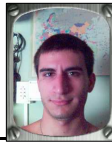


Artículo Realizado Por:

Argentero Cristián D.
[(CR@M3R)]



*Estudiante de las
"Ciencias Informáticas"*

Contacto (MSN): cdaznet@hotmail.com



ISO 17799

"LA SEGURIDAD DE LA INFORMACIÓN NO ES UN PRODUCTO SINO UN PROCESO"

Quien tiene la *capacidad* de contar con *información idónea*... ¡Posee el control!

¿Cuántas veces hemos "sentido" esta frase en la actualidad?

Y... Hablo de "sentido", por el simple hecho de que quién no la escuchó pronunciar por ahí, la padeció en "carne propia" (o, más categóricamente dicho: *por sus propios medios*).

Ahora bien... Vale aclarar, también, que la *víctima de un ataque* (cualquiera sea) tiene la posibilidad de brindar *una defensa*, la cual debe ser más poderosa, potente y eficaz que la de su enemigo, para así...

¡Triunfar!

Pero... ¿Qué tal si nos libramos de todas esas consecuencias traídas por las luchas y evitamos los costosos gastos de "La Guerra Digital" con *una solución* predilecta y/o adecuada?

Pues, entonces, a continuación quedará revelado el "misterioso enigma" de *quién* se hace llamar *solución* y que puede estar al alcance de todos... De todos aquellos vinculados como responsables de realizar la gestión de la Seguridad de la Información, dispuestos a iniciar, implantar, mantener o resguardar la integridad de (valga la redundancia) *La Seguridad de una Organización*.

Su nombre es: **ISO 17799**.

"¿La información y los datos valiosos de la empresa están protegidos adecuadamente? ¿Están garantizados los negocios que se desarrollan y su continuidad? ¿Se garantiza el retorno de la inversión empresarial? ¿Qué debe hacerse para garantizar un nivel adecuado de seguridad de la información? ¿Qué soluciones y tecnologías deben implementarse?"

Esas son algunas de las preguntas con las que (frecuentemente) nos topamos en vuestro ámbito de trabajo.

En una fórmula (*como hecha a medida*) responderemos a tales interrogantes como Profesionales del Terreno.

Introducción ("Entrando en Clima")

La información es un valioso patrimonio empresarial que existe y se presenta en diversas formas.

Puede estar impresa, escrita en papel, almacenada electrónicamente o (lo que es mucho peor) abandonada en ciertas oficinas destinadas, supuestamente, a la "reserva" de la misma. Además, la información se muestra en filmes, grabaciones o directamente mediante el lenguaje oral (conversacional). Y se transmite por diferentes medios (sean éstos, convencionales -analógicos- o de última generación -digitales-). Independientemente del carácter que adopte, se recopile o se comparta, la información y los dispositivos y equipamiento asociados, deben ser protegidos adecuada y eficazmente, garantizándose la disponibilidad, integridad y confidencialidad de la misma, con normas estandarizadas y adoptadas correctamente para la gestión de la seguridad de la información empresarial o doméstica.

Surge así, el requerimiento (necesidad + expectativa) de crear un estándar internacional de alto nivel para la administración de la seguridad de la información, el cual fue publicado por la ISO (International Organization for Standardization – *Organización Internacional para la Estandarización*) en diciembre de 2000 (y, contemporáneamente actualizada) con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones.

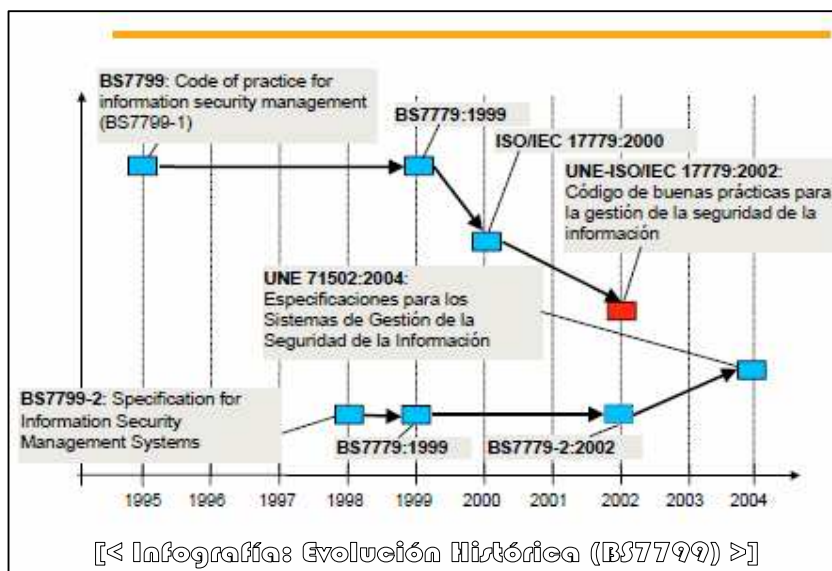
He aquí, la tan querida: ISO 17799.

