Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

EL FACTOR GENTE Y LA SEGURIDAD DE LA INFORMACION

Abstract — *La importancia de las normas de "seguridad de la información" se viene extendiendo a nivel corporativo como un componente de negocios, más allá del concepto de "seguridad informática" limitada al área tecnológica. Efectivamente, tanto los Principios del Gobierno Corporativo como las Guías de Seguridad de la OECD (Organización para Cooperación y Desarrollo Económico) conducen a considerar también los riesgos organizacionales y operacionales. Aquí es donde aparece el "factor gente", individuos y grupos, generalmente descuidado y/o desconocido, incluso por el "management", al implementar medidas de seguridad. Como tales medidas generalmente plantean cambios de conducta, pueden entrar en conflicto con los esquemas de las personas, por su resistencia natural a los cambios y los mecanismos de defensa que se disparan. Esto nos dice que se necesita no sólo concientización sino un comportamiento adecuado, todo lo cual requiere una amplia discusión a todo nivel y el aporte de disciplinas como la Psicología Social.*

Palabras Clave — *creencia, conocimiento, actitud, comportamiento, comunicación, participación, compromiso, responsabilidad, cultura corporativa, concientización, gente, resistencia al cambio, seguridad de la información, seguridad informática, medidas de seguridad.*

INTRODUCCIÓN

Generalmente se dice que virus y hackers son quienes ponen en riesgo la información. Pero muchas veces la verdad es otra: que el descuido y el uso inadecuado de usuarios legítimos causen mucho mayor daño que aquellos.

Esto se pone de manifiesto en un escenario corporativo cuando al analizar los riesgos organizacionales y operacionales [1], surge un factor generalmente descuidado y a veces hasta desconocido relacionado con las personas y los grupos, y que llamamos el "factor gente"[1].

Por ejemplo, muchos de los desaciertos y fallas en los planes de seguridad que suelen encontrarse se deben a que el personal técnico no conoce suficientemente los riesgos no técnicos, y de allí que tampoco la problemática y gestión del comportamiento de las personas, con todo lo que implica a nivel de la implementación de medidas de seguridad.

Incluso, en parte como consecuencia de todo ello, puede ocurrir que alguna empresa tenga un grueso manual de Políticas de Seguridad Informática, en algunos casos finamente encuadernado y con el sello de importantes consultoras, pero... ¡que muy pocas personas lo han leído y menos aún llevado a la práctica!

Este tipo de experiencias, propias y de terceros, señala que ***la seguridad de la información depende de la gente***, individuos y grupos, ***más que de la propia tecnología***, toda vez que las personas son el eslabón más débil en el cumplimiento de medidas de seguridad. Y esto es así porque la naturaleza humana y las interacciones sociales son frecuentemente más fáciles de manipular que producir brechas en las protecciones tecnológicas.

Efectivamente, a menudo se da que la explotación de las debilidades del comportamiento humano puede soslayar controles técnicos y procedimientos existentes. Es el caso de la **Ingeniería Social**, es decir la forma de persuadir a las personas para que proporcionen información confidencial.

En consecuencia, la implementación efectiva de un plan de seguridad no se logra desde un punto de vista exclusivamente técnico, sino teniendo en cuenta el comportamiento humano y el contexto social en el que las personas están inmersas.

1010

[1] Lo denominamos *factor gente* en lugar de *factor humano* porque "gente" involucra al individuo y al colectivo.

Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

Lo comentado hasta aquí señala que las medidas de seguridad requieren cambios de actitudes y comportamiento, lo que naturalmente genera sensaciones negativas en la mayoría de las personas, por su resistencia natural a los cambios y los mecanismos de defensa que se disparan.

La gestión de cambios de conducta a nivel personal, grupal y aún organizacional, incluyendo las redes sociales internas y la propia cultura corporativa, nos enfrenta con ciertos desafíos de características nada técnicas, que van desde un mejor conocimiento de las personas hasta la capacidad de liderar esos cambios.

