LA CONCIENCIACIÓN AL USUARIO FINAL COMO MECANISMO EFECTIVO PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

David Alexander Guatavita Diaz
davidguatavita@gmail.com
Universidad Piloto de Colombia

Resumen— En el siguiente documento se aborda un tema que es poco tenido en cuenta a la hora de realizar la gestión de riesgos en las organizaciones, se trata de la concienciación al usuario final y como esta puede surtir efectos positivos en la compañía sin necesidad de tener que invertir grandes cantidades de tiempo y dinero en la implementación de controles técnicos. Además redundando en grandes beneficios tanto para la compañía como para la vida personal de los empleados.
En esta era digital donde existe la hiperconectividad, es importante ser conscientes de los riesgos que conlleva utilizar la tecnología. En las próximas páginas se abordará esta situación y cómo, con sencillas acciones se puede atacar este problema que día a día crece al interior de las compañías.

Ìndice de Términos— NTC-ISO/IEC 27000, activo, amenaza, análisis de riesgo, confidencialidad, integridad, disponibilidad, control, evaluación de riesgos, vulnerabilidad, sistema de gestión de seguridad –SGSI-, riesgo, impacto.

Abstract— In the following ducts a topic is addressed that is little taken into account when making risk management in organizations, it is about the final user awareness and how it can have positive effects in the company without having to invest large amounts of time and money in the implementation of technical controls. In addition, resulting in great benefits for both the company and the personal life of employees. In this digital age where there is hyperconnectivity, it is important to be aware of the risks involved in using technology. In the next pages this situation will be addressed and as with simple actions you can attack this problem that day grows inside the companies.

Keywords— NTC-ISO / IEC 27000, active, threat, risk analysis, confidentiality, integrity, availability, control, risk assessment, vulnerability, security management system -SGSI-, risk, impact.

I. INTRODUCCCIÓN.

La gestión de riesgos es uno de los factores más importantes a tener en cuenta cuando se habla no solamente de seguridad informática, si no de cualquier proceso que se quiera implementar en una organización, sea cual sea la naturaleza de esta, se encuentra expuesta a numerosos riesgos.

La gestión de éstos comienza detectando los posibles peligros o amenazas a los que se expone, para después adoptar las medidas oportunas e implantar los procesos necesarios para minimizar o eliminar esos peligros.

Es de suma importancia darle a esta el lugar que corresponde en la compañía, debido a que se pueden afectar las operaciones diarias de la empresa, traduciéndose en pérdidas, ya sean económicas o reputacionales que en últimas van a afectar a la organización.

Cuando se habla de seguridad, siempre se piensa en la ciencia aplicada netamente a temas tecnológicos, dejando a un lado a los usuarios, quienes finalmente, si no tienen una conciencia adecuada frente a los riesgos asociados a su labor son quienes representan el mayor peligro para la materialización de riesgos de seguridad de la información , por esto es necesario tener en cuenta los tres pilares que hacen de la

seguridad en una organización algo vital, estos son : *los procesos corporativos*, la *tecnología* que los soporta y las *personas* que los realizan. Pero como se va a evidenciar, en la mayoría de las empresas, solo se enfocan en los primeros dos y esto hace que la estructura de seguridad se vuelva frágil, resultando en que los usuarios se conviertan en el eslabón más débil de la cadena de seguridad dentro de las organizaciones.

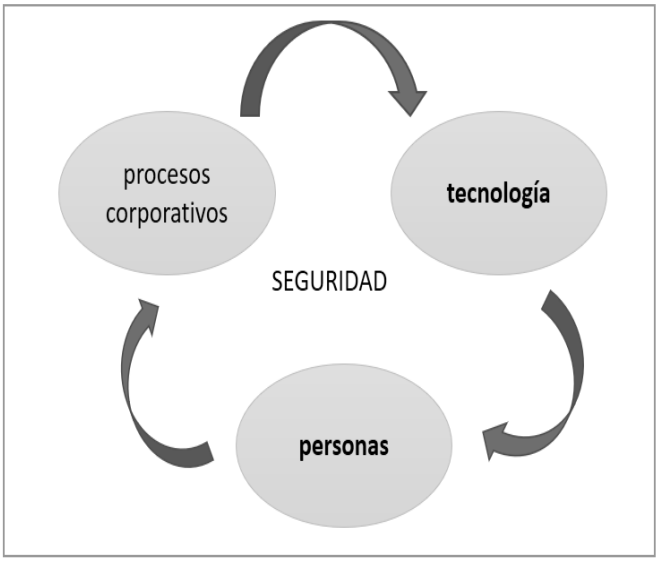

Figura1. Pilares de la seguridad.[8]

