INGENIERIA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero

Luis Eduardo Patiño Durán[1]

Universidad Pontificia Bolivariana
Bucaramanga, Colombia
lepaduran@hotmail.com

Resumen

Cualquiera que sea la actividad o ubicación en la empresa, el trabajo de cada empleado llega a los clientes en forma de servicios; dicho servicio se basa en atributos y lo convierten en una guía para orientar los modos de actuación de cada uno de los colaboradores, frente a clientes y compañeros. Con la actualización de la banca que va de la mano con la globalización y las nuevas tecnologías, se han diversificado los canales transaccionales, condición que aumenta los riesgos de la seguridad y crea nuevos escenarios para cometer delitos financieros. Para prevenir la mayoría de ataques externos se invierte en tecnología, pero prevenir ataques internos y de ingeniería social resulta un poco más complejo para cualquier organización; una posible solución es capacitar constantemente a los colaboradores, concientizarlos, sensibilizarlos realmente de lo que implica para la entidad y para si mismo la pérdida de información confidencial. Entonces, resulta importante conocer algunos conceptos que ayuden a identificar los ataques, los delincuentes, los medios utilizados para extraer datos y por supuesto ejemplos que hagan más palpable y real la Ingeniería Social en nuestro medio y diario actuar. Al final del documento se darán algunas recomendaciones para evitar ser victimas de este tipo de ataques.

Palabras claves

Fundamentos del servicio, confidencialidad, ingeniería social, ataque, confianza.

[1] Candidato a Especialista en Seguridad Informática, Universidad Pontificia Bolivariana Seccional Bucaramanga.

Abstract

Whatever the activity or the business location, the work of each employee reaches customers in the form of services; the service is based on attributes and make it a guideline for the modes of action of each of the partners, to customers and colleagues. With the upgrade of the bank that goes hand in hand with globalization and new technologies, channels have diversified transactional, condition that increases safety risks and creates new scenarios to commit financial crimes. To prevent external attacks most invested in technology, but to prevent internal attacks and social engineering is a little more complex for any organization; one solution is to constantly train employees, and sensitize them aware really of what it means for the company and for himself the loss of confidential information Then, it is important to understand some concepts that help to identify attacks, offenders, the means used to extract data and examples of course do more palpable and real social engineering in our environment and daily action. At the end of the document will give some recommendations to avoid being victims of such attacks.

Keywords:
Fundamentals of service, confidentiality, social engineering, attack, trust.

1. Introducción

Los cambios que sufren las organizaciones, las reestructuraciones, los avances tecnológicos, la competencia, las regulaciones y la demanda de clientes, permite observar los riesgos y retos a los que se encuentran expuestas. La mayoría son controlados y/o contrarrestados con inversión en equipos, tecnología y aun creemos que es suficiente, pero realmente estamos descuidando una técnica peligrosa, difícil de identificar, que ataca “el eslabón más débil” de la cadena, como es la ingeniería social, usada para obtener información principalmente mediante engaños [1].

Las entidades del sector financiero en su mayoría ofrecen los mismos productos y canales de servicio a sus usuarios, con tasas de interés muy semejantes, razón por la cual se crea la necesidad de utilizar nuevas estrategias que ayuden a fidelizar y captar un mayor número de clientes, una de ellas, es la atención y el servicio. El concepto de servicio está basado principalmente en cinco atributos, amabilidad, agilidad, facilidad, claridad y cumplir lo prometido [2], todos ellos vulnerables a la Ingeniería Social.

¿Por qué es tan efectiva la ingeniería social? ¿Es necesario ser un experto en tecnología para obtener información mediante esta técnica en este tipo de organizaciones?

Conocer un documento con aspectos básicos y situaciones a manera de ejemplo para identificar un ataque de Ingeniería Social, sería una buena herramienta para prevenir y estar alertas ante posibles fraudes y ofrecer una reflexión para alcanzar las metas cumpliendo las normas.

2. Algunos Conceptos

Los recursos a través de los cuales las entidades financieras generan sus ingresos son en su mayoría del público, por ello busca, consolidar relaciones de largo plazo con los clientes respondiendo a sus necesidades, aumentar el promedio de clientes atendidos, asegurar la calidad de la operación desde el principio y optimizar el tiempo de respuesta a las solicitudes.

Como colaborador se conocen los diferentes tipos de riesgos a los que se expone quien trabaja en una entidad financiera; el área en la cual desarrolla su actividad, ¿Recibe llamadas sospechosas? ¿O correos electrónicos solicitando información de la entidad o de clientes? ¿Supuestos clientes quieren ganar su confianza?

2.1 Riesgo

"Es la posibilidad de incurrir en pérdidas por deficiencia, falla o inadecuaciones en, el recurso humano, los procesos, la tecnología, la infraestructura, o por la ocurrencia de acontecimientos externos, que tengan capacidad de incidir en el desarrollo del negocio, para nuestro caso, de la entidad financiera; esta definición incluye el riesgo legal y reputacional, asociados a tales factores" [3]. Algunos tipos de riesgo desde el punto de vista de seguridad de la información y relacionados con el fraude electrónico son:

Riesgo de actuación: Se da por el desconocimiento o incumplimiento de las normas de seguridad en el uso de la tecnología o de la información, lo que conlleva a que se entregue información personal y/o confidencial a terceras personas.

Riesgo Inherente: Está asociado con la utilización de la tecnología en los canales electrónicos (Internet, cajeros automáticos, banca móvil, comercios electrónicos, audio, etc.), lo que conlleva a cometer errores que no pueden ser controlados, dada la naturaleza misma de los servicios.

Riesgo de contagio: Está asociado con la utilización de Internet, recepción de software o archivos a través de correos electrónicos o la instalación de software de origen desconocido, lo que ocasiona que la estación de trabajo se infecte con aplicaciones maliciosas.

2.2 Información

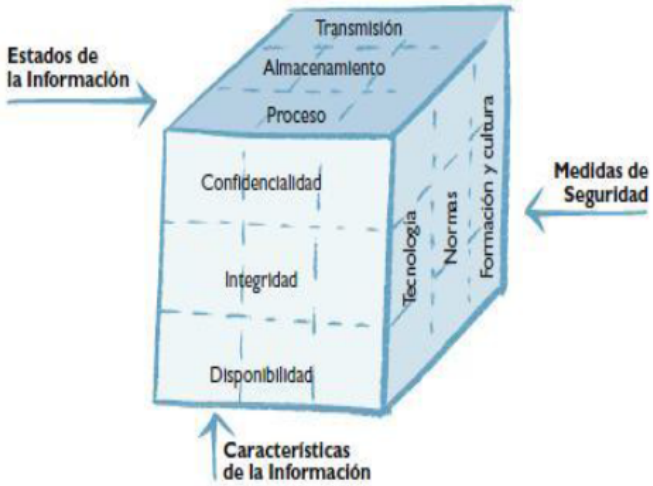
Es un activo, el cual, como cualquier otro activo de negocios, tiene valor para una organización y consecuentemente necesita ser protegido adecuadamente.

De acuerdo a la forma de comunicarse puede ser, Impresa, escrita en papel, transmitida por correo convencional o electrónicamente, exhibida en videos corporativos, hablada en reuniones [4].

2.3 Seguridad de la información

De acuerdo a John R. McCumber, son todas aquellas medidas tecnológicas, de normas y procedimientos y de formación que aseguran la confidencialidad, integridad y disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión. Esta definición parte de un modelo fácil y completo de seguridad, independiente del entorno, arquitectura o tecnología que gestiona nuestra información [5]. De acuerdo a la Figura 1, el modelo de tres dimensiones se convierte en un cubo con 27 celdillas como marco de actuación.

Figura1. Modelo de McCumber



Fuente: Grupo Ibermática en [5]

La seguridad de la información está caracterizada por la preservación de los siguientes aspectos o propiedades [6]:

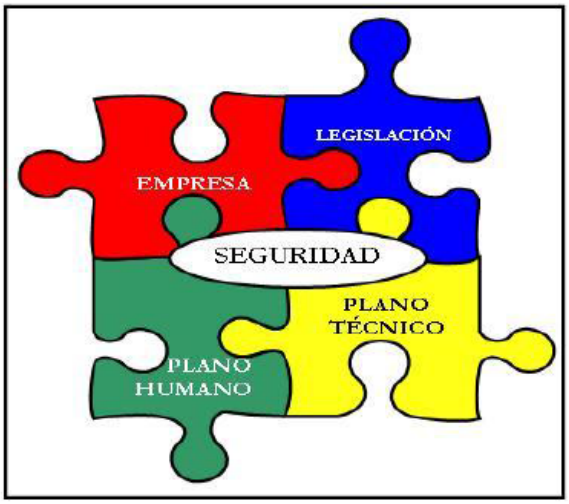
Confidencialidad: Los recursos del sistema solo pueden ser accedidos por los elementos autorizados.