El panorama planteado es bastante complejo y, salvo escasas excepciones [2] [3] [4], está muy poco o sólo parcialmente contemplado en las buenas prácticas de seguridad de la información. No es el único caso; algo similar ocurre en otras actividades de diferentes disciplinas y otros ámbitos frente a cambios organizacionales.

Para circunscribir la situación apelamos a un razonamiento heurístico considerando no sólo las relaciones causa-efecto sino también, al amparo de un pensamiento lateral, las características que aunque disímiles pudieren aportar a la resolución de las cuestiones planteadas. Adicionalmente procuramos apoyo profesional en cuanto al conocimiento y gestión de las personas, como se comenta más adelante. A continuación se presentan algunos de los aspectos más relevantes que facilitaron el manejo y logro de las metas requeridas.

RESISTENCIA A LOS CAMBIOS

Las sensaciones negativas mencionadas surgen casi naturalmente al implementar medidas de seguridad, ya que en muchos casos dichas medidas pueden entrar en conflicto con los esquemas de las personas, esquemas que responden al cuadro complejo de la realidad sobre el cual basamos nuestros juicios y la forma en que consideramos nuestras interrelaciones sociales.

Esta reacción se manifiesta por el comportamiento de una persona tendiente a retardar, desacreditar, desestimar o impedir la realización de un cambio.

La resistencia al cambio puede responder a factores lógicos. como por ejemplo al posible extendido tiempo y esfuerzo que puede demandar la nueva situación, así como al entorno psicológico de las emociones, sentimientos y actitudes de una persona, y también a características sociológicas de valores sociales basados en criterios y/o intereses grupales.

Esta resistencia no es pareja en todas las personas. Los psicólogos nos dicen que tales diferencias responden a la transferencia de escenarios que cada persona trae inconscientemente del pasado. También, que la visualización de tales escenarios es un acopio personal que puede generar en algunos casos una fuerte resistencia al cambio.

Todo esto nos indica que para obtener resultados adecuados en los planteos hechos hay que ahondar en las raíces de esta problemática, lo que requiere un minucioso análisis, estudio y consideración.

CREENCIAS, CONOCIMIENTO, ACTITUD Y COMPORTAMIENTO

El análisis comienza con cuatro conceptos básicos: *qué cree, qué sabe, qué siente* y *qué hace* una persona, en nuestro caso frente a medidas de seguridad.

Una **creencia** es una actitud o estado mental que considera como cierta una información determinada. Las creencias son las bases personales subjetivas del comportamiento del individuo.

Según los epistemólogos, el **conocimiento** es algo que se “sabe” sólo cuando es una creencia cuya verdad puede justificarse. La condición de verdadera es un estado objetivo independiente de la persona. Necesitamos entonces que las creencias a transferir deriven en un conocimiento preciso.

La **actitud** se refiere a una evaluación o *respuesta emocional* respecto de objetos o hechos. En las actitudes de una persona pueden influir una cantidad de condiciones propias y también externas que han sido investigadas especialmente por algunos estudiosos del tema.

Según Herzberg hay dos tipos de factores que actúan por separado en las actitudes de las personas: Los factores de satisfacción o insatisfacción en el ambiente de trabajo, y los factores motivadores dados por los estímulos recibidos.

Por su parte, Maslow establece que las actitudes de las personas se modelan a partir de las necesidades personales, no sólo las básicas de supervivencia y seguridad sino también en un entorno de gestión participativa como se verá más adelante, las necesidades sociales en cuanto a su aceptación y valorización por los demás, así como las necesidades de reconocimiento y autorrealización.

Los estudios muestran que aún estímulos aparentemente menores pueden influir en las actitudes. Es el caso de los premios, incluso pequeños pero que refuercen las acciones hacia lo buscado. Por ejemplo algo tan simple como un caramelo o dulce en el escritorio de las personas que al retirarse al fin del día se han deslogeado de sus máquinas y/o no han dejado papeles sobre el escritorio y cerrado con llave los archivadores o gavetas que contienen documentos.

Creencias, conocimiento y actitudes pueden ir desparejos. Se puede tener claro y justificado (*conocimiento*) que no debe bajarse de la Web material resguardado por la propiedad intelectual, pero igualmente hacerlo pensando (*creencia*) despreocupadamente (*actitud)* que nadie lo notará.

