TITULO: Resumen biográfico de Vincent Van Gogh.

SUBTITULO: En seguridad informática hay que hacer y saber vender.

Autor: Alejandro C. Corletti Estrada. (acorletti@hotmail.com).

Madrid, junio de 2004.

DESARROLLO

Vincent Willem van Gogh nace en Groot Zunder (Holanda) el 30 de marzo de 1853 en el seno de una familia de clase media. Destaca en el aprendizaje de inglés, alemán y francés, pero a los 15 años abandona sus estudios. En sus primeros años de adulto se vuelca obsesivamente a la religión, llegando a predicar en varias ocasiones, luego la deja de lado. Su vida transcurre entre Etten, La Haya, Londres, Paris, Masnes, Nuenen, Arles, Auves y otros pueblos.

Es mantenido durante casi toda su vida por su querido hermano Theo.

Hasta los 30 no tendrá vocación artística, si bien antes hizo varios dibujos, es en 1883 cuando pinta su primer cuadro titulado "Muchacha bajo los árboles", al que siguen varios más inspirados en su compañera sentimental y en motivos campestres, desencadenando luego en las grandes obras maestras hoy reconocidas mundialmente.

Theo continúa su apoyo económico como anticipo de las ventas de unos cuadros que nunca se venderán. Vincent dirá a este respecto:

"Yo no tengo la culpa de que mis cuadros no se vendan. Pero llegará el día en que la gente se dará cuenta de que tiene más valor de lo que cuestan las pinturas".

Toma contacto con los mayores artistas de la época y va migrando sus obras hasta el estilo que lo define claramente, el neo-impresionismo marcando su propio estilo único.

Su personalidad es claramente inestable, pasando por el alcohol, los hospitales psiquiátricos, los desengaños, los cambios de creencias, ataques donde se tragaba sus pinturas, y hasta el suicidio.

En 1890 compran el primer cuadro suyo "El viñedo rojo", en julio de ese mismo año viaja a París a ver a su hermano, el cual está pasando por una situación difícil, y creyendo que él era parte de esos problemas, sale al campo y se dispara con un revólver, causa que dos días después lo lleva a la muerte un 29 de julio de 1890.

A lo largo de su corta vida, Van Gogh, realiza cerca de 750 pinturas y alrededor de 1600 dibujos, pasando por diferentes etapas de creación.

RESUMEN:
Van Gogh, Vincent
Nacionalidad: Holanda

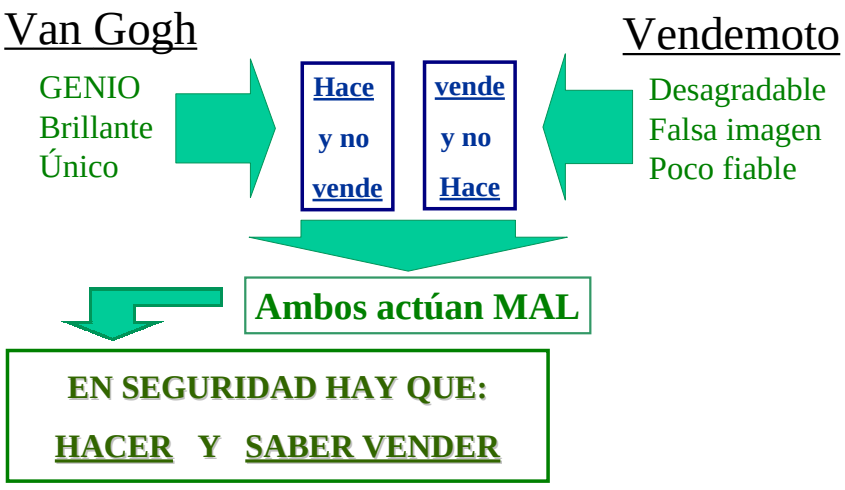
Nació en Groot Zunder en 1853
Estilo: Neo-Impresionismo (Padre del mismo).
Clasificación Opinión pública: GENIO DEL ARTE.
Primer genio de la pintura contemporánea
Más de 800 cuadros en ocho años
Vendió en vida uno solo.
Murió en muy mala situación económica (1890)

Timoteo Vendemoto: Imaginemos este tipo de personajes (de hecho más comunes de lo deseado).