Integridad: Los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados

Disponibilidad: Los recursos del sistema deben permanecer accesibles a los elementos autorizados.

Y entonces, tal como se muestra en la Figura 2, abarca el plano humano y técnico en la entidad financiera con el cumplimiento de la respectiva legislación.

Figura2. Alcance Seguridad de la Información



Fuente: El autor

2.4 Servicio

Es el conjunto de actividades interrelacionadas que ofrece un suministrador con el fin de que el cliente obtenga el producto en el momento y lugar adecuado y se asegure un uso correcto del mismo [7]. De este modo, el servicio podría presentarse como un bien de carácter no material.

De manera más clara, es todo lo que hacemos en beneficio de otros y para alcanzar un propósito común, servimos a los miembros de la familia, a los clientes, a la empresa y al país. Prestar

Un excelente servicio a los clientes, compañeros y a su propia labor desde el puesto de trabajo y por ende ayudar al cumplimiento de los objetivos organizacionales (generadores de bienestar, progreso y desarrollo), se convierte en una nueva misión para los colaboradores de las entidades financieras.

2.4.1 Fundamentos del Servicio [2]

Amabilidad: Buen trato, cordialidad y excelente disposición de la atención al cliente. Hacer que la otra persona se sienta importante y hacerlo sinceramente. Demostrar al cliente disposición e interés durante todo el contacto. Adoptar postura y gestos adecuados que denoten interés y disponibilidad. Conservar una actitud amable ante clientes alterados o enojados, no alterarse cuando el cliente este alterado, ni discutir con él.

Agilidad: Acción de “hacer” las cosas con celeridad, disposición y oportunidad, en un tiempo que se ajuste a los estándares definidos y a las pautas del mercado, para que el cliente sienta cumplida su expectativa. Responder a las demandas de los clientes en menor tiempo que el esperado. Plantear rápidamente alternativas de solución a los problemas o inconvenientes

Facilidad: Lo sencillo, amigable y efectivo que sea el actuar del colaborador, de los procedimientos, formatos y herramientas, frente a cada contacto o momento de verdad, que conllevan a una mejor comprensión por parte del cliente y al cumplimiento de las promesas. Ceder en la posición hasta donde sea permitido por las normas de la organización para lograr la satisfacción del cliente. Establecer acuerdos que permitan que tanto los clientes como la organización salgan beneficiados.

Claridad: Transmisión de información veraz, consistente, precisa, de fácil entendimiento y acorde a las necesidades del cliente, basada en el conocimiento global de la organización y de los productos, servicios, normas y procedimientos.

Responder o presentar la información siempre con la verdad. Escuchar con atención la información transmitida por el cliente. Mantenerse informado sobre la competencia. Demostrar seguridad de conocimientos y habilidades frente al cliente.

Cumplir lo que se promete: Es la disposición de cumplir y lograr consistencia entre los compromisos anunciados al cliente y los resultados entregados, enmarcados en condiciones de competitividad. Es no prometer más allá de lo que se puede cumplir.

Aquí se debe conocer a cabalidad los alcances y las limitaciones de los productos y servicios ofrecidos. Responder a las solicitudes de los clientes dentro del plazo acordado y ser coherente con lo que se ofrece y con lo que efectivamente se brinda al cliente.

Todos los fundamentos deben estar regidos por políticas de servicio y para cumplirlas es necesario, generar alertas sobre situaciones o desviaciones en productos, servicios o procesos que no se ajustan a lo esperado frente a los fundamentos de servicio de la entidad financiera; elevarlas a la instancia correspondiente para que se adopten correctivos; mantenerse informado y actualizado sobre los productos, servicios, normas y procedimientos.

El ingeniero social se aprovecha de estas acciones en la atención comercial o telefónica del cliente para lograr sus objetivos.

3. Ingeniería social

Ingeniería Social es la técnica usada para obtener información personal y/o confidencial mediante engaños; el objetivo del hacker es obtener información que le permita obtener acceso no autorizado a un sistema de valores y la información que reside en el sistema [8].

El delincuente puede identificarse como cliente, colaborador de otra oficina y/o área, o como proveedor, personalmente o mediante el envío de correos electrónicos, llamadas telefónicas o cartas.

3.1 Ingeniería Social y la confianza

La única cosa en la que todo el mundo parece estar de acuerdo es que la ingeniería social es en general, la manipulación inteligente de un delincuente a la tendencia natural del ser humano de confiar en sus semejantes.

La seguridad tiene que ver con la confianza. La confianza en la protección y la autenticidad. Generalmente aceptado como el eslabón más débil de la cadena de la seguridad, la naturaleza del ser humano a confiar en la palabra de los demás, deja a muchos de nosotros vulnerables a los ataques [8].

3.2 Características de la Ingeniería Social

Los ataques de ingeniería social tienen lugar en dos niveles: el físico y el psicológico [8]. El entorno físico de estos ataques pueden ser: el lugar de trabajo, el teléfono, el reciclaje o basura y on-line. El entorno psicológico se basa en la persuasión y los métodos básicos son: la suplantación, el halago, la conformidad, la difusión de la responsabilidad, y la simple amistad. Independientemente del método utilizado, el objetivo principal es convencer a la persona que el ingeniero social es alguien en quien se puede confiar y divulgar información sensible, aprovechándose también del desconocimiento de la seguridad de la información que tienen la mayoría de los usuarios de la información.

La técnica de ataque “Ingeniería social” puede explotar, entre otros, los siguientes aspectos:
Todos queremos ayudar…
El primer movimiento es siempre de confianza hacia el otro…
No nos gusta sentirnos culpables por negar la ayuda…
A todos nos gusta que nos halaguen…

¿Por qué es tan efectiva la ingeniería social?

La esencia de la ingeniería social es ganar acceso no autorizado a los sistemas para cometer fraude, entrometerse en los sistemas y robar información e identidades; entre otras, existen dos razones fundamentales que la hacen tan efectiva:

Porque se considera que la seguridad de la información simplemente debe orientarse al aseguramiento de computadores y redes de datos, sin tener en cuenta que hay intervención de personas en el procesamiento y manejo de la información.

Porque para el delincuente es más efectivo y de cierta forma más fácil conseguir información engañando a las personas que atacando la tecnología, de paso aprovecha que no necesita ser experto en esta última materia.

3.3 Perfil del Atacante

No es fácil identificar un perfil único del delincuente, pero, por lo general en la mayoría de fuentes leídas sobre ingeniería social, dentro de los cuales se encuentran [8] y [9], se pueden mencionar las siguientes características:

Podría ser un hacker, espía, ladrón o detective privado

Permanece en calma cuando está al acecho

Actúa como si perteneciera a la organización

Estudia a sus víctimas y sabe cómo reaccionaran

Se retira si observa que algo comienza a fallar

Si el desafió es muy grande trabaja en equipo

3.4 Fases de la ingeniería social

Se podrían determinar tres fases en la acción de esta modalidad de fraude;

Recopilación de información: El delincuente hace llamadas telefónicas, envía correos electrónicos e información a través de páginas Web, se cuela en redes sociales y busca información en la basura, entre otros.

Selección de la víctima: El delincuente simula pertenecer a la organización, usa tarjetas de acceso y nombres falsos, busca gerentes de oficinas, subgerentes, asesores, encargados del soporte técnico, recepcionistas, asesores de servicio al cliente y cajeros entre otros, lo que indica que cualquiera puede ser víctima de un ataque de ingeniería social.

El ataque: Se basa en rutas periféricas de persuasión como imposición de autoridad, carisma, reciprocidad, necesidad urgente, validación social o aprovecha la existencia de nuevos productos o servicios para usarlos en su técnica de ataque [9].

Imposición de autoridad: El atacante se muestra como una persona autoritaria en cierta forma intimidante y con una necesidad urgente, menciona la figura de una vicepresidencia o altas directivas, incluso dando sus nombres para lograr mayor atención.

Carisma: El atacante usa modales amistosos, agradables, conversa sobre intereses comunes, adula para ganar confianza y obtener información sobre una persona, grupo o producto.

Reciprocidad: El atacante ofrece o promete ayuda, información u objetos que no necesariamente le has requerido. Esto construye confianza, da la sensación de autenticidad y confiabilidad.

Necesidad Urgente: El atacante establece un contacto repetido, indica que la información se requiere con urgencia y que si no se facilitan, surgirán problemas en los procesos, habrá personas perjudicadas y directivos molestos.

Validación social: El atacante acecha a las personas que necesitan "ser tomadas en cuenta" o que tienen cierto potencial de ser rechazadas dentro de su grupo social.

Nuevos productos o servicios: El atacante aprovecha el lanzamiento de nuevos productos para conseguir la información, haciéndose pasar como líder, participante activo del lanzamiento del producto o que tiene relación con el mismo y así poder engañar a su posible víctima.

3.5 Medios de Ataque

Los medios utilizados para realizar fraude en esta modalidad son las llamadas telefónicas, los correos electrónicos, en los sitios de trabajo e incluso fuera de la oficina.

