cómo se da cuenta que está ante un fraude?, o ¿Ante una anomalía en el sistema informático?**

Respuesta: La inexistencia o ausencia de controles, establecen una probabilidad muy alta en la ocurrencia de actos de fraude o hechos que pongan en riesgo los pilares fundamentales de la seguridad informática.

Relativo a las anomalías en un sistema informático, la posibilidad de fallo en cualquiera de los elementos que intervienen en el proceso del sistema constituye ciertamente a una fuente de riesgo en la ocurrencia de un fraude. Lo anterior puesto que, estas debilidades o fallas en los sistemas

10) **En el caso de que exista un fraude que no ha sido detectado por la auditoria, y es detectado posteriormente por diferentes motivos ¿Qué grado de responsabilidad tiene en esos casos la auditoría?**

Respuesta: La responsabilidad del auditor dependerá del enfoque de auditoría utilizado. En un enfoque sustantivo (revisión detallada y significativa de todos los aspectos que cubre la seguridad de la información) la responsabilidad del auditor es mucho mayor.

NOMBRE: OSCAR VALLARIN
CARGO: SUBGERENTE DE MEDIOS DE PAGO, BANCO INTERNACIONAL

1) ¿Qué políticas de seguridad utilizan en su sistema bancario?

Respuesta: Algunas se pueden decir, otras que no te las puedo decir, por razones obvias, normalmente en el sistema financiero, en general la asociación de bancos el tema de la seguridad de la transaccionalita vía web, o transaccionalita electrónica es un tema. ¿Por qué? Porque ha ido creciendo no cierto el tema del fraude electrónico ha ido creciendo y eso involucra montos bastantes considerables o sea si uno costo- beneficios no cierto si uno yo creo que con el 10% de lo que se frauda efectivamente podríamos tener medidas bastante de fondo son temas no menor. A ver yo te puedo hablar en el banco nosotros el tema lo tenemos abordados, normalmente a nosotros nos interesa primero que nada que el cliente asuma no cierto que toda transacionalidad en la web tiene un grado de inseguridad, y el banco trata en lo posible de que ese grado de inseguridad se minimice yo no me atrevería a decir que es un 100% porque eso sería una mentira yo creo (siempre va a existir un riesgo) exactamente la idea es colocarle las mayores cortapisa no cierto lo mismo que un asalto a una casa tú le coloca alarmas, le coloca rejas le coloca perros te compra la pistola y así sucesivamente de alguna forma no cierto tratas de minimizar en consecuencia acá en el banco yo te puedo comentar que nosotros estamos tratando que la carretera entre el cliente y el banco sea segura, y que ambos sepamos que estamos hablando con el personaje en cuestión, o sea el cliente este casi 100% seguro de que está hablando con el banco, y que el banco este 100% seguro que está hablando con el cliente. Y eso es un tema no menor porque hoy día hay gente que se mete entremedio no cierto o alguien que puede usufructuar de información no cierto de alguien con el fin de poder defraudarlo. Hoy día existen los fraudes no cierto de a bancos han defraudado

(Al ingresar a la página del banco me fije que también tenían unas medidas de seguridad, que ustedes le daban a entender al cliente cierto, como deberían ser las cosas, ¿esas podríamos decir que esas son como puntos que ustedes están dando?)

Nosotros de alguna forma yo creo que uno de los temas es la comunicación yo creo que es tremendamente relevante que el cliente, a ver hoy día el comercio electrónico se está masificando poco a poco y en consecuencia en la medida de que la gente tiene mayor o menor conocimiento de la carretera que está utilizando, puede estar mayor o menormente expuesta, en consecuencia hoy día no todo el mundo a ver, por ejemplo los jóvenes hoy