Un usuario común puede ver en la seguridad una serie de barreras para hacer lo que considera que está bien y que probablemente puede afectar los intereses de la organización si no es consciente de los riesgos a los que se encuentra expuesto. Además, puede llegar a pensar que las personas encargadas de la seguridad en la compañía son paranoicas y se aprovechan para maximizar las situaciones de riesgo dadas. En este orden de ideas, lo anterior puede resultar cierto; sin embargo, lo que sucede es que las áreas de seguridad son conscientes de las amenazas que hay en el entorno, por otra parte, como encargados y responsables de la seguridad de la información deben velar por el correcto uso de los recursos de la organización.

¿Cuántos de los usuarios han pensado que su propia máquina es poco importante dentro de la organización como para que un atacante pueda tener interés en ella?. Es por esto, que los usuarios tienen que ver que los atacantes no saben ni les interesa quién está del otro lado del equipo, por lo que cualquier objetivo es de suma importancia, toda vez que al obtener acceso a un dispositivo de la red, pueden monitorizarla o intentar escalar privilegios administrativos obteniendo así el acceso que tanto desean. También deben ver, que estas personas tienen un motivo para llevar a cabo la acción, unos intereses que tienen sentido para dicho atacante, que busca una oportunidad, momento o situación para ejecutar la acción, y unos instrumentos que son los tres pilares mencionados anteriormente.

Tampoco se debe descuidar el hecho que al desempeñar las labores sobre medios tecnológicos, estos tienen un riesgo potencial de inseguridad, que es un elemento inherente de la operación diaria de las organizaciones en cada uno de sus procesos.

Mientras las empresas pretenden ser cada día más seguras, la problemática de la inseguridad sigue creciendo. Durante los últimos años, los robos de información y la exposición de datos fueron los titulares más visibles en las noticias a nivel mundial en cuanto a temas de seguridad, esto no se debe a falta de controles (puesto que los hay), sino a que las metodologías de gestión de riesgos de seguridad se enfocan mucho en la parte de procesos y tecnología más no en las *personas*.

Por lo anterior, se puede concluir que: para abordar la seguridad de manera integral, es necesario realizar un programa adecuado de concienciación de los usuarios en este tema, debidamente apoyado en las políticas corporativas de seguridad (obviamente contando con el apoyo y aprobación de la dirección) y con un adecuado proceso de seguimiento y actualización, que finalmente se traducirá en beneficios para toda la organización, minimizando las exposiciones y perdidas por el uso inadecuado de los recursos tecnológicos.

II. CONCEPTOS BÁSICOS Y DEFINICIONES

Los siguientes son los términos y definiciones que se

encuentran presentes en el documento y se encuentran basados en la norma NTC-ISO/IEC 27001 e ISO 31000, los cuales son inherentes a los procesos de gestión del riesgo. Para una mejor comprensión de este documento, se toman como referencia los términos y definiciones establecidos en la Norma NTC-ISO/IEC 27001, norma NTC-ISO/IEC 27005 y la norma NTC-ISO/IEC 31000.

Activo: En relación con la seguridad de la información, se refiere a cualquier elemento relacionado con el tratamiento de la misma, es decir sistemas, soportes, edificios, personas, que tengan valor para la organización.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Confiabilidad de la información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones, la ejecución de las misiones y funciones.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones. La revelación no autorizada de la información calificada de acuerdo con un nivel de confidencialidad alto implica un grave impacto en la organización, en términos económicos, de su imagen y ante sus clientes.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como las exclusiones de controles del anexo A de la norma técnica NTC-ISO/IEC 27001:2013.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. La información debe estar en el momento y en el formato que se requiera en el momento indicado, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los clientes de la organización.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición del sistema, servicio o red, que indica una posible violación de la política de seguridad, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: pérdida de reputación, implicaciones legales, etc.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la organización debe ser clara y completa, solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Responsable de Seguridad Informática: En la organización el comité de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al Subsistema de Gestión de la Seguridad de la información (SGSI).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información; para efectos de entendimiento en organización, el SGSI hace referencia al Subsistema de Gestión de Seguridad de la Información.

Sistema de gestión de la seguridad de la información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

III. EL ESLABÓN MÁS DÉBIL DE LA CADENA.

Para empezar, esta frase del hacker más famosos de la historia:

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero por que ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: La gente que usa y administra los ordenadores." Kevin Mitnick.