Encontrar buenos ejemplos reales de los ataques de ingeniería social es un poco complicado. Las organizaciones difícilmente admiten que han sido víctimas de ataques (admitir una violación de la seguridad de la información, no es sólo vergonzoso, sino que puede dañar la reputación de la organización) y si se acepta el ataque no se ha documentado de la mejor manera (porque incluiría sitios y nombres reales de áreas y empleados de la organización) o esta información está muy reservada y solo algunos directivos o expertos tienen acceso a ella.

Por esta razón se realizó el siguiente ejercicio y a través de los diálogos se muestran algunas situaciones y técnicas que utilizan los delincuentes para obtener información confidencial a partir de la manipulación de usuarios legítimos. Se espera con esto ayudar a prevenir los ataques más comunes de ingeniería social

3.5.1 Teléfono

En la figura 3 se ilustra un ejemplo bastante efectivo en oficinas o áreas administrativas en las cuales existe personal temporal o colaboradores haciendo reemplazos.

Figura3. Ataque Telefónico

Victima: Buenos días, Banco XXX, Sucursal Nariño, habla Maria del Pilar, ¿Con quién tengo el gusto?

Atacante: Buenos días, Maria del Pilar, ¿Cómo estas? Te habla Alvaro Uribe, colaborador del área de mercadeo; estamos en una campaña para nuestros clientes de banca móvil y requerimos información de algunos clientes

Victima: Que interesante don Alvaro, cuénteme de que se trata

Atacante: Te voy a enviar un correo y antes de una hora me envías la información que te solicito ahí.

Victima: Claro, don Alvaro, como se que es muy importante para la entidad, yo le colaboro lo mas pronto posible. Hasta luego.

Auxiliar-Victima: Jefe, esta es la información que me solicitó de los mejores diez clientes de nuestra oficina con el nombre, teléfono, correo electrónico, dirección y saldo de cuentas.

Victima: Perfecto. Inmediatamente enviaré la información, ya que es muy importante para mercadeo; voy a llamar a don Alvaro, a ver si recibió el correo. *El teléfono suena ocupado.* Que raro, ¿sería que marqué mal? Volveré a llamar. *Suena ocupado.* Ojalá haya recibido el correo, ya que es algo importante para la entidad.

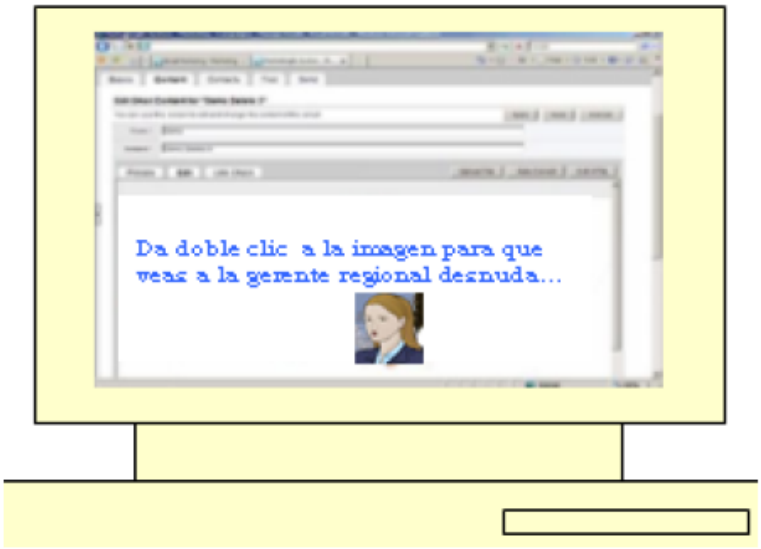
Fuente: El autor

En muchas ocasiones, encontramos que los responsables de los mensajes enviados o llamadas telefónicas no se pueden contactar, bien sea porque el número de teléfono no existe o porque su identidad es ficticia. A través de engaños como la suplantación de identidad, logran, la emisión de reportes, robo de datos personales o de contraseñas, entre otros tipos de información confidencial

3.5.2 Computador

Aunque la entidad cuente con políticas claras en seguridad de la información, no está exento de ser vulnerable a los intentos de fraude. El engaño a través de Internet es el medio más común para el ataque de ingeniería social y tiene muchas formas de ser llevado a cabo, tal como se ilustra en las figuras 4 y 5.

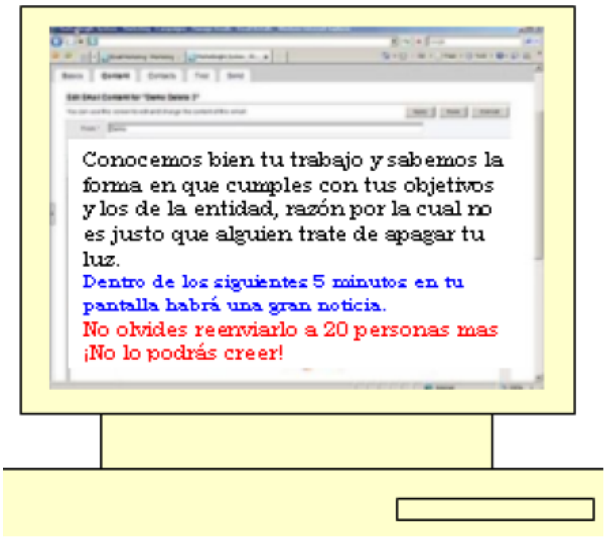
Figura4. Ataque por correo



Fuente: El autor

No dar entrada de virus informáticos al computador. Se debe usar responsablemente el correo electrónico.

Figura5. Ataque por correo cadena



Fuente: El autor

El delincuente finge ser empleado, compañero de trabajo, técnico o cliente. Por este medio se pueden hacer llegar memos falsos que solicitan respuesta e incluso las famosas “cadenas”, que llevan a revelar información sensible o a violar las políticas de seguridad de la organización. Es importante tener en cuenta que cualquier archivo adjunto que se reciba puede estar infectado con virus, troyanos o spyware, entre otros.

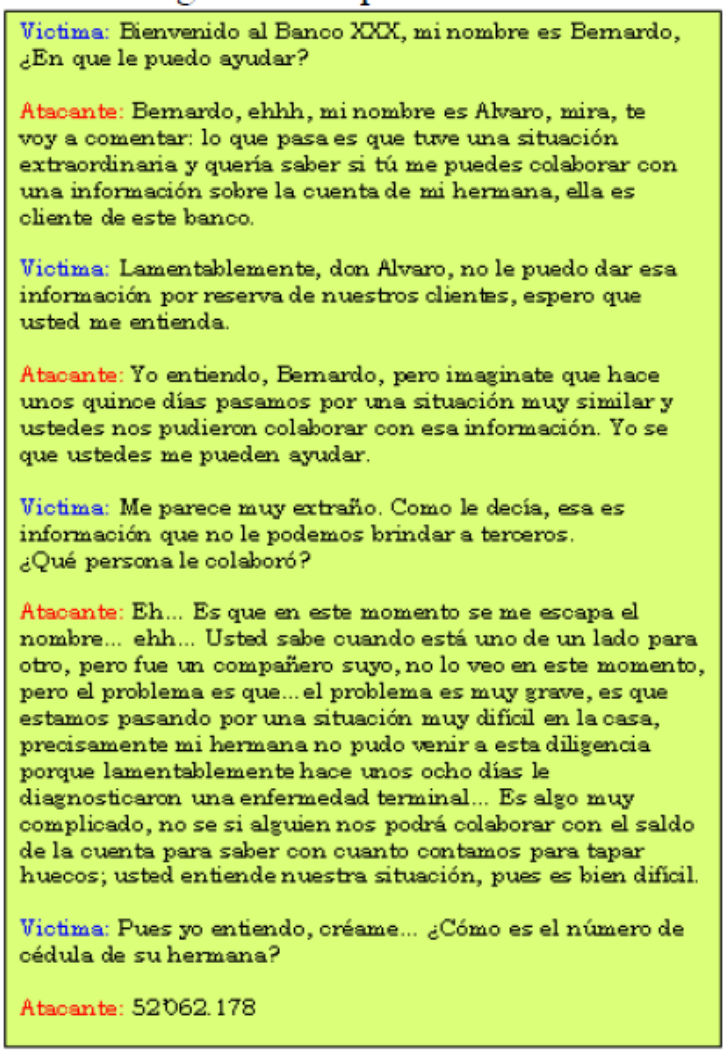
Los ataques no aplican a todos los colaboradores, por ejemplo a los encargados del área de tecnología o de auditoria resulta más difícil engañarlos a través de este medio y el delincuente y el ataque quedaría en evidencia y sería reportado inmediatamente.