El **comportamiento** de una persona está relacionado habitualmente con su estilo personal, es decir su personalidad. Las personas pueden clasificarse según diferentes tipos de personalidad, como Carl Jung lo sugiriera originalmente, a partir de indicadores basados en dicotomías o conceptos opuestos.

Posteriormente, Myers-Briggs extendieron a cuatro los indicadores de personalidad: extrovertido o introvertido, sensible o intuitivo, racional o emocional, y juicioso o perceptivo, con lo que resultan 16 tipos diferentes de personalidad. Puesto que el comportamiento se encuadra según estas categorizaciones, se puede deducir que algo similar ocurrirá con respecto a los riesgos y las correspondientes respuestas personales.

Por otra parte, no siempre el *comportamiento* se corresponde con la *actitud*. Consideremos dos casos.

Uno se da cuando el comportamiento de una persona no responde en realidad a sus propias actitudes, sino que se adapta al comportamiento dominante en un grupo.

Otro caso puede darse como resultado de entrevistas personales con quienes por ejemplo han contestado previamente a cuestionarios como los propios del Método Delphi de investigación prospectiva. Entrevistas que buscan establecer el nivel de credibilidad de esas personas y apreciar si se corresponden actitudes y comportamientos.

Estas entrevistas, como en otras interacciones personales y grupales, pueden conducir a interpretaciones incorrectas, conocidas como **errores de atribución**. Esto ocurre al no considerar el contexto de los hechos y/o la existencia de prejuicios ante características o rasgos personales que aún destacándose, pueden derivar de una primera impresión o impresiones parciales que no identifican realmente a las personas.

Salvando distancias y en sentido opuesto es lo que ocurre con el Phishing -un tipo de ingeniería social- que en forma de e-mail *parece* venir de una institución legítima, como un banco, con una advertencia de medidas no deseadas contra el destinatario, por lo cual se solicita generalmente dar clic a un sitio Web, aparentemente también legítimo y similar al verdadero, donde se le piden datos privados como contraseñas, etc.

En los cambios de comportamiento hay un aspecto muy importante a considerar, además de entender claramente lo que se busca. Se trata de reconocer los llamados *habilitadores* y *bloqueadores* que actúan en las conductas humanas.

Los ***habilitadores*** son patrones de pensamientos positivos que posibilitan el éxito. Se manifiestan cuando se hacen preguntas que revelan interés y el propio lenguaje corporal en su aspecto positivo. El sustento principal de su acción radica en creer en las propias condiciones y capacidades propias, la autoestima, ver las cosas nuevas como oportunidades, y aceptar responsabilidades que pueden potenciar las posibilidades personales y laborales.

Los ***bloqueadores***, por su parte, son patrones de pensamientos negativos. Aquí podemos mencionar la ya comentada resistencia al cambio, así como también características personales no orientadas a la acción, debido a dejar las cosas para después y la propia pasividad, la formulación de excusas racionales pero de comportamientos irracionales, y por sobre todas las cosas, simplemente el no sentirse suficientemente cómodo con algo.

Los bloqueadore***s*** de la comunicación se manifiestan por ejemplo en distintas formas de interrumpir una conversación, la tendencia a considerar fallas o problemas como de otros y no propios, expresiones rotundas reiteradas respecto al comportamiento como “siempre” o “nunca”. Y también en forma pasiva pero con lenguaje corporal, alejándose del interlocutor o por medio de ciertas expresiones en la cara.

Resumiendo se puede decir que lograr un cambio de comportamiento, no sólo en los demás sino en uno mismo, es el mayor desafío a enfrentar. Para ello se necesita tener claro el comportamiento deseado, así como reconocer los habilitadores y bloqueadores, identificando motivadores adecuados de fortalecimiento y compensación respectivamente.

Para producir cambios de *comportamiento* hay que trabajar sobre las *actitudes*. Y para influir sobre las actitudes se hace necesario persuadir para desarrollar *creencias* que lleguen a constituir verdadero *conocimiento*.