Definiendo textualmente, la información es un fenómeno que proporciona significado o sentido a los elementos de la sociedad. En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje. En consecuencia, un dato deja de serlo, una vez que establece un sentido, un valor semántico para el usuario, mediante asociaciones lógicas entre sí, y otros datos sueltos que a su vez carecen de valor individualmente. Por otra parte, los datos se perciben, se integran y generan la información necesaria para producir el conocimiento que finalmente permite tomar decisiones para realizar las acciones cotidianas que aseguran la existencia. La información, por tanto, procesa y genera el conocimiento humano. En el proceso de toma de decisiones un dato no sirve, necesitamos Información [2].

Además de la definición anterior, la información, después de las personas, es el activo más importante de toda organización, por lo tanto, se le debe dar un tratamiento seguro. Sin importar el cargo que se ocupe en una compañía, se maneja Información que es esencial para los intereses de la misma.

Al referirse a la definición de la real academia española de la lengua, seguridad es la "cualidad de seguro", siendo seguro "libre y exento de todo peligro, daño o riesgo". A partir de estas definiciones, se podría definir entonces la seguridad como la sensación de bienestar de algo; una propiedad intangible que nos indica que ese algo está libre de peligro, daño o riesgo. Ese algo, en este caso particular, es la información. "Siempre hay que tener en cuenta que la seguridad comienza y termina con personas" [3].

A través de un estudio de Datapro Research Corp. Se pudo establecer que los problemas de seguridad en los sistemas responden a la siguiente distribución:

- Errores de los empleados 50%.
- Empleados deshonestos 15%.
- Empleados descuidados 15%.
- Otros 20% (Intrusos ajenos a la Empresa 10%; Integridad física de instalaciones 10%).

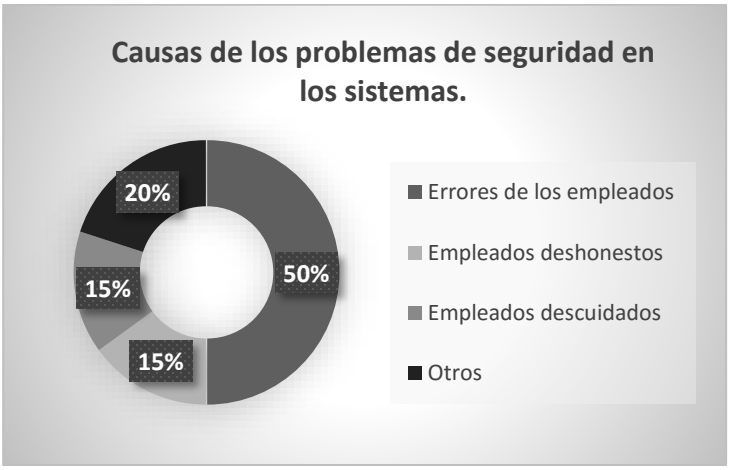

Figura2. Problemas de seguridad en los sistemas[3]

Se puede notar que el 80% de los problemas, son generados por los empleados de la organización, que se podrían tipificar en tres grupos grandes:

• Problemas por ignorancia.
• Problemas por falta de interés.
• Problemas por mala intención.

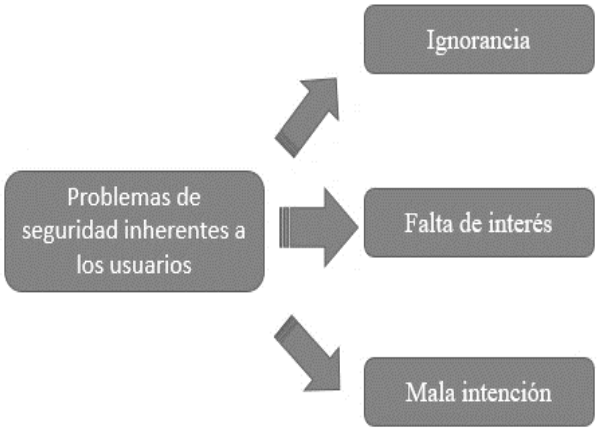

Figura3. Problemas de seguridad inherentes a los usuarios.[3]

Entre estas razones, la ignorancia es la más fácil de direccionar. Sin embargo, desarrollando estrategias de entrenamiento y procedimientos formales e informales son fácilmente neutralizadas. Los usuarios, además, necesitan de tiempo en tiempo, que se les recuerden cosas que ellos deberían conocer [4].