Normalmente en las entidades financieras existen manuales de seguridad de la información y la política específica para este caso sería algo como: Los empleados no deben enviar mensajes de correo electrónico con contenidos hostiles que molesten a los receptores del mismo, tales como comentarios sobre sexo, raza, religión; así mismo cuando un empleado reciba este tipo de mensajes debe comunicarlo a su jefe inmediato y a seguridad informática [10].

3.5.3 Oficina de Trabajo

En el diálogo ilustrado en las figuras 6 y 7, el atacante hace de su petición una necesidad urgente, apelando a los sentimientos del colaborador, para obtener con mayor facilidad la información.

Figura6. Ataque en oficina



Fuente: El autor

Figura7. Ataque en lugar de trabajo

Atacante: Hola, ¿Cómo estas? Mucho gusto, mi nombre es Álvaro Uribe. ¿Te acuerdas de mi, Mariita?

Victima: Buenos días. Pues, la verdad, con tantos clientes que vienen a la oficina, me es difícil recordarlo, pero dígame ¿en que le puedo ayudar?

Atacante: Yo soy amigo de Salvatore Serrano, el gerente de esta sucursal, viejísimo cliente de este banco. Bueno, no importa. Oye, mi vida, estas muy bonita hoy, Mariita.

Victima: Ay, muchas gracias, don Alvaro, muchísimas gracias.

Atacante: Bueno, imagínate que tengo un inconveniente con el banco. La semana pasada hice una consignación a nombre del señor Andrés Arias, pero no aparece el soporte, así que quisiera que me dieras el saldo de su cuenta, por favor.

Victima: Bueno, don Álvaro, quisiera colaborarle, pero por seguridad de nuestros clientes, no estamos autorizados para dar información confidencial.

Atacante: Ay, Mariita, es que me dijeron que tu eres muy amable y hermosa. Es que el problema no fue mio, sino del banco, yo hice la consignación bien y en la caja parece que me metieron mal los datos en el computador; yo creo que es error de ustedes, entonces quisiera que tu me ayudaras. Salvatore me dijo que era fácil hacer esa vuelta, pues no sé.

Victima: ¿Usted tiene copia de consignación?

Atacante: Ese es el rollo Mariita, que no tengo la consignación, mi vida, colabórame con eso porque es un negocio muy importante para mi y sino reviso ese dato, me meto en un problema gravísimo para mi y mi familia; por favor, ayúdame, ¿si?

Victima: Mmmm...¡que pena, don Àlvaro, pero no le puedo dar la información sin la consignación ¡

Atacante: Mariita y tú con esos ojos tan bellos, ¿no me vas ayudar? Vamos, yo sé que tú quieres y puedes ayudarme a solucionar este tema. Mira que yo hablo con Salvatore y serás muy bien recompensada.

Victima: Don Álvaro, usted me pone en un dilema.... Mmmm.... Bueno, esta bien, le voy a colaborar, pero, no le comente a nadie porque me pueden sancionar.

Fuente: El Autor

3.5.4 Un Ataque Interno

Por lo general este tipo de ataques es realizado por colaboradores que abusan de sus derechos, buscan dañar la imagen de la entidad o simplemente vengarse de sus compañeros o superiores.

Inicialmente el atacante ingresa identificado como colaborador de tecnología, realiza un recorrido por el área e identifica la primera vulnerabilidad, los nombres de los usuarios escritos en papeles pegados al monitor de cada estación de trabajo (En 18 equipos de 24 existentes en el área), posteriormente nota que al lado del teclado se encuentra escrita la contraseña para acceder al equipo (en su mayoría la misma contraseña y la genérica que se da para activación o desbloqueo). Indaga sobre los roles de cada usuario en la recepción indicando que es para realizar una actualización en los aplicativos (con ello puede resolver cual usuario maneja información realmente importante).

Al ingresar a los equipos tiene a su disposición el correo electrónico, memos, documentos personales, la forma en que se maneja , se ordena y se clasifica la información, datos de clientes con historia laboral, crediticia, empresa en la cual labora, cargo y salario, entre otros. Ahora bien supongamos que este delincuente es un empleado temporal o de outsourcing y posteriormente se va a trabajar a la competencia y el core del área es precisamente la forma en la que se organiza y distribuye la información.

Otro…

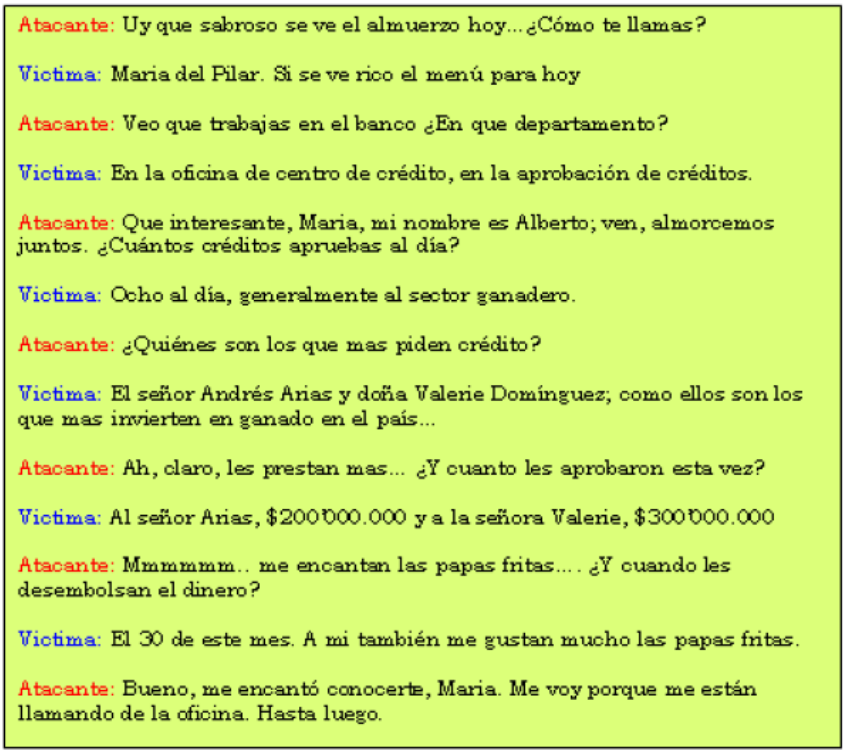
Un alto directivo solicita colaboración a su secretaria para ingresar a su estación de trabajo y extraer una información para la reunión que tiene en 5 minutos en otro lugar; la secretaria bloquea la contraseña y llama a la mesa de ayuda, la persona que le contesta identifica que la llamada se esté realizando desde el número telefónico de quien solicita el servicio (Telefonía IP) y accede a reiniciarla; la secretaria quien es muy amiga de algunos funcionarios de una oficina, observa las cifras de cumplimiento de las demás y entrega esos datos a su contacto, para metas, estrategias, premios y/o bonificaciones; también puede ver, llamados de atención, decisiones tomadas en documentos próximos a ser emitidos, clientes a visitar con datos financieros viables, firmar electrónicamente transacciones incluidas en el SARLAFT, entre otros; tiene a su disposición el correo corporativo y envía un mensaje citando a los colaboradores a una reunión extraordinaria, ¿Qué consecuencias traería en la pérdida de tiempo? ¿Cuántos clientes se dejarían de atender, gestionar o visitar por ausentarse de su puesto de trabajo e irse a una reunión ficticia? ¿Qué pasaría si el contrato laboral de esta persona está próximo a vencerse?

Una política aplicable a este caso sería, los archivos y mensajes de correo son información privada. El correo electrónico se debe manejar como comunicación directa y privada entre el originador y el receptor. Los funcionarios no deben utilizar una cuenta de correo electrónico que pertenezca a otro funcionario. Si hay necesidad de hacerlo en caso de ausencia o vacaciones se debe recurrir a mecanismos internos como redirección de mensajes [10].

3.5.5 Fuera de la oficina

En el diálogo ilustrado en la figura 8, el delincuente utiliza cualquier espacio para sacar información haciendo conversación amable, con el pretexto de la afinidad en gustos, para que la víctima revele datos importantes.

Figura8. Ataque fuera de oficina



Fuente: El autor

Tener en cuenta que por sus cargos y responsabilidades dentro de la entidad financiera, no es nada recomendable divulgar información confidencial a personas que no tienen porque saberlo. En todos los casos se atacan las vulnerabilidades que ofrecen los fundamentos del servicio y la confianza que da el colaborador, tratando y creyendo cumplir con los objetivos del negocio. Ataques realizados con niveles bajos de habilidades tecnológicas, simplemente valiéndose de conocimientos prácticos y básicos, que pudieron ser evitados si los colaboradores tuviesen presentes las políticas y normas de las que se supone dispone la entidad para disminuir las amenazas; queda en evidencia que no es suficiente que existan, estén impresas y archivadas.