Nació en esta última generación, acostumbrado a tener más de lo que se debe, a obtener las cosas sin mayor esfuerzo, no muy afecto al trabajo, pero con una innata condición de vendedor. Como descubre este perfil rápidamente, abandona los estudios temprano y se dedica al comercio, abriéndose camino velozmente, pues, la verdad es que sabe hacerlo. Vende y sigue vendiendo, aunque los avances tecnológicos lo superan ampliamente, pues no tiene ningún tipo de formación; pero como sabe convencer, él vende. Es más, a esta altura del siglo, son tantas las tecnologías que desconoce, que reconoce entre amigos, que ya no tiene la menor idea de lo que está vendiendo, pero, él vende y vende.....y vende.

Nació en Avivón (1970).
Estilo: Impresionismo rápido.
Opinión pública temprana: GENIO COMERCIAL.
Opinión pública añeja: GRAN CAPACIDAD DE VENDER.
Opinión de los que lo conocen: Vendemoto.
Formación: Escasa.
Antecedentes: Supo vender hasta lo invendible, o lo que no tiene.
Conocimientos de lo que vende: Absolutamente nulo.
Vive y..... seguirá viviendo (sobre todo de los demás y los que no lo conocen a fondo).

REFLEXION INICIAL



> Dejando ahora esta informal presentación, en mi experiencia de trabajo en seguridad creo seriamente que el problema más importante que pasa estos momentos toda Gerencia de Seguridad, es que no sabe VENDER.
>
> (y al decir TODA, creo no equivocarme en una tolerancia de -10%)

Volviendo a los ejemplos, no me agrada para nada la figura del segundo personaje, pero posee una gran virtud, la cual si se conjuga con el "saber", da resultados excelentes y ciertos, pues ahora no se está mintiendo, sino que se está dando a conocer de buena fe, algo que se sabe y se es consciente que está bien hecho. Por favor no me mal interpreten, pues repito, no digo vender mal ni tratar de vender cosas que no están bien hechas, **pero sí digo**, que si hacemos las cosas bien y no las vendemos, nos morimos ignorados por el resto del mundo, a pesar de ser tan genios como Van Gogh, cosa que reconozcamos, es un crimen histórico.

El tema no es fácil para nada, pues ¿Qué se puede vender de seguridad?, existen pocas armas para este desafío, pero se debe tratar de encontrarlas sino, es muy poco probable que se puede justificar una inversión adecuada año tras año.

La empresa Ernest & Young realiza año a año una encuesta de seguridad a gerencias de más de 1500 firmas en el mundo. Lo que más me llamó la atención dentro de todos los aspectos que destaca de la realizada en 2003 es que: " *El ROI (Retorno de la inversión), no está valorado como medida de efectividad de los gastos de seguridad"*. Esta expresión es clarísima, no puede ser de otra manera, pues ningún director ve, que lo que gasta, le está siendo reintegrado de alguna forma. Este creo que fue el aspecto que más me llevó a pensar que es una obligación de la Gerencia de Seguridad "El saber vender", tan obligación como cualquier otra medida técnica que se adopte, pues sino año a año tendrá menos recursos para los detalles técnicos hasta que, por falta de apoyo, no pueda "hacer" bien las cosas, pues no vendió. En definitiva, sino mostró resultados, imaginando las mil formas de justificar este ROI, morirá como Van Gogh.

El caso más concreto son los matafuegos de una empresa , año a año se gasta mucho dinero en ellos, pero ahí están, sin hacer nada. Aunque a veces se escuchan casos de incendios muy "sospechosos", no suele ser una buena medida, generarlos para justificar su uso. Estoy casi seguro, que si no existieran las leyes que lo hacen obligatorio, desaparecerían poco a poco de la gran mayoría de sus sitios, o por lo menos la inversión de mantenimiento se reduciría substancialmente. Bueno, este es un buen punto de partida, pues recordemos que ya existen leyes que nos apoyan (LSSI, LOPD, etc). PRIMER PASO: sacar provecho de lo que nos ofrece la ley y mostrar resultados.

Se debe plantear dentro de la política de seguridad, muy detalladamente todo lo relacionado a esta legislación, declarar los ficheros correspondientes, y REALIZAR AUDITORÍAS, tanto internas (y si es por personal ajeno a la gerencia mejor: abogados, contadores, administrativos) como externas, que permitan evaluar realmente (sin vender motos), el nivel alcanzado en estos aspectos, pudiendo generar informes y acciones de mejora. Estos dos últimos documentos (Informes y acciones de mejora), permiten:

- Planificar acciones y etapas (hitos).
- Presentar resultados periódicos y de avance.

- Justificar el empleo de los recursos.

Otra analogía que siempre encuentro en este tema, está nuevamente relacionada (como en otros artículos), con aspectos militares.