Pero el asunto no es tan fácil, porque en Colombia existen pocas organizaciones que cuenten con un programa de concienciación a los usuarios en temas relacionados con seguridad de la información. En algunos casos, las intenciones son puntuales, por lo que no llegan a tener la continuidad necesaria como para lograr algún cambio de actitud en los usuarios.

Como diría Christian Linacre, gerente de seguridad de Microsoft Latinoamérica: "La seguridad es tan fuerte como el eslabón más delgado de la cadena". Por esto, los usuarios son el punto más vulnerable en la cadena de seguridad, toda vez que su desconocimiento de unas buenas prácticas de seguridad puede ocasionar incidentes y poner en riesgo la disponibilidad, confidencialidad e integridad de información. En consecuencia, los usuarios son la herramienta más importante para proteger la información, ya que se pueden establecer todo tipo controles técnicos y gastar muchos recursos tanto financieros como humanos intentando tener las mejores tecnologías en seguridad. Sin embargo, sin la colaboración de los usuarios no se logrará minimizar los riegos, ya sea intencional o no la acción que ejecute un usuario, si no tiene conciencia de lo que puede pasar con estas acciones de nada servirán todos los esfuerzos hechos desde el área técnica.

Otro de los aspectos fundamentales a abordar en este tema es el ámbito jurídico y legal en el que se desenvuelve la legislación colombiana, si bien esta a mejorado a favor de los propietarios de la información, se puede concluir que en un 100% no es específica y actualizada para las nuevas tecnologías y los nuevos desafíos tecnológicos que van evolucionando en ataques más sofisticados día a día. Por ejemplo, en las situaciones que se evidencian en el día a día relacionadas con incidentes de seguridad, se aplica el código penal vigente y no siempre es posible ajustar o adaptar las leyes a los delitos informáticos nuevos. Los ciberdelincuentes no se sienten tan vigilados, pero sí más protegidos tras el anonimato que les ofrece internet, por medio de proxys anónimos y diversas tecnologías que hacen difícil individualizar a la o las personas que se encuentran detrás de estos ataques.

Por las razones anteriores, se entiende que la solución a los problemas de seguridad de la información de una compañía, además de la aplicación de herramientas técnicas de control (antivirus, antispam o cortafuegos), corresponde a la implantación de un programa de concienciación y sensibilización en seguridad que incorpore buenas prácticas para que los usuarios en sus actividades diarias, se responsabilicen del cuidado de los activos de información, previniendo y gestionando los riesgos de la organización en la vida digital y permitiéndole a la compañía diferenciarse de sus competidores.

IV. ¿ES NECESARIO UN PROGRAMA DE CONCIENCIACIÓN?

Generar conciencia acerca de la seguridad es algo que puede causar un gran debate entre los expertos,

algunos están de acuerdo en que se necesita; otros lo llaman una pérdida de tiempo y recursos.

David Aitel, en una columna para las OSC, expresó la opinión de que este tipo de formación no era necesaria:

"En lugar de gastar tiempo, dinero y recursos humanos en tratar de enseñar a los empleados a ser conscientes, las empresas deberían centrarse en dar seguridad al entorno y segmentar la red. Es una filosofía corporativa de TI mucho mejor que los empleados puedan ser capaces de hacer clic en cualquier enlace y abrir cualquier archivo adjunto, sin riesgo de dañar a la organización".

"Porque van a hacerlo de todos modos, así que puede hacer un plan para ello. Es el trabajo del CSO, CISO, o del gerente de seguridad, asegurarse de que las amenazas se detengan antes de llegar a un empleado. Y si estas medidas fallan, asegurarse de que la red esté segmentada correctamente para limitar la propagación de la infección".

Sin embargo, la otra cara de este argumento proviene de Ira Winkler:

"La pregunta que debemos hacernos es si las pérdidas evitadas por desarrollar la conciencia son mayores que el costo del programa de sensibilización. Así, por ejemplo, si todos los ataques de phishing exitosos tienen un costo asociado con el mismo, si reduce los ataques de phishing a un 50%, estará mitigando el 50% de las pérdidas potenciales".

"La opinión original también dice que un programa sofisticado de conciencia de seguridad puede evitar entre el 90-95% de los ataques. Una reducción del 90% a más de la pérdida siempre será un buen retorno de la inversión en seguridad, especialmente cuando el costo de los programas típicos de concienciación de seguridad es mínimo".

Los programas de sensibilización o concienciación no son un reemplazo de la infraestructura y las políticas de seguridad que existen o que están por ser definidas en la organización, tampoco son un sustituto para la respuesta y gestión de incidentes de seguridad. No lo pueden ser. Lo único en que se enfocan es en aumentar la posibilidad de recuperación y disminuir los tiempos de respuesta cuando ocurra un incidente.