La ISO 17799¹, al definirse como una guía protocolar (conjunto de normas a llevar a cabo) en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios:

- ⊙ **Confidencialidad:** asegurar que, únicamente, personal autorizado tenga acceso a la información.
- ⊙ **Integridad:** garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas; preservando exactitud y completitud de la misma y de los métodos de su procesamiento.
- ⊙ **Disponibilidad:** cerciorar que los usuarios autorizados tendrán acceso a la información cuando la requieran y sus medios asociados.

Tales premisas en la protección de los activos de información constituyen las pautas básicas (deseables) en cualquier organización, sean instituciones de gobierno, educativas, de investigación o (meramente) pertenencias hogareñas; no obstante, dependiendo de la naturaleza y metas de las estructuras organizacionales, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

Como ha de saber, es “misión imposible” conseguir el 100% de Seguridad en cualquier aspecto de La Vida. Por lo tanto, el objetivo de la seguridad en los datos es (acéptese el *juego de palabras*) para asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una eventualidad, así como optimizar la inversión en tecnologías afines y prosperar en las novedosas oportunidades que nos brindará el porvenir del tiempo.



Como todo buen estándar, el ISO 17799 da la pauta en la definición sobre cuáles metodologías, políticas o criterios técnicos pueden ser aplicados en el régimen de manejo de la seguridad de la información. La toma de decisiones sobre un marco de referencia de seguridad basado en ella proporciona beneficios a toda organización que lo implemente. Ya sea en su totalidad o en la parcialidad de sus postulaciones estipuladas.

Su elaboración y práctica integra mecanismos de control primordiales, que le permiten a las organizaciones demostrar que cuenta con el estado de la seguridad de la información pertinente; situación que resulta muy importante en aquellos convenios o contratos con terceros que establecen como requisito contractual la *Declaración BS7799*² u otras disposiciones de perfil similar que se acentúan mucho en “los tiempos que corren”.

¹ Su nombre, concretamente, técnico y/u oficial es: ISO/IEC 17799. Vulgarmente, reconocida como: ISO 17799. Vale precisar que, ISO no es un acrónimo; proviene del griego “iso”, que significa “igual”. Es un error común el pensar que ISO significa “International Standards Organization”, o algo similar. Por ejemplo: en inglés su nombre es International Organization for Standardization, mientras que en francés se denomina Organisation Internationale de Normalisation; el uso del acrónimo conduciría a nombres distintos: IOS en inglés y OIN en francés, por lo que los fundadores de la organización eligieron ISO como la forma corta y universal de su nombre. Más Información: www.wikipedia.org.

² Código de prácticas especificados en el Sistema de Administración de la Seguridad de la Información dispuesto por el BSI (British Standard Institute – Instituto de Estándares Británicos) que forman los cimientos sobre los cuales se considera la confección de la ISO 17799 (provista de un carácter internacional y apto). Consistente en lo descrito según el famoso “Círculo de Deming”: PDCA (Plan, Do, Check, Act - Planificar, Hacer, Verificar, Actuar). Más Información: www.bsiamericas.com.

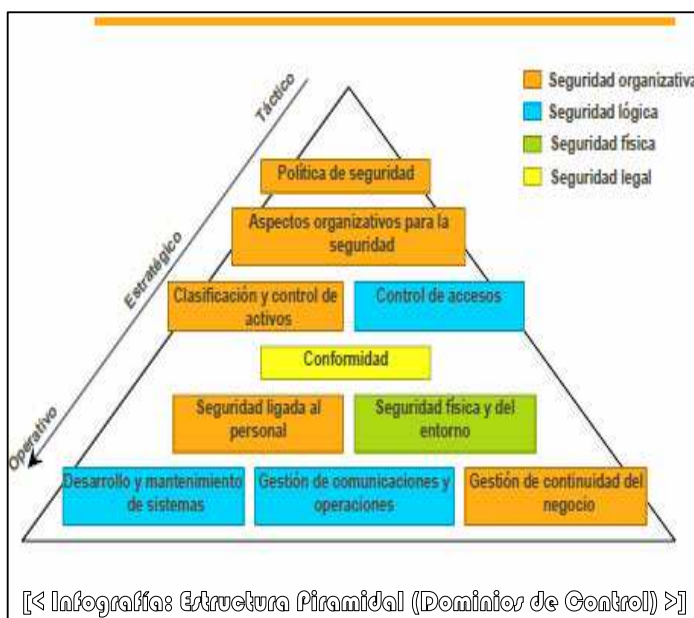
Desarrollo (“Poniéndonos a Punto”)