COMUNICACIÓN

La persuasión, o sea cambiar las actitudes de una persona o grupo, y así influir en su comportamiento, se describe en términos de la **comunicación**. Pichón Rivière dice que la comunicación es el riel del aprendizaje para que éste sea posible y exista, con lo que se resalta la importancia capital de las interacciones personales en el camino de la producción de cambios.

Aquí se pueden plantear conceptos en base a *quién*, *qué* y *cómo*. O sea, quién debe comunicar las medidas de seguridad, qué decir y cómo decirlo.

En primer lugar, ***quién*** comunica debe tener capacidad de comunicación; ser didáctico, conocer lo que piensan los demás, sus actitudes y creencias, y comprender su comportamiento evitando los errores de atribución.

Qué se dice depende de las personas que reciben la comunicación, sea un usuario operativo, un técnico o un ejecutivo.

Cómo se comunica es un poco un arte; el comunicador debe ser persuasivo y evitar tanto la forma meramente discursiva como las indicaciones perentorias. La aspereza en palabras y gestos genera resentimiento.

La forma de comunicar cambia cuando se habla ante un grupo o en forma individual. Una forma de comunicación estructurada con un grupo de personas puede concretarse por medio de reuniones de trabajo y aún reuniones informales. La variante no estructurada, en cambio, es la interacción directa con otra persona.

En las conversaciones individuales hay que considerar el estilo del interlocutor. Hay personas más abiertas pero también las hay cerradas o reservadas. Y en un contexto dialéctico hay quienes van directamente al grano, mientras otros son más reflexivos.

En la comunicación, muy especialmente en las reuniones personales, es recomendable tener en cuenta un criterio similar al comentado al hablar de las diferentes personalidades. Por ejemplo, una persona "sensible" tendrá mayor preferencia por los detalles que otra del tipo "intuitivo".

Además, al hablar puede ser más importante lo gestual de las actitudes que el contexto de lo que se dice. Y que comunicarse es algo más que simplemente hablar. Es una calle de doble vía; también hay que escuchar lo que dicen los demás.

PARTICIPACIÓN, COMPROMISO Y RESPONSABILIDAD

Sabemos que la implementación de medidas de seguridad puede provocar reacciones negativas, sea por una percepción de pérdida de la libertad de acción por parte del personal en general, o bien una supuesta invasión al área de los técnicos, o hasta displicencia o desinterés incluso en ejecutivos.

Veces hay en que los efectos de tales circunstancias pueden ser más profundos aunque más bien pasivos, efectos tan adversos que a algunas personas puede costarle reaccionar positivamente de tal situación.

Estas situaciones se corresponden con el concepto de ***Resiliencia***, es decir, la característica de resistir y superar efectos adversos, reaccionando positivamente frente a las dificultades, tomándolas incluso como puntales de fortalecimiento.

Pilares de la resiliencia son una autoestima consistente, introspección, independencia de pensamiento, capacidad de relacionarse y la toma de iniciativas.

La mayor o menor resiliencia es uno de los aspectos de la ***Inteligencia Emocional*** que engloba el control y manejo de las percepciones y reacciones de las personas.

Otro de los aspectos de la Inteligencia Emocional se refiere al manejo interpersonal que entra en juego cuando las personas interactúan entre sí. En este punto se pueden mencionar la empatía, la capacidad de influir, la comunicación (incluso el liderazgo) y demás habilidades que permiten un funcionamiento provechoso a los miembros de un grupo.

El equilibrio y la visión positiva propios de la Inteligencia Emocional se vuelcan en acciones a partir de la capacidad de *participación, compromiso y responsabilidad*.

La **Participación** es el proceso que permite a las personas ejercer mayor influencia sobre las condiciones de su trabajo. Se trata de un concepto bastante reconocido y comentado últimamente, y de hecho es uno de los pilares básicos de la Gerencia Participativa y de la Gerencia por Objetivos.