Mientras que entrenar a los empleados para actuar como sensores de ataques de phishing o correos electrónicos con archivos adjuntos maliciosos es útil, eso no quiere decir que este tipo de campañas no tendrán éxito. Sin embargo, esto significa que el equipo de seguridad puede saber sobre el problema cuanto antes y esta podría ser la diferencia entre prevenir o sufrir un compromiso en alguna de las características de la seguridad de la información (integridad, disponibilidad, confidencialidad).

Los beneficios de implementar un plan de concienciación en seguridad de TI se pueden observar en la siguiente imagen:

Figura4. Beneficios de implementar un programa de seguridad.[8]

Además de lo anterior, si la organización está en el proceso de implementación de un SGSI o si ya lo posee, es necesario implementar un programa de concienciación según lo establece la norma NTC-ISO/IEC 27001, donde se describa claramente que las personas relacionadas con el sistema de gestión de seguridad de la información deben estar capacitadas y concienciadas.
La falta de capacitación y concienciación es uno de los principales motivos de fracaso de los proyectos de seguridad de la información en las organizaciones. La seguridad normalmente es una carga para las personas de la organización, ya que a nadie le gusta

cambiar de contraseña con gran frecuencia, además de tener que recordar contraseñas mucho más complejas. Y esta actitud se repite en las demás reglas de seguridad. Es por esto que, si no se les explica a los empleados la necesidad de llevar estos pasos a cabo, es probable que busquen algunas formas de eludir dichas reglas. La manera de abordar este tema es explicándoles los beneficios que tendrá la organización con las medidas de protección adecuadas. También es importante explicarles los beneficios que obtendrán los trabajadores con todos estos cambios. Si se utilizan contraseñas de alta seguridad, es menos probable que alguien pueda acceder sin permiso a las cuentas, ya que si esto ocurriese sería el propio empleado el que se tiene que hacer cargo de los daños que pueda producir el incidente.

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita contesta lo siguiente: los tipos de intrusos podrían clasificarse desde el punto de vista del nivel de conocimiento, formando una pirámide, así:

• Clase A: es el 80% en la base, son los nuevos intrusos que bajan programas de internet y prueban, están jugando (…) son pequeños grupitos que se juntan y dicen vamos a probar.

• Clase B: es el 12% son más peligrosos, saben compilar programas, aunque no saben programar. Prueban programas, saben cómo detectar qué sistema operativo está usando la víctima, prueban las vulnerabilidades del mismo e ingresan por ellas.

• Clase C: es el 5%, es gente que sabe, que conoce y que define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

• Clase D: es el 30% restante. Cuando entran a determinados sistemas, buscan la información que necesitan.

Para llegar desde la base hasta el último nivel, se tarda de 4 a 6 años, por el nivel de conocimiento que se requiere asimilar.

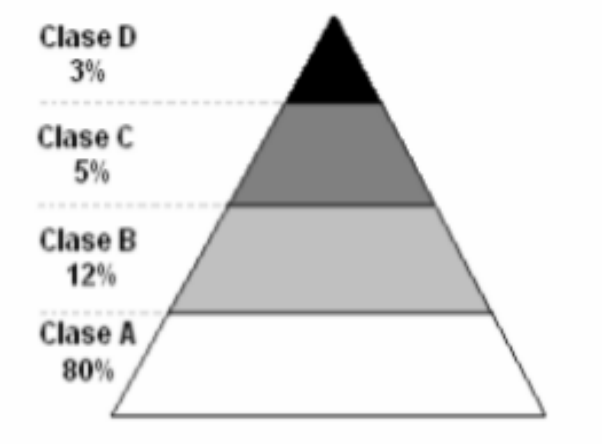

Figura5, Tipos de intrusos. [7]

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta. Puesto que se supone un entorno de confianza que en ciertos casos no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretarias, personal de seguridad, personal de limpieza y mantenimiento, entre otros) puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, nadie mejor que el propio personal de la organización conoce mejor los sistemas y sus debilidades), lo normal es que más que de ataques se trata, las situaciones corresponden a incidentes causados por un error o por desconocimiento de las normas básicas de seguridad. Se debe recordar siempre, que decir "No lo hice a propósito", no va a servir para recuperar datos perdidos, ni para restaurar un hardware dañado o robado.