día tienen la costumbre de bajar cualquier cosa de internet sin ningún problema no se preocupan de donde vienen ni fotos ni ninguna cosa, y normalmente Hoy día esta gente, ¿Tú conoces los malware? (sí) en consecuencia usan fotos, usan un montón de pequeños no cierto puede ser una pequeña película o algo no cierto en la que tú la bajas que entretenido y además te puso en tu PC un bichito que de alguna forma va a entregar información que necesita la persona que te va a tratar de defraudar. La idea nuestra es esa es poder detectar que desde donde tú te estás comunicando no tiene ninguna cosa extraña, nosotros tenemos esa herramienta, con el fin de que nuestros clientes la puedan bajar a su PC, ya que están definidas a su IP. En consecuencia cuando el cliente quiera hacer transferencias con el banco él va a decir usare el computador de mi empresa y el de mi casa (o sea como ustedes ya tienen definido el IP entonces yo en el caso de que fuera a un ciber café o estuviese en el extranjero y quisiese hacer una transacción no se va a poder). Yo te voy a decir por seguridad esto tú lo estás haciendo de otra a lo mejor tomare una segunda o tercera medida efectivamente eres tú o te pondré una tercera clave y por esta vez te la voy a hacer desde España ¿Por qué? Porque estoy acá ya pero la idea es de alguna forma yo creo que esto tiene que ser compartido entre el cliente y el banco, el banco tiene que entregarle las mayores herramientas para que el cliente se sienta seguro cuando está trabajando con el banco pero hay que tomar en cuenta no cierto que el cliente también tiene un grado de responsabilidad en el sentido como bien tú dices no irse a un ciber café no hacer una transferencia monetaria porque normalmente la mayoría de los fraudes se hacen en los ciber café es más las transferencias telefónicas también son peligroso. (¿Entonces uno recomendaría hacerlo siempre la transferencia del mismo computador?). La idea es que ambos sepamos yo banco sepa que el cliente el que esta, no cierto porque él me definió que lo hacía desde esa dirección etc. Y viceversa él sabe no cierto que cuando él se comunica con el banco efectivamente es con el banco y no está con una página que puede ser un phishing o algo así. De hecho nosotros tenemos antiphishing y detectamos y las tratamos de botar y gracias a Dios no hemos tenido ningún siniestro.

2) ¿Cuáles son los mayores ataques que recibe el sistema bancario en línea, y de que se trata este ataque?, y ¿Cómo combaten los phishing?

Respuesta: Hoy día no cierto el tema de transferencia electrónica, transferencias de dinero los famosos malware, te colocan una semillitas en tu pc, de alguna forma te empiezan a detectar la información clave de tus tarjeta coordenada y un montón de cosas,

eso en el sistema financiero, y en el banco propiamente tal no hemos tenido fraudes electrónicos. (¿Pero ustedes no reciben ataques porque yo investigaba que lo phishing son el mayor ataque que reciben los bancos?) hoy día por ejemplo al banco a ver hay algunos clientes que nos han dicho mira me salió que me están pidiendo ustedes una información como por ejemplo las tarjetas coordenadas, lógicamente ellos nos informa pero es porque a sus PC le han puesto un malware, a nosotros como banco aun no nos han hecho phishing porque el banco no puede tener ningún elemento que puedan atacarlo, nosotros tenemos un antiphishing, y en consecuencia sabemos en forma inmediata cuando alguien va a copiar una página, y se atacara esa página, porque normalmente te va a atacar desde Zambia de cualquier país menos Chile pero existen herramientas que permiten hacer este tipo de cosas pero gracias a Dios tenemos y no todos los bancos lo tienen pero poco a poco se está masificando que le tienes que dar seguridad al cliente porque cuando se conecte con el banco (yo creo que cuando uno va a hacer una transacción lo más importante es la seguridad). Uno de los temas que nos preocupa a nosotros a ver, normalmente no quiero estigmatizar pero con la cuenta Rut, hubo problemas serios porque para tener una cuenta Rut lo único que se sabe es el Rut, y nada más. En consecuencia lo ideal es que el banco conozca a cada cliente que está detrás que tiene un ingreso quien el fin de evitar este tipo de situaciones, pero verdaderamente la banca está preocupada tú has escuchado que en el mismo metro te han dicho que no te roben el sueldo, pero en general la banca está preocupada de los movimiento electrónicos, si uno ve el número de cheques hoy va en disminución los usos de uso de tarjeta de crédito y de débito crece pero muy poco, pero lo crece en manera es potencial son las transferencia y todo lo electrónico crece con una rapidez, hoy día, antiguamente tu hacías una transacción electrónicamente te pedían claves, pero hoy con webpay y yo te identifico a ti con tarjeta coordenada o toquen es identificar quien hace la transacción, para evitar problemas.

3) ¿Qué ocurre cuando se pierde información de la transacción por cualquier motivo, como se respalda la información?