La importancia de facilitar la participación del personal en una empresa se basa en factores como:
a) El personal conoce como nadie las tareas que se realizan.
b) El resultado de una motivación adecuada conduce a una formación y capacitación consistente.
c) La generación de un importante nivel de compromiso entre el personal gerencial y el operativo.

La participación es crítica para el éxito de un proyecto. La experiencia muestra que la mejor forma de llevar adelante un cambio, tal como la implementación y vigencia de medidas de seguridad, es promover que el personal participe en el proceso mismo, ganando así confianza mutua y credibilidad. Generalmente a mayor participación menor será la resistencia al cambio, y más estable el cambio con el correr del tiempo.

Para establecer tal participación hay que conocer primero qué motiva a las personas en cuanto a sus necesidades personales como ya se comentara. De hecho, la participación resulta ser un mecanismo motivador importante al permitir satisfacer las necesidades de reconocimiento y autorrealización,

Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

fortaleciendo las capacidades del personal y ampliando sus perspectivas. En este punto se destaca el trabajo de Mc Gregor que postula los valores humanos y sociales, posicionando al hombre como persona y nó como un recurso, destacando la iniciativa individual.

Que las personas se involucren en algo tiene su razón de ser básica en la psicología de dichas necesidades y en los factores motivadores que modelan sus actitudes, por lo cual la motivación y el comportamiento de la gente son elementos primordiales del éxito de un proyecto.

Además, para una participación adecuada, el personal necesita que se les provea con información relevante al caso. Una buena estrategia en este punto puede comenzar proporcionando al personal el conocimiento adecuado y haciéndoles saber el comportamiento esperado, teniendo en cuenta las diferentes actitudes de las personas. Y que dicho enfoque en el caso del personal de supervisión sea trasladado luego de manera análoga al personal que cada uno tenga a su cargo.

Un ejemplo significativo de participación es el conocido concepto del “buy in” que en nuestro caso puede aplicarse diciendo que la gente “comprará” un plan de seguridad si ha participado activamente en el proyecto.

El **Compromiso** responde al involucramiento de las personas en las metas de un proyecto. Suele decirse que el compromiso es concomitante de la participación. Más exacto probablemente es decir que una participación directa adecuada conduce a un mejor compromiso en la formación de la **Responsabilidad** correspondiente, incluyendo el establecimiento de roles que faciliten la auditoría de la aplicación de estos conceptos.

El compromiso puede verse en función tanto de factores organizacionales situacionales como del factor de la predisposición personal de cada uno. También se lo puede considerar como una construcción multidimensional, los individuos del grupo y las razones que motivan la adhesión de cada uno al grupo.

En nuestro caso, el compromiso se puede lograr partiendo de una definición clara de metas y objetivos para que el personal se involucre y comprometa en un proyecto como el de seguridad; en primer término los principales ejecutivos de la empresa como foco de difusión, así como en forma especial los miembros del Foro (ver recuadro **Foro de Gestión**) que habitualmente instalamos en nuestros proyectos de seguridad.

La aplicación del concepto “buy in” puede no ser suficiente para algunos integrantes del Foro de Gestión. Son los que, además de discutir la redacción y aplicación de los controles de seguridad, después tendrán que coordinar posteriormente sus respectivos grupos operativos, asumiendo la responsabilidad de manejar de manera similar al personal correspondiente. Se necesita entonces también propender a un nivel adecuado de liderazgo.

Los coordinadores y supervisores pueden llegar a ser los más influyentes en la motivación del personal para el cambio, y ayudarlos en la transición correspondiente. Por eso deben recibir una atención especial, incluso primeramente para convencerlos de la necesidad de cambios.

Su trabajo incluirá también promover la formación de valor en la gestión en su personal, asumiendo la responsabilidad de actuar sobre ellos para transformar las conductas que hagan a los cambios que implica un plan de seguridad.

Una de las formas más eficaces de lograr este objetivo es por medio de reuniones individuales adicionales al Foro de Gestión, complementadas con reuniones grupales de coordinadores/supervisores, que pueden servir para compartir ideas y experiencias, al tiempo que el centro de la escena se corre del capacitador principal, con la ventaja que eso significa. También, es un buen escenario para discutir innovaciones que impliquen mejoras en los procesos de cambio correspondientes a la implantación de medidas de seguridad.