V. ¿QUÉ NO ES UN PROGRAMA DE SENSIBNILIZACIÓN?

Hay que tener claridad de lo que es y no es un programa de sensibilización, por lo que las siguientes prácticas no se deben considerar como un programa, ya que muchas organizaciones confunden estas actividades con uno y no debe ser así, debido a que estas son actividades desarticulas y que no abarcan el grueso de la organización:

- Charlas presenciales donde se tocan temas generales y donde no todos participan.

- Charlas donde no se ha establecido grupos funcionales.

- Charlas que se tocan temas sin haber evaluado la necesidad de la organización

- Aficheś donde no se ha coordinado con la alta dirección sobre lo que se quiere fortalecer y como se debe comunicar

- Charlas donde no se ha determinado como medir los cambios de conducta, aptitudes y valores de los colaboradores.

- Charlas donde se explican lo que deben hacer, pero no se les indica porque lo tienen que hacer.

Un programa de concienciación es un proceso estructurado, sistemático y continúo dirigido a las personas para proporcionar y desarrollar los conocimientos, habilidades, aptitudes, valores y conductas para cumplir con los requisitos establecidos en la política de seguridad.

VI. ¿CÓMO ABORDAR EL PLAN?

Es indispensable que una vez se ha logrado definir que se va a atacar y para que se va a hacer, se genere una serie de pasos que permitan abordar el plan de concienciación, que sea exitoso para los objetivos que se pretende. Por lo tanto, es importante estructurar y hacer que el plan sea lo más completo y comprensible para los usuarios.
Uno de los principales pasos para la construcción de un buen programa de concientización sobre la seguridad es separarlo de la capacitación para el área técnica. La conciencia de seguridad no es lo mismo que la formación en seguridad cuando se trata de los empleados.

La capacitación en seguridad informática sirve para generar un conjunto de controles tecnológicos apoyado en normas y procedimientos, que es lo que la mayoría de los auditores buscan al evaluar el cumplimiento de la norma ISO 27001. Por el contrario, concientizar sobre la seguridad, tiene como objetivo modificar el comportamiento de los usuarios. Si esta labor se hace bien, los empleados de la compañía se convertirán en una extensión del programa de seguridad existente. Sin embargo, mientras que la capacitación en seguridad puede hacerse anualmente para el personal técnico involucrado, los programas de sensibilización son un proceso continuo que debe ser objeto de una revisión para asegurar el mejoramiento continuo.

Basado en lo anterior, se debe llevar una serie de pasos que aseguren que el programa sea exitoso. Esto deberá incluir una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a concienciación y formación en este tema.

Los pasos que se deben seguir al llevar a cabo un programa exitoso son:

a) Establecer el plan. En este punto se debe tener en cuenta los siguientes factores:
   - Objetivos
   - Programa.
   - Factores de éxito.
   - Modelo.
   - Recursos.

b) Implementar. En este punto se debe tener en cuenta los siguientes factores:
   - Alcance del programa.
   - Información necesaria.
   - Selección de los temas.
   - Desarrollo de los contenidos y sus métodos.
   - Elaborar el plan.
   - Ejecutar y monitorear el plan.
   - Comunicar los resultados.

c) Monitoreo y revisión. En este punto se debe tener en cuenta los siguientes factores:
   - Establecer los criterios de evaluación.
   - Monitorear revisar y evaluar.

d) Mejora. En este punto se debe tener en cuenta lo siguiente:
   - Implementar Mejoras.

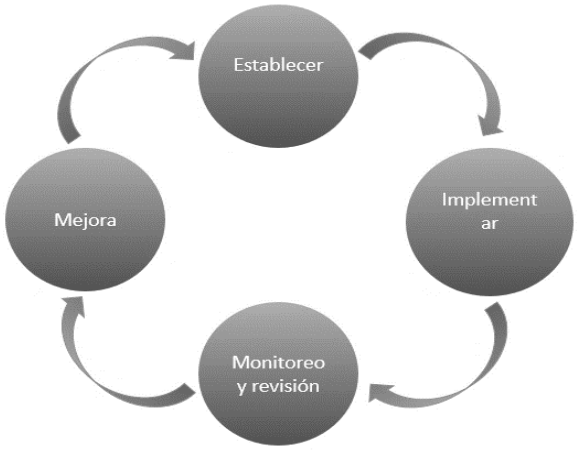

Figura7. Fases de la implementación.[8]

Un programa de concienciación debe incluir:

1. Políticas y objetivos del programa de concienciación.

2. Criterios de análisis y evaluación de los resultados del programa

3. Alcance del programa de concienciación

4. Estructura del cuadro de mando (objetos y atributos de medición).

5. Organización del programa de medición (asignación de responsabilidades, competencias y recursos).

6. Identificar los factores de éxito y los riesgos del programa de concienciación.

7. Establecer el proceso y los procedimientos del programa (recolectar datos, elaboración de métricas e indicadores, generación de los informes).