3.6 Identificando un Ataque

Analizar al interlocutor, teniendo en cuenta que él…

- Podría ser una persona excesivamente amable.
- Piensa demasiado antes de dar una respuesta a una contrapregunta
- Cae fácilmente en trampas cuando se afirma una mentira.
- Tartamudea o usa mucho las muletillas “umm” “eeehhh” “esperame un momento” para ganar tiempo y pensar en una respuesta.
- Solicita información confidencial por fuera de los protocolos o canales previamente definidos por el banco.
- No se puede contactar a la persona que hace la solicitud, en el teléfono o extensión que facilita.

- Puede mostrarse como una persona autoritaria, que menciona al presidente o altos directivos, incluso hace alarde de su poder y su cargo tratando de intimidar.
- Evidencia falta de conocimiento de la organización y hace preguntas triviales de asuntos conocidos por la gran mayoría de los colaboradores.

3.7 Recomendaciones para evitar un ataque

Con lo anterior resulta difícil pero importantísimo, no ser paranoico ni perder la calidez para atender al cliente (Externo e Interno), teniendo en cuenta algunos consejos para no caer en un posible ataque de ingeniería social, como son:

- Mantener una actitud cautelosa para dar cualquier tipo de información.
- Al usar el teléfono, confirmar nombres y verificar los números de las extensiones telefónicas, con algún otro dato adicional que en lo posible solo lo sepa el contacto.
- No dejarse intimidar o halagar para terminar dando información.
- No permitir que una persona desconocida "descreste" con un aparente conocimiento de las personas o procesos internos, con el fin de ganar confianza para obtener información.
- No usar el correo electrónico corporativo para inscripciones en sitios web, diligenciar formularios no relacionados con el banco o responder encuestas; usarlo solo para temas laborales.
- Evitar brindar información que pueda comprometer la seguridad de los sistemas y la personal; datos como usuario, contraseña, fecha de nacimiento, familiares, empresas, tarjetas, salud, costumbres o datos económicos, entre otros.
- Destruir apropiadamente los documentos confidenciales.
- No responder ni reenviar mensajes en cadena que lleguen al correo electrónico sugiriendo un beneficio si se reenvía (buena suerte, premios o paz espiritual, entre otros).

3.8 ¿Cómo reaccionar ante un ataque? [8]

En el caso de que un empleado detecte algo sospechoso, él o ella tendrá los procedimientos establecidos para denunciar el incidente.

Cuando se crea la duda y se presienta que se está mintiendo, procurar confirmar las solicitudes de información que son inusuales, nunca confirmar con los datos sugeridos por el sospechoso, remitirse a una fuente confiable.

Si existen dudas de la veracidad de la fuente que solicita información, reportar al área de la entidad encargada de la seguridad de la información, teniendo claro el número telefónico y/o las extensiones de los contactos.

Es muy importante mantener cordialidad y amabilidad al atender a los clientes internos y externos, así, como mucho tacto para identificar un posible delincuente que busque aprovecharse de la buena fe del colaborador para captar información confidencial.
Muchas organizaciones caen en el error de planificar solo los ataques físicos. La seguridad de la información se debe extender a todos los puestos de trabajo de la entidad, independientemente de si los empleados usan computador.

Los ataques deben ser publicados y los empleados entrenados en la forma de clasificar la información de acuerdo a su confiabilidad y en la responsabilidad de preservarla y mantener a salvo sus datos confidenciales.

Trabajo futuro

Los ataques presentados se mostraron desde el punto de vista del delincuente malintencionado, bien sea interno o externo, pero, ¿Que ocurre con todos aquellos colaboradores que se saltan las políticas de seguridad sin ninguna mala intención, que cumplen con sus tareas de forma ágil y efectiva y que simplemente por cumplir con sus metas, objetivos del área o de la organización, se salen de la norma? La mayoría de políticas que tratan de la seguridad de la información (sino son todas), están orientadas a identificar y prevenir ataques de origen malicioso, entonces, que hacer con aquellos usuarios que se llevan trabajo a la casa, que facilitan cambios de clave a sus clientes en su estación de trabajo, que dejan las conexiones remotas habilitadas en las terminales administrativas y financieras de una oficina, que se van para la competencia atraídos por un mejor salario, en conclusión, que sin quererlo perjudican la organización y aumentan las amenazas de la información.

Según David Wall en su publicación, Seguridad en la Organización y amenazas internas, existen los atacantes internos no malintencionados o descuidados [11]. Para nuestro caso particular, este tipo de acciones anteriormente mencionadas, ¿Pueden ser consideradas de Ingeniería Social? ¿Qué atención y que recursos otorga la entidad financiera a este tipo de ataques sin intención?

4. Conclusiones

Atacar el servicio y la confianza de los colaboradores, en las diferentes áreas de una entidad financiera con ingeniería social, termina mostrando que no es suficiente todo el esfuerzo que realiza la presidencia para evitar la fuga de información con tecnología.

La principal defensa contra la ingeniería social es educar y entrenar, estando vigilantes a que todos los colaboradores cumplan las políticas de seguridad de la información. La capacitación de los empleados es esencial, mantener cursos, boletines, emisión de cartas reglamentarias e información actualizada, facilita el estar alertas; si la acción solicitada está prohibida por la política, el empleado no tiene más remedio que rechazar la solicitud del atacante.

Cambiar la cultura de los colaboradores en su área de trabajo es muy complicado, se debe mostrar con ejemplos reales y a manera de reflexión las vulnerabilidades y los riesgos que tiene la información confidencial y las consecuencias que traerían a sí mismo o a la organización, la no aplicación de las normas de seguridad. Utilizar el llamado “cliente incógnito”[2] para este tipo de demostraciones sería una buena opción.

De los riesgos se desprende que los problemas de seguridad en las entidades financieras no son únicamente de índole tecnológicos, por eso nunca se eliminan y en consecuencia se debe entender la seguridad de la información como un proceso que nunca termina.

[2] Colaborador que conoce los procesos de la entidad y llega a oficinas o áreas administrativas fingiendo ser cliente y solicitando información con cámara oculta, para posteriormente evaluar el servicio.

El incremento de los productos, servicios y canales bancarios, es directamente proporcional al aumento del número de amenazas, la entidad financiera debe contar con el esfuerzo y compromiso individual y colectivo de todos los colaboradores para cumplir su propósito y lograr estar orientada a los clientes, evitando la fuga de información.

Agradecimientos

Por todo el apoyo, el empuje, la motivación, la exigencia y espera a lo largo de la Especialización, mil gracias a la Ingeniera Angélica Flórez Abril. A todos los colaboradores de las diferentes áreas comerciales y administrativas del Banco Caja Social que desde su puesto de trabajo aportaron conocimiento y experiencias con clientes internos y externos para poder realizar ejemplos palpables. A mi familia que a pesar de las dificultades en el camino nunca han desfallecido en su apoyo y entusiasmo para ayudarme a lograr mis objetivos. A mi grupo de trabajo que permitió ausentarme en los horas que requería mi paso por la Universidad.

Bibliografía

[1]. WHITAKER, Andrew. Top 10 Social Engineering Tactics. Junio, 2009. Disponible en informIT, The Trusted Technology Learning Source. En internet, http://www.informit.com/articles/article.aspx?p=1350956

[2]. Vicepresidencia de Desarrollo Humano, Productividad y Servicio. Fundamentos del servicio BCSC. Guía de servicio BCSC. Julio de 2006. Disponible desde Intranet BCS

[3]. ARBOLEDA, Eulalia. Manual de Riesgo Operativo. Junio 29 de 2007. Carta Reglamentaria nº 2609. Disponible desde Intranet BCS.

[4]. ISO/IEC 17799 Code of Practice for Information Security Management, Primera Edición 2000 www.isostandards.com

[5]. La Seguridad de Información. Documentos de reflexión estratégica y tecnológica. Publicación editada por el Grupo Ibermática, Nº 93. 5 Abril 2000. Tomado de: http://www.ibermatica.com/ibermatica/publicaciones/documentos/documentos093

[6]. CARVAJAL, Armando. Introducción a la Inseguridad de la Información. Fundamentos de la Inseguridad de la información. Modulo I. Especialización en seguridad informática. Marzo, 2008. Pág. 5-7. UPB Bucaramanga.

[7]. CALDERON, Neyra. Presentación. Servicio al cliente. Lima, Perú. 2002. Tomado de: http://www.monografias.com/trabajos11/sercli/sercli.shtml

[8]. GRANGER, Sarah. Social Engineering Fundamentals, Part II: Combat Strategies. Enero, 2002. Actualizado Noviembre 2010. Disponible desde: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies

[9]. JAMEY, Heary. Networkworld. Top 5 Social Engineering Exploit Techniques. Noviembre, 2009. Disponible desde, http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html

[10]. HERRERA, Jaime Andrés. Manual de Seguridad Informática y Tecnología. Vicepresidencia de Tecnología. Gerencia de Aseguramiento Informático y Continuidad del Negocio. Código: AD-SIT-001. Ultima actualización 10 Nov. 2011. Disponible desde Intranet BCS

[11]. WALL, David. Seguridad en la Organización y amenazas internas: atacantes internos maliciosos, descuidados y sin malas intenciones. Prevención contra la pérdida de datos. Octubre de 2011. Disponible desde Internet: http://www.idg.es/idgconnect/whitepaper/DescargaWhitepaper.aspx?white=720&or=web

Biografía

Luis Eduardo Patiño Durán. Auditor Interno ISO: 27001:2005, UPB-SGS. Ingeniero de Sistemas, Universidad Industrial de Santander. Actualmente trabaja en el área de Servicio de Asistencia Tecnológica para el Banco Caja Social, brindando soporte y apoyo a las oficinas, áreas administrativas y clientes empresariales de la regional Oriente.