Aunque en general se necesita promover en forma conjunta el compromiso y la participación, e incluso suele decirse que no hay compromiso sin participación, puede haber excepciones aceptables. Es por ejemplo el caso de ejecutivos que aunque no participen activamente en un proyecto, igualmente establecen el compromiso y asumen la responsabilidad dada por el apoyo necesario para promover y sostener el proyecto.

FORO DE GESTIÓN

El propósito del Foro de Gestión en un proyecto de seguridad de la información es la participación de las personas a las que atañen las políticas y controles que se deben implementar, dentro de un marco dialéctico. De esta manera se busca lograr un consenso lo más amplio posible en la redacción de las medidas correspondientes facilitando así su puesta en vigencia.

El Foro de Gestión responde a un mecanismo colectivo de participación de composición dinámica. No es un único grupo sino que para cada tema se forma un grupo con las personas que guarden relación por sus propias actividades.

Para ello se manejan grupos ad hoc del tipo mixto multifuncional, es decir, de distintas áreas y niveles jerárquicos de la empresa, para lo cual debe haber personal con cierto nivel de capacidad para tomar decisiones tales como coordinadores y supervisores, personal técnico de Sistemas y Tecnología, y usuarios de operaciones de las áreas en cuestión.

Estos últimos son importantes, porque los trabajadores que realizan el trabajo del día a día ven los defectos, errores y fallas, tiempos perdidos y otras características que pueden necesitar tratarse. Son los que pueden decir cuán fácil o difícil resultará de llevar adelante un control o política, haciéndolos realmente aplicables e incluso facilitando posteriormente la medición de su efectividad, determinación que hoy día puede basarse en la ISO 27004, por ejemplo mediante el uso del Balanced Scorecard (BSC).

Los técnicos, por su parte, muchas veces tienen cuestiones propias del área con relación a las medidas de seguridad, y además pueden aclarar las interacciones con otros controles.

Finalmente el personal decisor con su comportamiento y participación es el que deberá apoyar definitivamente la adopción de las medidas correspondientes.

Para que el Foro de Gestión sea productivo y eficaz debe reunir en sus objetivos:
a) Propiciar un ambiente de colaboración y apoyo recíproco entre sus integrantes, facilitando que las personas se manifiesten y ofrezcan sugerencias.
b) Motivar y crear conciencia del trabajo que se realiza.
c) Facilitar una mejor comunicación entre el personal en general y los de mando que participen.

La participación, compromiso y responsabilidad de los miembros de un Foro de Gestión simplifican la transferencia a terceros de los alcances de cada control, reduciendo la resistencia natural a las medidas de seguridad y facilitando su aceptación.

CULTURA CORPORATIVA

La Cultura Corporativa concibe la organización como una malla organizativa. Surge a partir de los Valores establecidos con la Misión de una empresa, valores que son las creencias, costumbres y prácticas que comparten los que manejan una organización.

La cultura corporativa de una organización tiene diferentes componentes que pueden categorizarse como sigue. Hay formas del tipo funcional que se basan en las jerarquías y la estructuración del trabajo. Otras se adaptan a los procesos de trabajo según las demandas del mercado. Y finalmente están las que buscan maximizar el rendimiento de los recursos propios.

En una organización conviven diferentes proporciones de estas manifestaciones de cultura. Generalmente la forma funcional es la más reacia a los cambios.

Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

Para mejorar la seguridad y específicamente la aceptación de las medidas correspondientes se requiere un ***cambio*** de creencias, actitudes y comportamiento tanto individual como grupal. En este punto, y tal como se comentara antes, la interpretación del comportamiento de las personas es crítica para comprender el escenario de un cambio de la cultura corporativa.

Para lograr los cambios deseados hay que procurar por medio de sucesivas charlas a niveles gerenciales, que estas personas lleguen a considerar la seguridad de la información como parte de las propias estrategias corporativas y por ende de la ***gestión y riesgos de negocios*** [5]. Esta es la visión que va más allá de lo estrictamente técnico que durante mucho tiempo ha venido dejando en un segundo plano las características más profundas de la seguridad de la información.