Respuesta: En todo sistema hay esta contingencia y está el riesgo operacional que nosotros llamamos todo esto esta corre en dos sistemas paralelos que toda transaccionalidad está respaldada, se pierde en producción pero está en otro lado, eso es por norma todo se encuentra normado, no puede perder toda la información, todos tienen los firewall correspondientes, con el fin de evitar que a la base de datos de un banco

alguien pueda llegar a hacer alguna maldad, y cada banco está muy normado quienes pueden acceder no cierto a esa información mediante protocolos bien estrictos y perfiles no cualquiera puede ingresar a la base de datos del banco, o sea eso es un hecho, yo no tengo ingreso a la base de datos. De acuerdo a perfiles yo puedo tener accesos a la información que está en la base de datos, pero de ahí a ingresar a la base de datos no, son cosas totalmente distintas.

4) ¿Cómo restringe los accesos de usuarios?, y ¿Cómo garantiza que la información entregada por el usuario sea confiable, y como se pueden dar cuenta cuando estas ante un intento de delito informático?

Respuesta: A través de perfiles, personas que por alguna razón esto está muy controlado el acceso de base de datos en producción, por oficiales de seguridad, que restringen esa capacidad de poder entregar, por ejemplo gente que está haciendo desarrollo, no tiene acceso a base de datos en producción sino que a base de datos en desarrollo, con el fin de que puedan hacer los desarrollos a gente externa o a proveedores externos que puede pasar a data a donde pueden hacer simulaciones, etc. Pero la data en producción esta tremendamente controlada, muy controlada eso es básico o sino cualquiera se lleva la base de datos para la casa.

¿Cómo garantiza que la información entregada por el usuario sea confiable, y como se pueden dar cuenta cuando estas ante un intento de delito informático?

Estas son dos cosas distintas como compruebo datos a ver aquí se comprueba a través de data sensible de un cliente, por ejemplo domicilio legal, donde vive normalmente tiene una fechas de vencimiento, esto se tiene que ratificar durante un años, se controla esto cada cierto tiempo en la página privada, no en la pública, o sea la persona que sé que entro con clave y yo ya sé que es el cliente (en el caso de alguna anomalía que comienza a dar datos que no corresponde) En el caso de cambio de domicilio se verifica que esto sea real, por contactabilidad por que según norma yo debo enviar información una vez al mes, por si tengo que cobrarle tengo que tener teléfono de contacto email, toda esa información que es sensible hay que ir controlándola, con mediciones de un ejecutivo. Medir la contactabilidad de una cartera de un ejecutivo por lo tanto medimos la contatabilidad de una cartera, y esto se mide enviando una cartolas, llamándolo por teléfono le mando dividendos hipotecarios los cupones de pago de las cuotas en consecuencia si un correo me sale devuelto comienzo a marcar este cliente no es

contactable porque la dirección que tengo ya no es por lo tanto esto es una tarea del ejecutivo de cuenta. Con el fin de tener la información muy actualizada.

¿Cómo se dan cuenta de que están ante un delito informático?

Existe aplicaciones que te dan esta información, en línea hay aplicaciones que me permiten detectar patrones de comportamiento del cliente, esto tiene notas de acuerdo a como se comporta el cliente. Ej. El cliente está haciendo un avance en efectivo en cajero automático en Viña y a los 5 minutos lo está haciendo en Santiago, es algo imposible, esto es un sistema computarizado. La idea es detectar la transacción casi en línea, y se trabaja para que antes de la autorización poder verla para denegar la autorización para tomar las medidas necesarias pero hacerlo antes, queremos meter toda lógica, a mayor cantidad de patrones se tiene, disminuye la cantidad de probabilidades que nos hagan un fraude, nos manda el sistema un alerta, y se cuenta al cliente Porque si una persona va siempre a sacar plata a las 6 de la tarde y de repente lo hace más tarde existe un patrón que cambia y me aparece una alerta que me tira. Para saber si es el quien lo hace u otra persona, es necesario la contactabilidad, todo es un todo.

5) ¿Quién asigna las contraseñas en el sistema, inicialmente y sucesivamente y está en que sistema se encuentran?

Respuesta: El oficial de seguridad, que se encarga de todas las aplicaciones del banco, y el entrega de acuerdo a instrucciones de la jefatura definidas a cada persona definidas de que tenga o no acceso a una determinada aplicación. Las aplicaciones entregan datos, los datos se manejan en la base de datos, puedo acceder a datos, pero acceder al dato bruto en un banco es algo totalmente limitado en un banco.

6) Se sabe que existen sellos de seguridad, firma electrónica, ¿Ustedes trabajan con algunos de estos instrumentos?