Las campañas de sensibilización son un instrumento conformado por diversas actividades, que buscan que el usuario al interior de una organización, se encamine por las buenas prácticas en seguridad de la información, respaldando así a la organización en la responsable tarea de proteger los activos de información [5], [6].

En una campaña de sensibilización nada puede quedar en el aire todo deber ser debidamente planificado y elaborado según sus objetivos finales, de los cuales los resultados deben ser los esperados por la organización, es necesario establecer indicadores que reflejen los diferentes estados de aplicabilidad de las actividades que componen la campaña.

Importante que el usuario primero sea educado y posteriormente capacitado.
Las alternativas que se recomiendan utilizar para que el plan de sensibilización sea factible son:

- Folletos
- Carteles
- Material BTL [3]
- Material POP [4]
- Uso de tecnología
- Presentaciones de Capacitación.

Es importante y necesario que cambie la mentalidad que existe en el factor humano de que no hay nada importante por proteger en su computador [15].

5. Cultura Organizacional en Seguridad de la Información.

La cultura organizacional es en esta era de la información uno de los más importantes elementos que caracterizan una organización[5], se da en el quehacer diario en las rutinas y acciones que se ejecutan al interior y que afectan el bienestar de la organización. A nivel empresarial puede llegar a comprometer el circulo en el que se mueve (clientes, empleados, proveedores y competencia).

Básicamente la cultura deja al descubierto la intención estratégica de una organización, es decir; como la organización desea cumplir con los objetivos o las metas que se ha propuesto, estableciendo su comportamiento como un elemento clave a la hora de competir con su entorno. [7][11].

[3] Material BTL: desarrollo e implementación de actividades de publicidad dirigidas a un grupo específico empleándose medios de comunicación alternos, innovadores y muy creativos.

[4] Material POP: material promocional colocado en sitios estratégicos para captar la atención del usuario e impulsarlo a participar, incluye los letreros, anuncios, etc.

[5] Se hace especial referencia al artículo LA CULTURA EN LAS ORGANIZACIONES, Un fenómeno central en el saber administrativo escrito por Paola Podestá, publicado en el 2009.

Es frecuenté encontrar a nivel organizacional diversos tipos de culturas y comportamientos, existen metodologías y modelos[6] encargados de estudiar ese comportamiento y una vez identificado responder a la pregunta ¿Qué se puede mejorar? Por éstas estructuras es que la cultura se transforma, se vuelve reflexiva y adopta ideologías de aceptación. Siendo la información entonces tan importante para la sociedad, entra a jugar el término cultura organizacional como un factor determinante a la hora de fortalecer el eslabón más débil (usuario).

Cultura organizacional se describe como el conjunto de modos de vida, costumbres, valores y creencias que generan al interior de una organización una identidad, la cual fortalece o debilita los objetivos planteados para el futuro éxito de las metas trazadas de la organización. Lo anterior nos permite inferir que mientras más cercanos estén los comportamientos de los individuos a dichos valores y principios, más integrada y congruente será la organización y sus resultados. En el sentido contrario, mientras más alejados estén los comportamientos de los individuos a dichos valores y principios, más desintegrada será la organización y sus resultados. Entonces, si se quiere gestionar la cultura de la seguridad de la información, se debe planear y ejecutar las medidas necesarias para que todos y cada uno de los usuarios que componen la organización se transformen en los aliados estratégicos a la hora de cumplir con los objetivos trazados por la organización para el futuro.

La seguridad de la información se ve afectada por los comportamientos de los usuarios dentro y para con la organización, en el compromiso de los empleados para con su organización, en la actitud de los empleados frente al cambio, en cómo se enfrentan los problemas y como se plantean las soluciones y entre muchos otros en el saber que tan importante somos para la organización en la que trabajamos y cuál es el grado de pertenencia que tenemos para con la misma [8].

De la buena gestión del grupo de TI encargado de promover la seguridad de la información, depende que nuestra cultura no se vuelva una cultura anómica, definida como de desinterés, falta de involucramiento, apática, indiferente viviendo en la incertidumbre, en la confusión, en la perdida de entusiasmo debido a la ausencia de recompensas para la premiación de éxitos, si no en una cultura integrativa, basada en la combinación de la orientación de los usuarios y los lineamientos estratégicos, en su visión, compromiso, trabajo en equipo, adaptación al cambio, llena de motivaciones, comunicación fluida y una alta preocupación por proteger y apoyar los objetivos de la organización para la cual trabaja. [30]

6. Innovación Tecnológica.

[6] Modelo de Shein (1987), En este popular modelo de cultura organizacional, la cultura se manifiesta en tres niveles: los artefactos se encuentran en la superficie, descansando sobre los valores y los supuestos en la base.

Las motivaciones a medida que avanza el mundo son diferentes, claramente hay un interés por la innovación tecnológica; pero se deja a un lado la protección y las buenas prácticas que se deben implementar a medida de que existan cambios en la organización.

Aquí entra otro concepto adicional como lo es la administración o manejo del cambio, que interviene directamente con los factores ya mencionados.

Para establecer un modelo exitoso de manejo del cambio se deben seguir una serie de pasos como lo son las expectativas, estrategias de comunicación, definición de roles, mecanismos de transferencia de conocimiento y lo más importante la adopción por parte de todos en la organización de las buenas prácticas en seguridad de la información.

Cada uno de los conceptos mencionados (Manejo del cambio, buenas prácticas de seguridad de la información, desarrollo de estrategias de enfrentamiento, sicología de la seguridad de la información, modelos organizacionales) serán los que de alguna forma faciliten el diseño de la estrategia para el aseguramiento de la información. [22].

7. Análisis de resultados de la encuesta aplicada a la fundación oftalmológica de Santander.

El instrumento de recolección de datos fue aplicado con el objetivo de diagnosticar la falta de compromiso y adopción por parte de la organización al implementar una campaña de sensibilización de seguridad de la información. Ver anexo 1. (*Encuesta-Foscal*, aplicada a la fundación Oftalmológica de Santander Foscal)

Población = 1000 Personas

Muestra de Población Encuestada = 159 Personas

Nivel de confianza de 93%

Se entregaron 210 encuestas con 15 preguntas; fueron contestados 159 encuestas correctamente, el resto no fueron contestados. Ver Anexo 2. *Resultados-Análisis-Encuesta-FOSCAL*

A continuación se presentan las conclusiones más importantes, resultado del análisis de las respuestas a las 15 preguntas de la encuesta.

Las conclusiones fueron las siguientes:

- Solo el 80% del personal encuestado presencio o estaba informado de la campaña de sensibilización en seguridad de la información realizada al interior de la organización. Lo

Importante no es que la mayoría se entere de la campaña si no todos los que conforman la organización, desde el presidente de la organización hasta las empleadas de servicio y vigilantes.

- Solo el 87% de la muestra encuestada sabe a que se refiere el termino seguridad de la información el resto lo desconoce siendo una cifra producto de la conclusión anterior.

- El 34% de la muestra desconoce o no identifica lo que es un activo y las responsabilidades que tiene en su labor sobre el mismo. Que importante es que el 100% tenga claro el concepto de activos de información e identifique los mismos en su labor diaria.

- Solo el 79% de la muestra piensa que su labor de protección ante la inseguridad de la información es importante para la empresa. Aquí debe ser claro que el 100% de la población debe sentirse importante y parte fundamental de la empresa, así mismo que entienda que un descuido puede llevar a afectar la continuidad de las actividades fundamentales de la organización.

- El 63% de la población encuestada no hizo parte de la identificación de activos o información valiosa que tiene la organización. Este porcentaje es muy alto lo ideal sería que la identificación se realizara con cada una de las personas que hace parte de la organización, realmente son ellos los que pueden sacar a la luz todo lo que saben y que se debe proteger.

- El 15% de la muestra desconoce las sanciones que existen en caso tal de que ponga en riesgo los activos de la organización, ósea, es para ellos transparente si pierden, divulgan o incumplen con las políticas de la seguridad de la información, esto es el resultado de que el 18% desconozcan las políticas de seguridad de la información. Siguiendo por este mismo tema se evidencia así mismo que el 38% señala que nadie les supervisa su labor de protección en seguridad de la información, un valor muy alto si se quiere concienciar a todo el personal que labora en la organización.