Por su parte, las charlas de concientización y educación a nivel personal y grupal extendidas a toda la organización constituyen un pilar fundamental especialmente en cuanto a los riesgos operacionales. Estas charlas fomentan la integración de la seguridad de la información en la cultura corporativa, y se potencian usando técnicas de ***Psicología Social***.

A veces no es fácil conseguir una audiencia plena para producir mejores resultados. Una oportunidad que se nos ha dado, surge cuando las empresas ya trabajan con Kaizen como estrategia que promueve actividades con participación del personal para la solución de problemas y la *mejora continua* de los procesos. Kaizen, por cierto, también se enfoca fuertemente en el tema de la participación y compromiso comentado antes.

La integración de las charlas generales de seguridad en las sesiones de Kaizen puede entonces resultar beneficiosa puesto que estas últimas generalmente concitan mayor interés y dedicación, además de ser promovidas específicamente por la alta gerencia en la mayoría de los casos.

DISCIPLINAS DE SOPORTE

La ***Psicología Social*** ya mencionada trata principalmente los grupos y el comportamiento en las interacciones entre las personas. Ofrece un adecuado aporte en cuanto a la comunicación y aprendizaje, la coordinación de grupos operativos, y en general las cuestiones que ayudan a comprender cómo trabajar mejor con las preferencias y predisposiciones de las personas. Ha venido resultando nuestro principal apoyo.

Adicionalmente la ***Psicología Conductista*** puede aportar una visión interaccionista entre el individuo y los individuos, aunque por otro lado puede limitar la concepción de algunas características de las personas en relación con los fenómenos sociales.

Especialmente en el ámbito de la comunicación puede ayudar el ***PNL*** o ***Programación Neurolinguística***. El PNL se enfoca en el individuo y la comunicación verbal y no verbal -es decir gestos, posturas, tono de la voz, etc.- que surgen de las relaciones interpersonales en cuanto a su contribución a los cambios buscados. El PNL permite comprender cómo las personas organizan sus pensamientos, sentimientos, lenguaje y comportamiento en sus acciones y en la producción de resultados.

También se destaca el ***Coaching*** que, con distinta estructura y contexto, tiene puntos en común con el PNL, como por ejemplo el cambio y las formas de lograrlo, aunque también busca mejorar el rendimiento y orientar al liderazgo. El Coaching es una herramienta muy adecuada para la atención requerida hacia los coordinadores y supervisores ya comentada antes, especialmente en el análisis del Compromiso y Responsabilidad.

BASES DE UN PROGRAMA DE ACCIÓN

Como todo programa de cambio se requiere una adecuada planificación, la identificación de los requerimientos y cuestiones claves, el análisis del origen de las situaciones que se plantean, y la determinación y desarrollo de las acciones a realizar.

Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

Conforme los antecedentes reunidos y comentados hasta aquí, un programa típico puede estructurarse como sigue.

En primer lugar se trabaja con cuestionarios para detectar los conocimientos, actitudes y comportamiento del personal involucrado en el proyecto de seguridad.

Estos cuestionarios se preparan teniendo presente siempre a las personas que van a contestar, y en base a tres grupos diferentes: usuarios en general, técnicos y personal gerencial. En el primer caso se trabaja con preguntas cerradas, es decir las que dan lugar a respuestas breves y concretas. Por el contrario para los técnicos y el personal gerencial algunas preguntas se redactan en forma abierta como para dar lugar a recibir mayores detalles.

A su vez, cada cuestionario se confecciona en tres partes. Una para establecer qué saben (*conocimiento*) las personas de las políticas y normas de seguridad. Otra para visualizar qué piensan (*actitud*) respecto de la seguridad y cómo la ven. Y finalmente, una tercera para detectar cómo actúan (*comportamiento*) frente a responsabilidades como por ejemplo la elección de contraseñas, cuidado con papeles y documentos en sus escritorios, etc.