Respuesta: Usamos segunda claves. Cada una de nuestras páginas están certificadas como segura, todos los bancos deben tenerlo. No existe ningún banco que no tenga esas certificaciones.

7) **Verificar integridad interna de los sistemas ¿Con que frecuencia realizan controles de externos a sus sistemas bancarios? ¿Y cómo los realizan, y que agentes son estos?**

Respuesta: Los controles son internos, viene una persona interna que es el oficial de cumplimiento, estos controles se hacen todos los días, transaccionalmente, el ve todos los días datos y datos, ejemplo una persona que deposita muchas personas que deposita muchas monedas, o mucho billetes de Luca, esta información llama la información se saca un patrón en el caso, hay leyes que definen que el banco debe conocer al cliente y de donde vienen sus flujos. El que dedica a las drogas debe tener un lugar guardada el dinero, si viene alguien de la calle, y me pide abrir una cuenta, y se debe saber en qué trabaja, y de donde puede sacar tanta plata. Por eso debe haber consistencia en la información.

8) **Factor humano, ¿En qué dirección se debe orientar al personal para que este sea de confianza debido a que se trabaja con información tan relevante?**

Respuesta: Hay mucha data que es sensible, el oficial de seguridad y la gente de contraloría define cual es la data sensible del cada producto, está en la base de datos totalmente encriptada. Si alguien quiere exportarla va a tener la información, pero no en vivo, en bruto, solo va a ver unas x, con el fin de mientras la información dentro del sistema pueda ser vista fluidamente, pero si quiero exportarla esta encriptada, que son los datas sensibles. Contraloría decide cual es las datas sensibles.

9) ¿Ha existido casos de fraude en este Banco? ¿Cómo que casos?

Respuesta: No existen fraudes, ellos estaban haciendo un cambio en la web y tenían que copiar su sistema estático, para poder avanzar pero el sistema inmediatamente echo a bajo lo que se estaba haciendo, por lo menos funciona.

10) ¿Responsabilidad?

Siempre tiene que haber una investigación. Una investigación completa, aquí hay de todo, Como en el caso que el hijo le saque la tarjeta al papa, y le hace la transferencia correspondiente, el tema de la seguridad es compartida, el cliente también tiene que cuidar los elementos que le entregan el banco, la tarjeta es personal. Son cosas personales, no se pueden entregar porque se prestan para situaciones complicadas. ¿En el caso de fraude externo? En el caso externo siempre se trata de cerrar estas puertas,

con el fin que el sistema financiero sea lo más seguro, tratar de tener una carretera exclusiva y no entra nadie, hoy todos las transferencia se hacen en carreteras exclusivas del banco, no es por ejemplo una transacción cuando me meto una carretera publica, de mi casa al banco, ahí cuando existe problemas, pero información de carretera privada hay no existe riesgos. Cuando salen a terceros son carreteras RBI (Inspección basada en riesgos) se mandan información de banco a banco, cuando entra un cliente al banco hay donde hay que darle mayor seguridad.

NOMBRE: LUIS MARCHANT
CARGO: ANALISTA SEGURIDAD DE LA INFORMACIÓN, BANCO DE CHILE

1) ¿Qué políticas de seguridad utilizan en su sistema bancario?
Respuesta: Están las políticas del banco, las normativas de seguridad de información, están basada en la normas internacionales en la ISO 27000, son información interna, todo o que está en la página es información entregada al público difusión de buenas prácticas, pero la políticas es interna.

2) ¿Cuáles son los mayores ataques que recibe el sistema bancario en línea, y de que se trata este ataque?, y ¿Cómo combaten los phishing?
Respuesta: Phishing, pharming, temas de ese tipo buscando fraude a las transferencias electrónicas. Educación, normalmente no podemos interferir en los PC de los clientes, si reciben correos infectados, más que nada educativo, niveles de educación, y niveles de autenticación, dinámica con claves, todos con niveles. Educando al cliente con los riesgos, y las cosas que no debe hacer.

3) ¿Qué ocurre cuando se pierde información de la transacción por cualquier motivo, como se respalda la información?
Respuesta: Desconozco esa información, pero cuando las transacciones no se terminan se deshacen. Hay investigaciones, técnicamente hay respaldan, de todos los movimientos.