- Importante que en las campañas de sensibilización en seguridad de la información se tengan en cuenta a todos los usuarios, incluyendo terceros, practicantes, altos ejecutivos es decir el 100% del personal que labora en la organización.

8. Ingeniería Social

La ingeniería social es uno de los métodos más usados para obtener de parte de la organización información significativa o sensible. Actualmente las organizaciones están realizando inversiones en seguridad de la información para la parte de tecnología, dejando a un lado el factor humano, que hace parte de los 3 pilares a resguardar dentro de la seguridad de la información, las personas se considera como el objetivo principal de la ingeniería social para la fuga de información. Un ataque de ingeniería social puede estar dirigido a una organización

objetivo, a un determinado empleado, a un grupo de empleados o a un usuario y puede ser efectuado por un colega, compañero o simplemente un anónimo.

Los medios utilizados para este tipo de ataques de ingeniería social pueden presentarse por medio de un correo, una encuesta o por la recolección de información por medio de un dialogo. No es necesario tener el conocimiento técnico para cometer una intrusión atravez de la seguridad de la red, solo es suficiente con que existan usuarios despistados y poco informados con las buenas prácticas de la seguridad de la información.

La firma Imperva, especializada en Seguridad Informática presento un informe en el cual se mencionan las vulnerabilidades en el 2011, entre las que se encuentran la perdida de información en dispositivos móviles y en segundo lugar las redes sociales y robo de información por parte de los mismos empleados [17], [18], [20]. Así mimo Netasq afirma que para el 2012 las principales brechas de seguridad se concentran en dispositivos móviles y nuevamente la fuga de información por medio de las redes sociales, haciendo énfasis en que el factor humano se presenta como el eslabón débil a la hora de proteger la información [19], [13], [14], [21].

9. Estrategia de Sensibilización seguridad de la información.

El modelo estratégico planteado a continuación se compone de un conjunto de acciones que implementados al interior de una organización, contribuye al cumplimiento del principal objetivo de este artículo, el cual es aumentar la efectividad de las campañas de sensibilización en seguridad de la información, así mismo servirá como punto clave de referencia para el cumplimiento de algunos de los puntos de la norma ISO 27001:2005, la cual brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).

La norma ISO 27001:2005 se compone de una serie de requerimientos que proponen un enfoque basado en procesos, y estos últimos en el modelo PHVA (Planear, Hacer, Verificar y Actuar). La cláusula 5.2.2 de la norma hace referencia a la formación, toma de conciencia y competencia, y describe que la organización debe asegurar que todo el personal apropiado, tiene conciencia de la pertinencia e importancia de sus actividades de seguridad de la información, así mismo a la contribución al logro de los objetivos de SGSI.

Con base a lo anteriormente descrito, a continuación se listan un conjunto de pasos, que proponen una guía a seguir para elevar el nivel de efectividad de las campañas de sensibilización en seguridad de la información, teniendo en cuenta que sería de vital ayuda para las organizaciones que pretenden mantener su entorno corporativo protegido de amenazas que rodean los sistemas de información y por ende sus activos (usuarios finales).

Para todo diseño e implementación de campañas de sensibilización en seguridad de la información, y para obtener mejores resultados al momento de culturizar todos y cada uno de los usuarios que componen la organización, se propone seguir el siguiente procedimiento:

7.1 NORMA ISO/IEC 27001:2005

Se debe adquirir por parte de la organización, el material fundamental, que para el caso de la seguridad de la información es el estándar internacional ISO/IEC 27001:2005 (Tecnología de Información, Técnicas de Seguridad, Sistema de Gestión de Seguridad de la Información y Requisitos), donde se describen cada uno de los pasos a seguir para mantener los 3 pilares que soportan la protección de la información, es decir, mantener la confidencialidad, integridad y disponibilidad de la información.

Es importante destacar que la información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

7.1.1 Sistema de Gestión de Seguridad de la Información – SGSI

Si bien es cierto, la norma ISO 27001 describe en su totalidad el modelo para el establecimiento del SGSI, pero para este procedimiento, es indispensable tener presente, algunos de los puntos que servirán como soporte para la culturización en seguridad de la información en toda organización.

Es necesario que una vez, el SGSI sea diseñado, y alineado con el contexto de la organización sea adoptado por la misma, si desde el principio los objetivos no se encuentran debidamente trazados, al final los resultados no van a ser los contemplados o esperados por la organización.

El SGSI es la parte del sistema de gestión de la organización, que basado en un enfoque de riesgos del negocio, aterriza y presenta los posibles problemas que se pueden presentar si no se realiza la gestión necesaria, por tal motivo es necesario para todo proceso de culturización y/o sensibilización se tengan en cuenta las siguientes actividades:

- Definir, desarrollar políticas, normas y procedimientos de seguridad de la información, que sirvan como soporte o punto de referencia para todos y cada uno de los usuarios de la organización, es decir, se dan a conocer roles y responsabilidades, así como las autoridades que estarán al pendiente de garantizar que las campañas de sensibilización, reflejen el resultado deseado.
- Es indispensable, y por ningún motivo se puede pasar por alto, que las políticas de seguridad de la información, obtengan la aprobación de la alta gerencia. No tiene sentido que se quiera crear y exigir cultura al interior de una organización, si desde el puesto más

alto no se brinda evidencia del compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI.

Dentro del modelo PHVA (Planear), antes del diseño de los planes de sensibilización, la organización debe realizar:

- Identificación, inventario y clasificación de todos los activos que posee la organización, si se desconoce lo verdaderamente valioso para la organización, si no se realiza un inventario de activos de información, no se puede saber qué información es confidencial, y por lo tanto que es lo que debo proteger.
- Identificar las vulnerabilidades y en du defecto las amenazas de cada uno de los activos identificados con anterioridad. Si conocemos las vulnerabilidades y amenazas podemos advertir en las campañas de sensibilización a todos y cada uno de los usuarios, de los posibles riesgos que se pueden generar por el no cumplimiento de las políticas de seguridad de la información.
- Identificar los propietarios de cada uno de los activos identificados con anterioridad; esto con el fin de establecer roles y responsabilidades, es decir, implementada la campaña de sensibilización en seguridad de la información, el usuario estará en capacidad de adoptar los controles que se ajusten al activo que tiene a su custodia.
- Entrevistar a cada uno de los usuarios propietarios de los activos, esto con el fin de identificar hasta qué punto la información que tienen a su disposición, es de vital importancia para la organización. Quien más que el propio usuario para que determine los requisitos que se deben tener para que la información se salvaguarde ante accesos no autorizados, modificación, o perdida de la confidencialidad o destrucción deliberada. Si se hace al usuario parte de la estrategia de las campañas de sensibilización en seguridad de la información, se le estaría dando un lugar al interior del proceso, por tal motivo se le daría a entender que el es importante para la organización, generando un sentido de pertenencia y compromiso con la misma.
- Identificar y hacerle saber a todos y a cada uno de los usuarios, el impacto que representa la perdida de confidencialidad, integridad y disponibilidad, de los activos que tiene a su custodia, es decir, si se le hace entender al usuario, que por su culpa o descuido, la organización puede sufrir un impacto negativo, se le creara la preocupación y por tal motivo el interés de protegerse y proteger los activos identificados de la organización.
- Diseñar los planes de sensibilización en seguridad de la información, es decir, una vez definidas las políticas, roles y responsabilidades, identificados los activos, identificados los propietarios de los activos e identificados los riesgos, se estará en la capacidad de diseñar a la medida de la organización, una campaña que cree la conciencia en los clientes internos y externos, en el papel que desempeña cada uno de ellos, para la consolidación y estructuración de un plan de seguridad acorde a las necesidades actuales de la organización.

Dentro del modelo PHVA (Hacer), posterior al diseño de los planes de sensibilización y con el propósito de continuar con el proceso de culturización en seguridad de la información se recomienda realizar las siguientes actividades:

- Definir el personal que será parte de la publicación y formación y los tiempos de divulgación de la campaña; es decir, asignar el personal que ejecutara las campañas de sensibilización en seguridad de la información y el momento oportuno de su aplicación.
- Implementar los planes o campañas de sensibilización en seguridad de la información; es decir, poner en marcha la etapa de formación y capacitación de los usuarios, asegurando que todo el personal se encuentre en la capacidad y competencia de responder al cualquier evento que coloque en riesgo la integridad, disponibilidad y confidencialidad de la información, y por tal motivo, que ponga en peligro la continuidad del negocio.

Dentro del modelo PHVA (verificar), posterior a la implementación de la campaña de sensibilización en seguridad de la información y con el propósito de continuar con el proceso de culturización en seguridad de la información se recomienda realizar las siguientes actividades:

- Medir constantemente la eficacia de las campañas de sensibilización en seguridad de la información; es decir, por medio de auditorías, pruebas de intrusión o mediciones de desempeño, se valida la efectividad y se le recuerda repetidamente al usuario, que el compromiso de proteger la información sigue en pie, y por lo tanto que debe seguir firme en su postura frente a cualquier riesgo. Es importante hacerle ver al usuario que no se capacita por capacitar, si no que se hace por un propósito común, y que de ello depende su puesto de trabajo o la misma estabilidad de la organización.