8. Establecer las técnicas y métodos.
9. Definir los objetivos específicos de los temas a abordar.

10. Establecer la planeación de las mediciones y la forma de llevar a cabo las actividades.

11. Informes de los resultados de los temas explicados.

12. Monitorear, revisar y mejorar el programa.

Al elaborar un programa de concienciación se debe tener en cuenta el perfil de los usuarios o la jerarquía, ya que para cada grupo objetivo se debe crear un material apropiado de acuerdo con sus funciones. Estos se definen en tres grandes grupos.

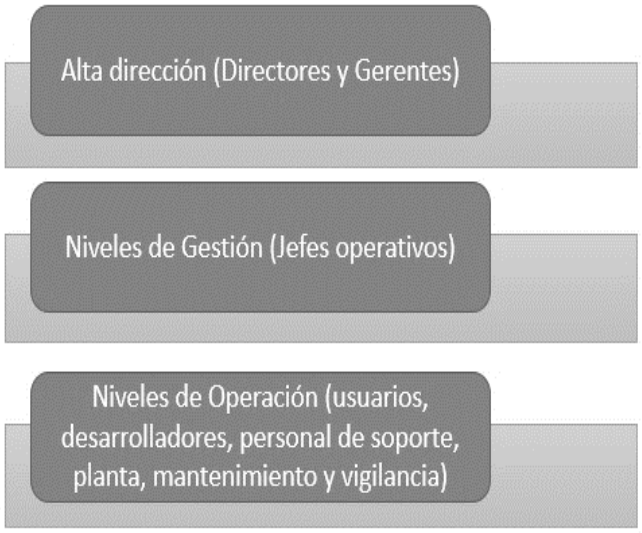

Figura8. Jerarquías.[6]

Los controles se clasifican en dos niveles de complejidad:

- Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Alcance de los controles:

- Procesos (PRO): aplica a la dirección o al personal de gestión.

- Tecnología (TEC): aplica al personal técnico especializado.

- Personas (PER): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Difusión de la política de seguridad** Documentas y difundes las normas de ciberseguridad de tu empresa para que estén siempre accesibles.	☐
B	PRO	**Concretar el plan de formación** Elaboras o revisas el plan de formación para elevar el nivel de seguridad de tu plantilla.	☐
B	PRO	**Programas de formación específicos** Desarrollas y aplicas programas de formación en ciberseguridad adecuados a los distintos puestos de trabajo.	☐
B	PRO	**Periodicidad de la formación** Tus empleados realizan cursos o van a charlas de concienciación, cada _____.	☐
B	PRO	**Evaluar el aprendizaje obtenido** Compruebas la asimilación del conocimiento adquirido por tus empleados.	☐
B	PRO	**Promover una cultura de seguridad de la información** Promueves una cultura de seguridad de la información que abarca a toda la cadena de suministro de la empresa y a tus clientes.	☐

Fugura9. Check List. [5]

A. Puntos clave

Los puntos clave de esta política son:

- Difusión de la política de seguridad. Las normas de seguridad de la información de las organizaciones deben estar correctamente documentadas y al alcance de todo el personal en todo momento.

- Concretar el plan de formación. Para garantizar el éxito del programa formativo, se deben seleccionar los aspectos que se quiere sean cubiertos:

    - Procedimientos y controles de seguridad básicos.
    - Necesidad de conocer y cumplir normas, leyes, contratos y acuerdos.
    - Seguridad en el puesto de trabajo, aplicaciones permitidas, uso correcto de los recursos, propiedad intelectual, protección datos personales, etc.

    - Concienciar a los empleados sobre la existencia y peligros de la ingeniería social.

    - Responsabilidad personal por acción u omisión y posibles sanciones.

- Programas de formación específicos. Es conveniente analizar si se deben desarrollar programas de formación y concienciación especializados para ciertos perfiles de empleados, tales como técnicos de soporte, administradores de sistemas, etc. Además, sería de gran utilidad elaborar una actividad formativa introductoria para los nuevos empleados.

- Periodicidad de la formación. Se debe establecer una periodicidad en las actividades formativas y de concienciación. De esta manera se consigue tener unos contenidos actualizados en materia de ciberseguridad y se reforzarán las debilidades detectadas o los mensajes de mayor importancia.