4) ¿Cómo restringe los accesos de usuarios?, y ¿Cómo garantiza que la información entregada por el usuario sea confiable, y como se pueden dar cuenta cuando estas ante un intento de delito informático?
Respuesta: Se le hacen cambiar periódicamente las claves, con mayúscula, minúsculas de las claves, y además otros niveles de autenticación claves dinámica, que la toquen un tonel, es un dispositivo que entregan los bancos con una clave temporal y única. Esta entrega una clave temporal y con esta se pide para meterse a la cuenta, esta se obtiene cuando se contrata el sistema. Y también se entrega clave a su celular. Combinación de varias claves. Enrolar su teléfono.
Por controles internos, en el banco puede alertar temas de potenciales fraudes, que apuntan a esto, e información de los clientes, a través de canales, de ellos mismos.

Existen normativas internacionales que exigen estas cosas. En contraloría. Aplican toda la normativa internacional del lavado de dinero.

5) ¿Quién asigna las contraseñas en el sistema, inicialmente y sucesivamente y está en que sistema se encuentran?

Respuesta: Área del banco que se dedica a entregar las cuentas, y esta todo normado, está definido según el cargo el perfil que adquiere, es un área que entrega los privilegios en el banco de lo que se necesita.

6) Se sabe que existen sellos de seguridad, firma electrónica, ¿Ustedes trabajan con algunos de estos instrumentos?

Respuesta: Existen sellos, de seguridad, todo está controlado, del desarrollo.

7) Verificar integridad interna de los sistemas ¿Con que frecuencia realizan controles de externos a sus sistemas bancarios? ¿Y cómo los realizan, y que agentes son estos?

Respuesta: Controles permanentes, va a depender la necesidad de la información su importancia pueden ser diarios, mensuales, depender del riesgo tanto infraestructura como información. Externamente existen auditorias, la Intendencia exige que hayan ciertas auditorias las cuales deben estar normadas, auditorías internas y externas.

8) Factor humano, ¿En qué dirección se debe orientar al personal para que este sea de confianza debido a que se trabaja con información tan relevante?

Respuesta: Con educación, capacitación, y controles en los procesos, y compromisos hechos por los usuarios.

9) ¿Ha existido casos de fraude en este Banco? ¿Cómo que casos?

Creo que sí, no creo que algún banco no sufra de esto.

10) ¿La responsabilidad?

Esta normada, va a depender de la investigación.

Categorías enfoque de sistema bancario

Oscar Vallarin; Subgerente de medios de pago; Banco International

Juan Marchant; Analista seguridad de la información; Banco de Chile

- **Políticas de seguridad:**
  - Con el cliente

Oscar Vallarin: nada que el cliente asuma no cierto que toda transacionalidad en la web tiene un grado de inseguridad, y el banco trata en lo posible de que ese grado de inseguridad se minimice yo no me atrevería a decir que es un 100% porque eso sería una mentira yo creo (siempre va a existir un riesgo) exactamente la idea es colocarle la más mayores cortapisa. En el banco yo te puedo comentar que nosotros estamos tratando que la carretera entre el cliente y el banco sea segura, y que ambos sepamos que estamos hablando con el personaje en cuestión, ósea el cliente este casi 100% seguro de que está hablando con el banco, y que el banco este 100% seguro que está hablando con el cliente. La idea nuestra es esa es poder detectar que desde donde tú te estás comunicando no tiene ninguna cosa extraña. Esto tiene que ser compartido entre el cliente y el banco, el banco tiene que entregarle las mayores herramientas para que el cliente se sienta seguro cuando está trabajando con el banco pero hay que tomar en cuenta no cierto que el cliente también tiene un grado de responsabilidad en el sentido como bien tú dices no irse a un ciber café no hacer una transferencia monetaria. Lo ideal es que el banco conozca a cada cliente que está detrás que tiene un ingresos con el fin de evitar este tipo de situaciones.

Estas son dos cosas distintas como compruebo datos a ver aquí se comprueba a través de data sensible de un cliente, por ejemplo domicilio legal, donde vive normalmente tiene una fechas de vencimiento, esto se tiene que ratificar durante un años, se controla esto cada cierto tiempo en la página privada, no en la pública, ósea la persona que sé que entro con clave y yo ya sé que es el cliente (en el caso de alguna anomalía que comienza a dar datos que no corresponde) En el caso de cambio de domicilio se verifica que esto sea real, por contactabilidad por

que según norma yo debo enviar información una vez al mes, por si tengo que cobrarle tengo que tener teléfono de contacto email, toda esa información que es sensible hay que ir controlándola, con mediciones de un ejecutivo. Medir la contactabilidad de una cartera de un ejecutivo por lo tanto medimos la coctatabilidad de una cartera, y esto se mide enviando una cartolas llamándolo por teléfono le mando dividendos hipotecarios los cupones de pago de las cuotas en consecuencia si un correo me sale devuelto comienzo a marcar este cliente no es contactable porque la dirección que tengo ya no es por lo tanto esto es una tarea del ejecutivo de cuenta. Con el fin de tener la información muy actualizada.