¿Podré seguir trabajando si se produce un siniestro en la oficina de la empresa en la cual trabajo (sin poseer Backup alguno de la información)? ¿Qué ocurriría si la competencia cuenta con el acceso a mis balances? ¿Cómo sé si habrá algún tercero externo interceptando el flujo de datos en mi red corporativa? ¿Podrán robar el código fuente, las agendas, las claves o nuestros futuros proyectos programados? ¿Alguien podrá entrar al centro de cómputos sin restricciones o control, copiar información o agregar un usuario de altos privilegios? ¿Y si cambian las reglas en el Software de manejo cotidiano sin previo aviso? ¿Podremos seguir trabajando si se origina alguna catástrofe natural (de magnitudes típicas)?

Este tipo de cuestionamientos en común cuando uno se encuentra vulnerable a tales amenazas, accidentes, descuidos y muchos otros puntos que podrían ser prevenidos (anticipándose con medidas convenidas o previamente pactadas según *Una Normalización* de modelos a efectuar).

La Norma *ISO/IEC 17799* establece diez dominios de control que cubren (casi) por completo la Gestión de la Seguridad de la Información:

- 1) *Políticas de seguridad*: el estándar define como obligatorias las políticas de seguridades documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.
- 2) *Aspectos organizativos*: establece el marco formal de seguridad que debe integrar una organización.
- 3) *Clasificación y control de activos*: el análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.
- 4) *Seguridad ligada al personal*: contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información. Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, o sea, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.



- 5) *Seguridad física y del entorno*: identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.
- 6) *Gestión de comunicaciones y operaciones*: integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.
- 7) *Control de accesos*: habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.
- 8) *Desarrollo y mantenimiento de sistemas*: la organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.
- 9) *Gestión de continuidad del negocio*: el sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.
- 10) *Cumplimiento o conformidad de la legislación*: la organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

De estos diez dominios nombrados se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de inspecciones) y 127 o más controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo). Ambos, se encuentran destinados a dotar y esparcir Seguridad a la Información en el “ambiente digital”, a través de numerosas auditorías, consultorías y/o paradigmas.

Cada una de las áreas constituye una serie de observaciones que serán seleccionadas dependiendo de las derivaciones obtenidas en los análisis de riesgos, conjuntamente, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle. Por eso, es aplicable a toda organización, independientemente, de su tamaño o sector de negocio; siendo un argumento fuerte y dinámico para los detractores de la norma y un “conjunto de instrumentos” flexibles a cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la IT³.

Pero... “*Siempre hay un Pero*” (así dice el lema), y es el consiguiente: como la ISO 17799 se forma de un compilado protocolar de normas y/o reglas fundadas en las Políticas de Seguridad, y éstas son erigidas y colocadas por el *Ser Humano*, no son inmunes a fallas o errores (infalibilidad absoluta) y con el tiempo deben ir siendo depuradas para acercarse lo más que se pueda (*y un poco más*) a un “monstruo desconocido”, aunque muy escuchado, que es llamado: *Perfección*.

Tal sentencia puede ser corroborada en el mismo *alegato* sobre el cual se excusan potenciales (factibles y/o aleatorios) inconvenientes de su *puesta en práctica*:

“No todos los alineamientos y controles de este código de práctica resultarán aplicables. Más aún, es probable que deban agregarse controles que no están incluidos en este documento. Ante esta situación puede resultar útil retener referencias cruzadas que faciliten la realización de pruebas de cumplimiento por parte de auditores y socios”.

Aquí, parecería decir (*según mi razonamiento de deducción implícitamente lógico*):

“Nos es grato anunciar que por más remedio que intentemos buscarle a ésta enfermedad (*INseguridad de la Información*), no podremos encontrarle una cura absoluta y/o total. Eso, dependerá (estrictamente) de sus criterios de decisión seleccionados y llevados a cabo. En tales casos, si quieren agregar o sacar algo... ¡Bienvenido sea para Ustedes!”.

Ésto da por sentado su propiedad de mutabilidad, actualización y adaptabilidad según las determinaciones organizacionales de las que dispongamos, sin embargo, presiento (y se que me acompañarán en tales laudos) que algo en ella podría innovarse y ser mejor.