En cuanto a la comunicación se trata de tener en cuenta los aspectos comentados especialmente en cuanto a resistencia al cambio, actitudes, comportamientos, y las consideraciones hechas en el recuadro ***Foro de Gestión***.

El proceso comunicacional se basa en charlas generales y reuniones individuales en el caso de los ejecutivos y algunos técnicos. En general en las primeras charlas y siempre que se considere necesario se busca iniciar las sesiones motivando la participación por medio de comentarios ajenos a la seguridad, buscando así vencer el escepticismo y posiciones a la defensiva que pueden tener algunas personas.

Especialmente en las conversaciones individuales hay que considerar la personalidad de la otra parte, como ya se comentara antes, para manejarse así en un escenario en que pueda sentirse cómodo. Es de gran importancia tener en cuenta los habilitadores y bloqueadores en las personas entrevistadas identificando, como ya se dijo, los motivadores que puedan apalancar los habilitadores y ayudar a sobreponerse a los bloqueadores. Pese a que pueda ser frustrante sobre todo al principio, la resistencia al cambio en algunas personas puede reducirse y hasta producir buenos resultados, especialmente si un diálogo sincero y el conocimiento de sus inquietudes se transforma en vehículo de una retroalimentación constructiva.

CONCLUSIONES

La problemática del Factor Gente constituye un tema muy poco conocido, investigado o considerado por parte de los expertos en Seguridad Informática, o sea técnica, lo que amerita su inclusión en Postgrados en Seguridad de la Información, enfocados especialmente en los *riesgos organizacionales y operacionales*, además de los conocidos *riesgos TIC*.

La experiencia ganada con el tiempo enriqueció las premisas iniciales de cómo resolver la incertidumbre original de escenarios de este tipo y similares que provocan cambios.

Una prueba piloto resultó al incluir hace casi tres años el tema del Factor Gente en un Trabajo Práctico del curso de Gestión y Auditoría de Riesgos y Seguridad de la Información, sorprendiéndonos el interés y dedicación observados en los asistentes a diferentes presentaciones de dicho curso.

Todo esto se amplió considerablemente al incorporar el tema en los trabajos específicos de proyectos de seguridad. Uno de los puntos más trascendentes fue tomar la decisión de incorporar un profesional de Psicología Social que acompañe al Foro de Gestión y a las reuniones individuales y grupales a modo de facilitador o agente dinamizador de las tareas a realizar y que, además, con su intervención movilice las objeciones y obstáculos que se presenten para producir soluciones adecuadas, propendiendo a que se establezca un entramado de relaciones vinculares manteniendo la bidireccionalidad de los vínculos.

Creemos que el material presentado puede constituir una guía introductoria para mejorar el manejo de los distintos aspectos de la conducta humana. Y útil también para reconocer las características de las personas con que se trabaja y, por extensión, que puedan transferir al personal a su cargo, conductas adecuadas a la seguridad de la información.

RECONOCIMIENTO

A Norma Robledo, Licenciada en Psicología Social, por los comentarios, observaciones y material que nos facilitara, así como por disparar el interés especial en los temas que coadyuvaron a nuestros objetivos principales.

REFERENCIAS

[1] Ormella Meyer, C.A., “Seguridad Informática vs. Seguridad de la Información”, *Página Web de la CEyTIC, Comisión de Electrónica y Tecnología de la Información y Comunicaciones del Centro Argentino de Ingenieros*: http://www.cai.org.ar y pestañas Dto.Técnico/Comisiones Técnicas/Electrónica y TIC/Publicaciones.
[2] Kabay, M.E., “Using Social Psychology to Implement Security Policies”, *Página Web*: http://www.mekabay.com/infosecmgmt/soc_psych_INFOSEC.htm
[3] Lucey David, "Managing the Human Factor in Information Security", John Wiley & Sons, 2009.
[4] Gupta Manish, Sharman Raj, "Social and Human Elements of Information Security, Emerging Trends and Countermeasures", Barnes and Noble, 2008.
[5] Ormella Meyer, C.A., “Estrategias Corporativas y Seguridad de la Información”, *Página Web de la CEyTIC, citada en* [1].