Juan Marchant: Están las políticas del banco, las normativas de seguridad de información están basada en las normas internacionales en la ISO 27000, son información interna, todo o que está en la página es información entregada al público difusión de buenas prácticas, pero las políticas es interna

- Con el sistema bancario

Oscar Vallarin: En todo sistema hay esta contingencia y está el riesgo operacional que nosotros llamamos todo esto esta corre en dos sistemas paralelos que toda transacionalidad está respaldada, se pierde en producción pero está en otro lado, eso es por norma todo se encuentra normado, no puede perder toda la información, todos tienen los firewalls correspondientes, con el fin de evitar que a la base de datos de un banco alguien pueda llegar a hacer alguna maldad, y cada banco está muy normado quienes pueden acceder no cierto a esa información mediante protocolos bien estrictos y perfiles no cualquiera puede ingresar a la base de datos del banco, ósea eso es un hecho, yo no tengo ingreso a la base de datos

Juan Marchant: cuando las transacciones no se terminan se deshacen

- **Medidas de seguridad:**
  - Con el cliente

Oscar Vallarin: nosotros tenemos esa herramienta, con el fin de que nuestros clientes la puedan bajar con a su PC, ya que esta están definidas a su IP. En consecuencia cuando el cliente quiera hacer transferencias con el banco él va a decir usare el computador de mi empresa y el de mi casa (o sea como ustedes ya tienen definido el IP entonces yo en el caso de que fuera a un ciber café o estuviese en el extranjero y quisiese hacer una transacción no se va a poder). Yo te voy a decir por seguridad esto tu lo estás haciendo de otra a lo mejor tomare una segunda o tercera medida efectivamente eres tu o te pondré una tercera clave y por esta vez te la voy a hacer desde España.

Juan Marchant: Educación, normalmente no podemos interferir en los PC de los clientes, si reciben correos infectados, más que nada educativo, niveles de educación, y niveles de autenticación, dinámica con claves, todos con niveles. Educando al cliente con los riesgos, y las cosas que no debe hacer
Se le hacen cambiar periódicamente las claves, con mayúscula, minúsculas de las claves, y además otros niveles de autenticación claves dinámica, que la toquen un tonel, es un dispositivo que entregan los bancos con una clave temporal y única. Esta entrega una clave temporal y con esta se pide para meterse a la cuenta, esta se obtiene cuando se contrata el sistema. Y también se entrega clave a su celular. Combinación de varias claves. Enrolar su teléfono.

- Con el sistema bancario

Oscar Vallarin: A través de perfiles, personas que por alguna razón esto está muy controlado el acceso de base de datos en producción, por oficiales de seguridad, que restringen esa capacidad de poder entregar

- **Ataques**
  - Principales ataques

Oscar Vallarin: Hoy día no cierto el tema de transferencia electrónica, transferencias de dinero los famosos malware, te colocan una semillitas en tu PC, de alguna forma te empiezan a detectar la información clave de tus tarjeta coordenada y un montón de cosas, eso en el sistema financiero. es porque a sus PC le han puesto un malware, a nosotros como banco aun no nos han hecho phishing porque el banco no puede tener ningún elemento que puedan atacarlo, nosotros tenemos un antiphishing, y en consecuencia sabemos en forma inmediata cuando alguien va a copiar una página, y se atacara esa página, porque normalmente te va a atacar desde Zambia de cualquier país menos Chile pero existen herramientas que permiten hacer este tipo de cosas pero gracias a Dios tenemos y no todos los bancos lo tienen.