Dentro del modelo PHVA (actuar), posterior a la verificación de las pruebas realizadas en la anterior actividad, y con el propósito de continuar con el proceso de culturización en seguridad de la información se recomienda realizar las siguientes actividades:

- Publicar los resultados de las mediciones que se realizaron en el punto anterior; es importante darle a conocer al usuario el reflejo de su desempeño, en el camino por garantizar la protección de la información.
- Se deben establecer procesos disciplinarios, para aquellos usuarios, que no cumplen o que de cierta forma, no tienen sentido de pertenencia con la organización; es decir, hay que hacerles entender que las políticas de seguridad de la información están establecidas y hay que cumplirlas, que no solo están en el papel, que el compromiso es de todos, desafortunadamente el ser humano, hace las cosas bajo presión, por tal motivo es indispensable, poner en práctica este tipo de sanciones, en algún momento las políticas las cumplirá no porque se las exijan, sino porque se le ha convertido a través del tiempo en una costumbre o mejor aún en una habito.
- Se deben establecer incentivos, tanto personales como por áreas de trabajo, que premien el hecho de estar comprometidos con la organización; es decir, si un usuario se siente incentivado, motivado en su labor diaria, reflejara un comportamiento de agradecimiento con su organización y por lo tanto evolucionara de tal manera que sus costumbres, valores organizacionales estén alineados con los propósitos estratégicos de la organización.
- Por último y no menos importante, se debe Involucrar a todos y a cada uno de los usuarios y en cada uno de los niveles que componen la organización, y de manera

activa, con el propósito fundamental de la seguridad de la información, que es la de proteger el ciclo completo de la información.

10. Conclusiones

Las organizaciones entienden la importancia que tiene actualmente los activos de información pero desconocen las buenas prácticas para protegerlos.

Las organizaciones pretenden protegerse de amenazas en seguridad de la información pero invirtiendo solo en una de 2 de los pilares fundamentales como los son la tecnología y los procesos, dejando a un lado quizás el más importante en estos tiempos de fuga de información las personas.

Es fundamental que las organizaciones implementen estrategias de sensibilización en seguridad de la información, que se centren en educar por medio de campañas de concienciación y posteriormente en capacitar al factor humano con respecto a las nuevas tecnologías implementadas en la organización.

El promover la cultura organizacional en seguridad de la información es una tarea continua y de seguimiento total, debido a la innovación tecnológica y a las amenazas que conlleva a utilizarla.

9. Referencias Bibliográficas

[1] Jeimy J. Cano. (2012) Pronósticos de seguridad de la información. [En Linea]. Disponible: http://www.infosecurityvip.com/newsletter/palabras_feb12.html

[2] National Security Institute. (2004). Improving Security from the Inside Out Improving Security from the Inside Out. [En línea]. Disponible: http://nsi.org/SECURITYsense.html

[3] C. F. Borghello. Capacitación y Concientización de Seguridad en Organizaciones. [En línea]. Disponible: http://www.segu-info.com.ar

[4] L. J. Ugas. (2002). Seguridad en organizaciones con tecnologías de información. [En línea]. Disponible: http://www.urbe.edu/publicaciones/telematica/indice/pdf-vol1-1/1-seguridad-en-organizaciones-con-tecnologias-de-informacion.pdf.

[5] FISMA. (2002). Construcción de una Seguridad de la Información, Tecnología de sensibilización y formación. [En línea]. Disponible: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[6] D. Rodriguez. (26/04/07). ¿Realmente Sirven los Programas de Culturización en Seguridad informática? [En línea]. Disponible http://www.portaldeseguridad.com/gdc_notapub.php?cod_nota=372.

[7] P. Podestá. (2009). Culture In Organizations A central phenomena in administrative knowledge. [En Línea]. Disponible: http://www.esan.edu.pe/publicaciones/cuadernos-de-difusion/26/Podesta.pdf.

[8] I. Rodríguez Guerra. (2004). Cultura Organizacional. [En linea]. Disponible: http://www.uned.ac.cr/paa/pdf/Materiales-autoev/10.pdf.

[9] S. Jaimes Beltrán, Á. Osorio Domínguez. (2009). La cultura Organizacional Y La Gestión Del Conocimiento. [En línea]. Disponible: http://www.javeriana.edu.co/biblos/tesis/economia/tesis218.pdf.

[10] G. Meléndez. Cultura organizacional. [En línea]. Disponible: http://cicia.uprrp.edu/Papers/Cultura%20Organizacional.pdf.

[11] Diccionario de la Real Academia Española. [2009] Cultura. [En línea]. Disponible: http://www.rae.es/rae.html.

[12] ACIMED. (2009). Clima Y Cultura Organizacional [En línea]. Disponible: http://scielo.sld.cu

[13]. J. Hernández. (2003). Estudio socio psicológico del clima organizacional. [En linea]. Disponible: http://www.uo.edu.cu/ojs/index.php/stgo/article/viewFile/14503333/765.

[14].P. Szabunia. (2010). El cerebro y la cultura organizacional: ¿Similitudes casuales?. [En linea]. Disponible: http://biblioteca2.icesi.edu.co/cgi-olib?session=66860510&infile=details.glu&loid=219547&rs=2514806&hitno=16.

[15]. F. Ferrá Homar. (2003). La Formación, Concienciación Y Sensibilización En Seguridad. [En linea]. Disponible: http://www.revistasic.com/revista56/pdf_56/SIC_56_quepreocupa.PDF.

[16].Área de Investigación y planeación. (2008). Modelo de seguridad de la información para la Estrategia de gobierno en línea. [En Linea]. Disponible: http://programa.gobiernoenlinea.gov.co/apc-aa-iles/5854534aee4eee4102f0bd5ca294791f/GEL_IP_CapacitacionSensibilizacion_ModeloSeguridad.pdf

[17] Watch Guard Technologies (2008). Las 10 principales amenazas a la seguridad de los datos de las PyMEs. [En Linea]. Disponible: http://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp_es.pdf.

[18] Inforgalte (2010). Las diez principales amenazas a la seguridad informática en 2011. [En Línea]. Disponible: http://www.inforgalte.com/blog/las-diez-principales-amenazas-a-la-seguridad-informatica-en-2011.php

[19] Fabien Thomas, Chief Technology Officer, NETASQ (2012). Las 5 principales amenazas para la seguridad en 2012. [En Línea]. Disponible: http://seguridad-informacion.blogspot.com/2012/01/las-5-principales-amenazas-para-la.html.

[20] Symantec Corp. (2012). El informe anual de Symantec sobre amenazas a la seguridad en Internet indica un incremento del 81% en los ataques maliciosos. [En Línea]. Disponible: http://www.symantec.com/es/es/about/news/release/article.jsp?prid=20120507_01

[21] Carlos Tori. Hacking Etico – Ingenieria Social Paper. Rosario: Segunda Edición, 2008, Capitulo III, pp. 87-106.

[22] A. Van de Ven, D. Polley, R. Garud , S. Venkataraman, Desarrollo de una cultura organizacional para innovar. Mexico: Oxford University Press, 2001, pp. 23 – 70.

10. Bibliografía

[1] Abravanel, Allane, Firsirotu, Hobbs, Poupart. Cultura organizacional aspectos teóricos prácticos y metodológicos. Editorial legis, 1988, pp. 15 – 80.

[2] C.F. Borghello (2007, Oct). Informe anual de seguridad del FBI/CSI [En línea]. Disponible: http://www.segu-info.com.ar. Fecha de consulta Noviembre 12 de 2009.

[3] J. Cano. (2004). Hacia un concepto extendido de la mente segura. Pensamiento sistémico en seguridad informática. Artículo de investigación (En revisión). Universidad de los Andes.

[4] J. Cano. (17-Jun-2008). Métricas en Seguridad Informática. [En linea]. Disponible: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/07-MetricasSeguridadInformaticaUnaRevisionAcademica.pdf.

[5] D. Páramo Morales. (Jun-2001). Hacia La Construcción De Un Modelo De Cultura Organizacional Orientada Al Mercado. [En linea]. Disponible: http://editorial.unab.edu.co/revistas/rcmarketing/pdfs/r22_art5_c.pdf.

[6] C. A. Biscione - Technical Account Manager North of Latin America Sun Microsystems. (1999). Ingeniería Social Para No Creyentes. Disponible: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf.

[7] O. Ruiz. (22-Jun-2007). La fuga de información - la amenaza y sus contramedidas. [En línea]. Disponible: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/VIIJNSI_ORuiz.pdf. Fecha de consulta Agosto de 2010.