En casi toda unidad militar de combate, existe un "polvorín", en este se almacena toda la munición que el elemento necesitaría en caso de conflicto. Como podemos imaginar, en la inmensa mayoría de los casos, este no se emplea (gracias a Dios), pero está ahí, y desde luego ninguno de sus jefes o comandantes, duda que debe estar ahí y cuanto más tenga mejor. Resulta evidente pensar que toda esa cadena jerárquica está preparándose para el supuesto de un conflicto, y por lo tanto conoce del tema. Bueno este es otro aspecto a considerar: Nuestros directivos, también saben de conflictos, desafíos, competencia entre empresas (casi guerras crueles) y análisis de riesgo → SEGUNDO PASO: Preparar pautas muy claras de estos riesgos, es decir análisis de riesgos concretos, valorar la información que se tiene, preparar "casos" sobre el impacto que causa en una organización los virus, troyanos, intrusos, negación de servicio, etc. Preparar exposiciones, invitar disertantes, redactar resúmenes gerenciales de hechos de seguridad ocurridos mensualmente. En concreto, mantener viva la consciencia de seguridad a nivel Directorio

Pero el tema del polvorín no queda aquí. El encargado de todo polvorín, debe ser una persona que conozca en detalle los recursos que tiene, pues la munición tiene un tiempo de vida, superado el cual, no puede ser utilizada y debe ser descartada (o retornada a la fábrica para reciclarla o aprovechar lo que quede útil). Mes a mes el stock envejece, y si no se lleva un control estricto y se está todos los días re acomodando y actualizando su información, se desperdicia. Es aquí donde se puede valorar un encargado bueno de uno malo, pues el bueno, es el que está permanentemente sabiendo del tema, y unos meses antes que la munición venza, la pasa al rubro "instrucción" y la misma se emplea para realizar ejercicios y prácticas, con lo cual, todos los usuarios de la organización están contentos, pues ven los resultados de ese trabajo y pueden aprender y perfeccionarse. Por supuesto el mal administrador, por error o por desconocimiento del tema, deja pasar estas fechas, debiendo desperdiciar literalmente la munición, con el daño directo que esto trae aparejado y también con el resquemor que genera el ver que se desperdicia un bien tan valioso para el resto. Pero ojo, que esto último sucede más a menudo de lo que se pueden imaginar.

¿No encuentran una enorme semejanza con el "polvorín" que tenemos en seguridad? Si hacemos bien el trabajo, nos actualizamos y llevamos el control de la seguridad de la empresa, nuestros usuarios lo notan. Ellos saben que les filtramos bien los spam, que no existen virus en la empresa, que los backup de sus datos están siempre, independientemente que ellos cometan errores, que el sistema no se cae, que en otros lados pasan cosas que aquí no, que cuando tienen dudas encuentran respuestas, etc. No olvidemos que todo director, es un usuario más, por lo tanto, si hacemos bien el trabajo, este también lo verá y notará que si bien tiene un recurso almacenado, su "munición" no se desperdicia. Aquí no entra en juego el vende moto, sino el Van Gogh que hace las cosas bien, pero que expone sus cuadros. Bueno, aquí tenemos nuestro TERCER PASO: Mostrar resultados concretos a los usuarios y esmerarnos en que se noten, con artículos, mails, novedades, recordatorios, etc.

METODOLOGÍA DE VENTA:

Para ir cerrando estas ideas, quiero presentar la visión que propongo acerca del trabajo de seguridad:

PROPUESTA

El primer paso es definir la estrategia que se desea para la seguridad de la Organización. Esta estrategia, como su nombre lo indica se realiza al más alto nivel de la organización y en la práctica tiene dos aspectos fundamentales:

- **Que la alta dirección quede comprometida con el problema** (pues desde aquí nace todo lo que se pueda o no realizar a futuro).
- **Crear consciencia de la importancia de la seguridad a este nivel.**

Recién a partir de aquí y bajo ningún punto de vista salteando esta etapa (problema muy común), es cuando puede comenzar a elaborarse el Plan de seguridad, el cual deberá realimentar muchas de las decisiones tomadas en la Política, generando con esto un Feedback permanente, característico de todo proceso dinámico.

Luego vienen, tanto el plan de seguridad como la documentación. Estos dos aspectos trato de separarlos bien, pues prefiero que desde el inicio se interprete el plan de seguridad (Cómo) de la organización como algo muy **"vivo",** y diferenciarlo nítidamente de todo un conjunto de documentación adicional, que la relaciono mas con "**procedimientos**" pues son elementos más estáticos y duraderos, que permiten estandarizar pasos a seguir metódicamente. No quiero entrar en detalles técnicos de los mismos pues no es el carácter de este artículo.