Juan Marchant: phishing, pharming, temas de ese tipo buscando fraude a las transferencias electrónicas

- Como me percato de ataques

Oscar Vallarin: Existe aplicaciones que te dan esta información, en línea hay aplicaciones que me permiten detectar patrones de comportamiento del cliente, esto tiene notas de acuerdo a como se comporta el cliente. Ejemplo el cliente está haciendo un avance en efectivo en cajero automático en viña y a los 5 minutos lo está haciendo en Santiago, es algo imposible, esto es un sistema computarizado. La idea es detectar la transacción casi en línea, y se trabaja para que antes de la autorización poder verla para denegar la autorización para tomar las medidas necesarias pero hacerlo antes, queremos meter toda lógica, a mayor cantidad de patrones se tiene, disminuye la cantidad de probabilidades que nos hagan un fraude, nos manda el sistema un alerta, y se cuenta al cliente

Juan Marchant: Por controles internos, en el banco puede alertar temas de potenciales fraudes, que apuntan a esto, e información de los clientes, a través de canales, de ellos mismos.

- **Controlador:**
  - Quien asigna estos

Oscar Vallarin: El oficial de seguridad, que se encarga de todas las aplicaciones del banco, y el entrega de acuerdo a instrucciones de la jefatura definidas a cada persona definidas de que tenga o no acceso a una determinada aplicación. Los controles son internos, viene una persona interna que es el oficial de cumplimiento, esto controles se hacen todos los días, transaccionalmente, el ve todos los días datos y datos.

Juan Marchant: Área del banco que se dedica a entregar las cuentas, y esta todo normado, está definido según el cargo el perfil que adquiere, es un área que entrega los privilegios en el banco de lo que se necesita.
Controles permanentes, va a depender la necesidad de la información su importancia pueden ser diarios, mensuales, depender del riesgo tanto infraestructura como información. Externamente existen auditorias, la intendencia exige que hayan ciertas auditorias las cuales deben estar normadas, auditorías internas y externas

- Factor humano

Oscar Vallarin: Hay mucha data que es sensible, el oficial de seguridad y la gente de contraloría define cual es la data sensible del cada producto, esa está en la base de dato totalmente encriptado. Si alguien quiere exportarla va a tener la información, pero no en vivo, en bruto, solo va a ver unas x o garabatos, con el fin de mientras la información dentro del sistema pueda ser vista fluidamente, pero si quiero exportarla esta encriptado, que son los datas sensibles

Juan Marchant: Con educación, capacitación, y controles en los procesos, y compromisos hechos por los usuarios.

Categorías Enfoque de Auditoría:

Carlos González; Ingeniero Informático; Baker Tilly

Luis Flores; Gerente de Informática; Fortunato y Asociados

- **Normativa:**

Carlos González: dentro de los ISO que son de informática en distintos niveles y enfocados en distintas cosas, hay algunos que son más para administración otros que son más para la parte técnica pero los ISO de la seria 27000 1, 2, 3,4 así dan una guía bien completa respecto a lo que uno debe revisar para considerar algo tanto un proceso informático general como en particular seguro. E instituciones públicas que se rigen por el decreto 83 que es una resumida de la ISO 27000 2 o 3 es un resumen de 3 a 4 hojas de lo básico que deberían cumplir y no cumplen. En seguridad y confidencialidad de la información acá es de poca o nula.

Luis Flores: Normas de auditoría generalmente aceptadas, incorporando la experiencia del auditor y tomando como referencia las mejores prácticas en seguridad de la información. (Ejemplo: ISO 27001)

- **Procedimientos:**
  - ¿Qué se busca?

Carlos González: Que no se filtre información confidencial, tratar que la información viaje solamente entre las dos entidades. La forma es hacer un tipo de túnel de un punto a otro y eso se hace encriptandolo, y esto sería más difícil, hasta el momento nada es totalmente seguro. También hay procedimientos que despiden a alguien y la cuenta sigue activa, y me echan a alguien y me fui enojado, y entre al banco y mi cuenta sigue activa, y los procedimientos deberían ser diferentes, y borrar todas las cuentas, todos sus accesos a todas las cuentas, y de ahí le notifica que te tienes que ir, en el banco de chile lo hacen así. Que primero te bloquean y después te echan.

Luis Flores: Uno de los objetivos que busca la seguridad lógica es verificar que cada uno de los usuarios de una organización sólo pueda acceder a los recursos que hayan sido autorizados por el propietario de la información impidiendo que personal no autorizado tenga acceso a éstos.

- ¿Qué se analiza?