Para ello tendría en cuenta las siguientes peticiones:

- ❖ *Interacción y transposición de procedimientos (métodos, normas, y/o reglas)*: que la disposición física del centro de cómputos, terminales o servidores no se contraponga con la norma IRAM que regula el recorrido físico dentro de las oficinas. Es indispensable la interacción con un profesional en Organización y Métodos, Analista o Ing. en Sistemas con vasta experiencia. Prestar mucha atención al implementar controles (para no estar debilitados o desordenados por “cosas” de otros lados).
- ❖ *Tendencias a las nuevas tecnologías*: tener presente en el flujo de datos la permeabilidad o apropiación de los mismos a través de la tecnología VoIP (Voice over IP – *Voz sobre IP*), unidades de almacenamiento secundarias transportables (Pendrives, Cámaras, Celulares, Etc.) y mensajeros instantáneos (usados para el Chat).
- ❖ *Reclutamiento de personal (empleados)*: es una de las claves del éxito de una organización, el atraer e incorporar a gente apropiada para desempeñarse en la implementación de estas normas. El agente de RRHH tiene que tener vastos conocimientos técnicos, comprobar las habilidades y referencias que estén en el CV del potencial postulante.
- ❖ *Adaptación inteligente al medio*: contar con el Software (recursos lógicos) y el Hardware (recursos físicos) convenientes para no perder la calidad de los servicios y/o bienes ofrecidos como producto.
- ❖ *Invertir en capacitación conveniente y acertada en los trabajadores*: tratar de entusiasmar e incentivar al usuario para que se faculte de mayores y mejores mañas (artilugios) al momento de operar en su cargo. De esta manera, se suprimirá (en enormes cantidades) la negligencia y las falencias a causa de ésta, teniendo secuelas de menor magnitud a la hora de resolver un problema.
- ❖ *Vigilancia en otros cuidados diversos a tener vigentes*: monitorizaciones, seguimientos e investigación de los campos a los cuales subyace la materia u oficio contratado.

³ Sigla proveniente del inglés que significa: *Information Technology* (Tecnología de la Información – TI).

Y... Para darnos el gusto con la *"frutilla del postre o la cereza del helado (o ambas)"*, ha de estar al tanto que *La Norma ISO/IEC 17799 no posee ningún tipo de certificación*. Ya que sólo son recomendaciones y no es necesario aplicar la totalidad de sus controles, sino adaptarlos a la organización para no hacer algo tedioso e inútil, como así tampoco... ¡PARANOICO!

Conclusión ("Al Fin Llegamos a la Meta: ¿Lo Logramos!?")

La *correcta clasificación* de los controles es una tarea que requiere del apoyo de especialistas en seguridad de la información o de alguien capacitado de manera similar, con conocimientos adquiridos en circunstancias de diversas índoles (*experiencia*) en la implementación de la (ya tan afamada y renombrada) *ISO 17799*; ya que cuando éstos se establecen de forma inadecuada o incorrecta pueden generar un marco de trabajo demasiado estricto y poco cómodo para las operaciones (eventos desempeñados) de la organización y de los que habitan en ella.

Empero, sólo queda que Usted pretenda intentar tomar la iniciativa y asumirla con coraje, firmeza, perseverancia, solvencia, compromiso, dedicación y... Por sobre todo: SEGURIDAD EN SÍ MISMO Y EN LO QUE LO RODEA, para emprenderse en un camino que, tanto su Organización como quienes la integran, le estarán agradecidos y le harán sentir (con un juicio de cierta razón) que *La Seguridad de la Información* es un árbol de raíces amargas pero... De dulces y ricos frutos a recolectar; parte de *Un Juego* al que apostó para... ¡Ganarlo!

Y... Recuerde Siempre para Nunca Jamás Olvidar:

"LA SEGURIDAD DE LA INFORMACIÓN NO ES UN PRODUCTO SINO UN PROCESO".-

EOF
(End Of File)

... SERÁ HASTA UN PRÓXIMO ENCUENTRO ...
(ENTRE VOS, LA AUTÉNTICA INFORMACIÓN Y YO)

{ MIS CORDIALES SALUDOS }

ATRIBUCIÓN-NoCOMERCIAL-COMPARTIRDERIVADASIGUAL 2.5
[HTTP://CREATIVECOMMONS.ORG/LICENSES/BY-NC-SA/2.5/DEED.ES_AR/](http://creativecommons.org/licenses/by-nc-sa/2.5/deed.es_AR/)

MARTES, 12 DE SEPTIEMBRE DE 2006