Los dos temas trascendentales (y que a menudo no se plantean así) son las **acciones** y **revisiones**. Estos pasos son los que nos dan origen a la planificación anual de seguridad, por medio de la cual se realiza lo siguiente:

- Análisis de la situación actual y estado inicial del sistema.
- Planificación anual con objetivos y umbrales a alcanzar.
- Preparación de informes periódicos y aperiódicos.
- Plan de revisiones y auditorías.
- Evaluación de resultados.

Para esta actividad se deben conjugar dos elementos:

- Organizativo.
- Técnico.

El organizativo es lo que prácticamente relaciono con un "mini elemento de marketing" que se debe tener en la gerencia de seguridad, y es el responsable de generar todo la información presentable, de manera que refleje exactamente la evolución de nuestro trabajo (sin engaños).

El técnico es el responsable de "cuantificar", es decir de generar los valores o parámetros que permitan demostrar objetivamente (y no subjetivamente) lo que está sucediendo, y nos deje evaluar la evolución de lo que se analizó y planificó, los umbrales alcanzados, realizar estadísticas, el grado de cumplimiento y/o las acciones correctivas a realizar, y en definitiva sea quien nutre de información en forma numérica a toda la gerencia. Sin contar con estos "números" una Gerencia de seguridad muere como Van Gogh. Por supuesto que si se trabaja bien, estos "números" son el resultado de la eficiencia con que se está trabajando, pues serán la imagen de los ataques que pasan y los que no, la prioridad de los mismos, el grado de bastionado de los sistemas, las actualizaciones realizadas, las medidas concretas adoptadas (Reglas en FWs, listas de control de accesos, criptografía, resguardos, preparación pre y post incidentes, etc.), en definitiva las acciones reales con que se trabajará a diario. Sobre este punto, me hago un poco de propaganda y aconsejo al lector que esté interesado, a leer más en detalle sobre este tema en otro artículo ***denominado "Matriz de Estado de Seguridad"*** que publiqué hace poco en Internet y que trata un poco de cómo poder realizar esta actividad.

A través de estos cuatro módulos recientemente planteados, es que se genera esta realimentación hacia el órgano estratégico de la organización (la Dirección), y por medio de estos informes, valores o estadísticas, podemos de manera eficiente, demostrar que se está invirtiendo bien en seguridad, que se cumplen los plazos y objetivos propuestos, que se mejora con las acciones tomadas, que se mantiene actualizado el sistema y en definitiva lograr justificar este retorno de la inversión (ROI), que evidentemente aún nuestros directivos no lo ven. Y aquí aparece entonces nuestro CUARTO PASO: Ser capaces de Cuantificar acciones y revisiones para realimentar la Estrategia, pues sin esta realimentación, la dirección esta ciega y sin lugar a dudas verá año a año que no existe ROI en seguridad, y sí en otras gerencias hacia las cuales destinará nuestros fondos.....y nos llegará un 29 de julio, como a Van Gogh.

REITERACIÓN FINAL (Cuatro pasos):

PRIMER PASO: sacar provecho de lo que nos ofrece la ley y mostrar resultados.

SEGUNDO PASO: Preparar pautas muy claras de estos riesgos, es decir, análisis de riesgos concretos, valorar la información que se tiene, preparar "casos" sobre el impacto que causa en una organización los virus, troyanos, intrusos, negación de servicio, etc. Preparar exposiciones, invitar disertantes, redactar resúmenes gerenciales de hechos de seguridad ocurridos mensualmente. En concreto, mantener viva la consciencia de seguridad a nivel Directorio

TERCER PASO: Mostrar resultados concretos a los usuarios y esmerarnos en que se noten, con artículos, mails, novedades, recordatorios, etc.

CUARTO PASO: Ser capaces de Cuantificar acciones y revisiones para realimentar la Estrategia

PD: Casi cerrando este artículo tuvimos una charla con José Ramón Merino (Responsable de seguridad de Metro) y dijo una frase que me quedó dando vueltas, la repito textualmente: *"Por qué no buscar un nombre al tema de seguridad que no sea tan drástico, como es el caso de un **plan de continuidad de negocio** que está tan de moda y en definitiva es un plan de contingencia, concepto que tienta mucho menos a la inversión de recursos"*. Es decir, sería bueno encontrar un nombre "más de moda" para representar a la seguridad informática, que no se relacione inmediatamente con "desembolsar dinero a fondo perdido". Me pareció una reflexión excelente, seguro a que alguien con una fuerte formación en marketing o publicidad se le ocurre algo..... les dejo la inquietud.

ALEJANDRO CORLETTI