Carlos González: lo normal, ósea Revisamos procedimientos, hacemos dos cosas una es revisar procedimientos auditoria y la otra es entregar seguridad para empresas. Primero se debe hacer un levantamientos de los procesos ver cómo influyen y de allí verificarlos, y después te introduces en la seguridad lógica, siempre que vas a auditar es lectura de procedimientos y entrevista de personal. Siempre es la parte teórica antes, piden todos los procedimientos, las políticas de redes políticas de creación de cuenta, respaldo, como son las transacciones entre sistema, depende de la empresa si te dan los contratos de los informáticos, por el mismo tema que te decía de confidencialidad, tiene que haber de los informáticos.
Yo tengo que revisar donde se están revisando los archivos, ejemplo el semanal que se halla hecho el ultimo día que corresponde y lo toma como prueba debe haber una comprobación del respaldo se debe analizar que esto sea real y te dicen que están abierto solo algunos tipos de puertos 80, 443 tú tienes que hacer un escaneo de esos puertos estén abiertos.

Luis Flores: Uno de los aspectos a evaluar es el procedimiento y políticas de seguridad asociadas principalmente a las altas de usuarios y a los controles existentes para detectar programas maliciosos (Malware) que pudieran afectar la disponibilidad, integridad y confidencialidad de la información manejada por la organización.

- **Riesgos:**
  - Procesos

Carlos González: se reconocen entre sucursales, tienen líneas dedicadas un cable o una línea óptica de una sucursal a otra, además ya no hay nadie metido ahí y además encriptado la información, entonces tratar de inyectar algo ahí es difícil, los sistemas lo hacen de forma cerrada, sería difícil porque no se puede acceder solamente desde el mismo banco puede acceder al sistema, y ciertos computadores con las autorizaciones correspondientes, a menos que allá un ataque interno ESO ES PELIGROSO, mas menos el 70% o 80% de los incidentes es de los que trabajan dentro de las mismas instituciones.

También puede ser que ellos te van a querer pasar lo que les conviene (institución auditada) depende de la metodología que se usa, usamos una exposición del riesgo, con una matriz interna, que no compartimos dependiendo del grado de compromiso, la severidad, la frecuencia que ocurren los errores que es más menos algo estándar, se da un cálculo numérico a ciertos riesgos que ya tenemos identificados la base de datos de nosotros es gigante entonces dependiendo el tipo de empresa de las aéreas más críticas hacemos un listado y después en base a eso hacemos una las pruebas de verdad, ósea supongamos una revisión en la parte lógica que diga la conexión web en el sistema web de pago no tiene nada encriptado esto es crítico para el negocio. El mayor riesgo es el tema que no hay control dentro de la empresa del informático, y esto conlleva que pueda haber infiltración de la información, modificación de la información.

Luis Flores: la utilización de herramientas CAT's que permiten analizar la información contenida en las bases de datos de los sistemas en evaluación.

Ejemplo de procedimientos de análisis de datos es la revisión utilizando datos de prueba. Se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.

- Factor Humano:

Carlos González: todo lo que te digan que no puedes hacer lo puedes hacer, el informático lo maneja todo, y eso es lo poco valorado acá en Chile, en los países primermundista igual esta mas, más avanzado el tema. Es mejor pocas que muchas personas pero esas pocas tienen que ser de confianza en la empresa, entonces la confianza se la vas dando a través de un sueldo, haciéndole firmar unas cláusulas de que no pueden sacar información y lo demandas si lo está haciendo, y que también allá un auditor informático, o un ingeniero informático con los conocimientos que trabaje de forma independiente.
El factor humano es el más crítico, puede existir un respaldo de todas las cosas y estar bien encriptados se puede gastar mucho en un software y programas pero si esta persona no hay control, no sirve de nada porque este se lleva la información en el pendrive. Los riesgos mayores son internos, pero en el área de lógica, de hacker son pocos, pero lo que tiene más existo y por lo tanto más riesgosos son los ataques internos.

Luis Flores: Personas no autorizadas (empleados o terceros) pueden tener acceso directo a los archivos de datos o programas de aplicación utilizados para procesar transacciones permitiéndoles realizar cambios no autorizados a los mismos.

- Recomendaciones:

Carlos González: Se dan recomendaciones se modifiquen los contratos, o análisis sicológicos

Luis Flores: se recomienda revisar los privilegios de los usuarios vigentes existentes en el (los) sistema(s) y validar que las atribuciones que les han sido asignados para el normal desempeño de sus tareas dentro de la empresa concuerden con las actividades que realizan en la actualidad a objeto de corregir eventuales privilegios que pudieran afectar la integridad y confidencialidad de las transacciones del sistema.