- Promover una cultura de seguridad de la información. Además de concienciar y formar a los empleados en ciberseguridad.Es conveniente exigir a las entidades externas que interactúan con los sistemas de información que sus políticas de ciberseguridad estén alineadas con la de la organización. Se debe extender el plan de concienciación a la mayoría de los proveedores y clientes.

- Evaluar el aprendizaje obtenido. Se debe considerar la necesidad de realizar evaluaciones entre los empleados para determinar el grado de concienciación y formación que sé ha alcanzado.

VII. EVALUACIÓN

Finalmente, para asegurar que el programa haya cumplido sus objetivos y que en realidad el público en general apropio los conceptos, se debe realizar una evaluación que permita medir y observar si se cumplió con dicho propósito o si por el contrario hay que hacer ajustes.

Como lo dice la European Network And Information Security Agency, Enisa: "Un punto de partida determinado antes de la puesta en escena ofrece una instantánea dentro de los grupos destinatarios. El cumplimiento de los objetivos debe revisarse a la vista de los resultados obtenidos y de la eficacia de los mismos. Si el plan no garantiza los resultados deseados, se debe modificar e iniciar nuevamente" [1].

A continuación, se enumeran ciertos factores a tener en cuenta para lograr una evaluación satisfactoria:

- Se debe tener cuidado con la implementación de tecnologías nuevas. La tecnología normalmente avanza más rápido que cualquier programa de concienciación.

- La correcta segmentación del auditorio es un factor decisivo. Hay que olvidar la expresión "Todos por igual", porque en la organización, los destinatarios nunca van a ser iguales.

- Un error muy común, es el "exceso de información".

- La falta de organización y seguimiento, pueden tirar todos los esfuerzos por la borda.

- El mensaje debe llegar donde debe llegar y para esto hay que explicar los motivos del programa.

- La ingeniería será la piedra en el zapato, por lo cual se debe prevenir a los destinatarios.

VIII. CONCLUSIONES.

La información es uno de los activos más importantes de toda organización por lo tanto, se le debe dar un tratamiento seguro. Lo anterior, hace que la información se convierta en el activo más importante y por esto de ser el eje central sobre el cual debe girar la seguridad, definiendo acciones de protección y mecanismos de control para garantizar al negocio, la integridad, disponibilidad y confidencialidad de dicha información.

La confidencialidad de la información es una característica requerida para las organizaciones modernas, donde no satisfacerla adecuadamente, implica posibles fallas que pueden poner en riesgo los negocios. Por esto, comprender la inseguridad de la información, más que detectarla, exige una reflexión profunda de la organización para avanzar en la gestión de la seguridad de la información.

Una forma de garantizar el tratamiento seguro de la información sensible y confidencial de la compañía es: evitando que ésta se vuelva pública de forma no autorizada, es el diseño e implementación de un programa de concienciación en seguridad de la información que pueda ser usado por las compañías para mostrar a los empleados, aquellos comportamientos que pueden provocar un problema de seguridad para la protección de los activos de información.

REFERENCIAS.

[1] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, ENISA. (2006). Guía del usuario: Elaborar programas de sensibilización sobre la seguridad de la información.

[2] MELZNER, S. (2009). "La diferencia entre datos e Información", [en línea], disponible en: http://sergiomelzner.com/negocios/la-diferencia-entre-datos-e informacion/

[3] SEGU-INFO. "Políticas de Seguridad de la Información", [en línea], disponible en: http://www.segu-info.com.ar/politicas/polseginf.htm

[4] "Manual de Seguridad en Redes", [en línea], disponible en: http://www.arcert.gov.ar/webs/manual/manual_

de_Seguridad.pdf

[5] INCIBE – PROTEGE TU EMPRESA – Kit de concienciación, [en línea], disponible en: *https://www.incibe.es/protege-tu-empresa/kit-concienciacion*

[6] CONCIENCIACION EN SEGURIDAD - [en línea], disponible en: *www.prime.pe*

[7] *EL FRAUDE INFORMATICO - [en línea], disponible en: http://www.cybsec.com/*

[8] Figura propia del autor.

Autor.

David Alexander Guatavita Diaz, ingeniero de sistemas, con experiencia en temas de infraestructura tecnológica, redes y servidores, en los últimos 2 años he venido incursionando en el tema de Seguridad. Actualmente trabajo para el gobierno colombiano a través del Instituto Nacional de Vias -INVIAS- donde me desempeño como ingeniero de infraestructura y seguridad.