La seguridad de los activos de información (1)

OSCAR ANDRÉS SCHMITZ
Chief Information Officer
de ING Bank
Oscar_schmitz@yahoo.com.ar

Todas las actividades de las organizaciones existen por la información utilizada. Las buenas prácticas aplicadas a su protección, gestión y utilización determinan el éxito del producto desarrollado.

Comienza el día. Despertamos escuchando la radio con los datos del tiempo, la situación de los transportes públicos y un resumen de las principales noticias. Información. Durante el viaje al trabajo, leemos el reporte del proyecto, comparamos el cuadro de situación, con las fechas y los desarrollos finalizados. Información. Accedemos a las oficinas, nuestra tarjeta de acceso no funciona correctamente, no reconoce el código de barras, volvemos a intentar y entramos. Información. Nos dirigimos a nuestro escritorio, ingresamos usuario y contraseña, accedemos a nuestra computadora. Información. Abrimos nuestros programas de desarrollo, la última versión de los códigos fuentes, los documentos de análisis y diseño, los informes de requerimientos, accedemos a la base de datos en cuestión y nos disponemos a trabajar. Información. Teléfono…, el nuevo integrante del equipo nos solicita soporte sobre el componente de encriptación que estaba publicado en la librería de nuestra la base de conocimiento de desarrollo. Información. El asesor externo en protocolos de comunicación nos visita a fin de acordar un mejor esquema que brinde mayor eficiencia al programa que estamos desarrollando. Información. En las últimas horas, coordinamos con el resto del equipo la integración de los diferentes desarrollos para armar la versión final, a fin de instalarla en el ambiente de prueba, para ser probada con los casos de prueba elaborados por los usuarios calificados. Información. El resultado de estas pruebas determinará que entreguemos a nuestros clientes el producto final en forma anticipada a la de nuestros competidores. Entendemos que nuestros competidores se encuentran retrasados en su desarrollo debido al incidente eléctrico que afecto a toda la zona. Nosotros pudimos sobrellevar esta eventualidad debido a nuestro sitio alternativo de contingencia en las afueras de la ciudad. Información. Información. Y más información.

¿Qué es un activo de información?

Si nos tomamos unos minutos para analizar la situación anterior comprendemos que en cada una de las actividades que desarrollamos diariamente estamos en contacto con información que nos permite mejorar el conocimiento y aprender, reducir nuestra incertidumbre permitiéndonos decidir la mejor acción entre varias, o proporcionar una serie de reglas con fines de control o evaluación.
La información se convierte en un activo, tan importante como los activos económicos y humanos que posee la organización, y por consiguiente deben ser protegidos de un modo adecuado. Ninguna persona estaría de acuerdo en perder dinero, debido a un agujero en el bolsillo. Ningún líder de proyecto estaría conforme en perder uno de los talentos de su equipo, particularmente en medio de un proyecto. Ningún programador estaría motivado en comenzar su día laboral al enterarse que la última versión del código fuente finalizado ayer, se ha perdido debido a que el

servidor que lo almacenaba quedó fuera de funcionamiento y la última copia de seguridad disponible es de un mes atrás.

Los tres pilares del valor de la información

¿Cuál es el valor de los activos de información para nuestra organización, para nuestro equipo de trabajo y para nosotros mismos? A fin de determinar el valor de estos activos, debemos conocer los tres pilares que clasifican la importancia y prioridad de los mismos:

- **Confidencialidad:** solo podrán acceder a la información (usarla, leerla o escucharla) las personas autorizadas.
- **Integridad:** la información con la que se trabaja sea completa y precisa, poniéndole énfasis en la exactitud tanto en su contenido como en los procesos involucrados en su procesamiento. Este pilar determina la manera en que es controlada la persona antes de acceder a la información.
- **Disponibilidad**: la información estará disponible siempre que cualquier persona autorizada necesite hacer uso de ella. Clasificando este pilar de acuerdo a la velocidad de recupero necesaria para que la información esté disponible.

¿Qué es la seguridad de la información?

La seguridad de la información protege a los activos de información respecto a una gran cantidad de amenazas, asegurando a la organización que la frecuencia y el impacto de los riesgos sean mínimos, considerando que la rentabilidad y la relación costo/beneficio sean los más eficientes. Las organizaciones dependen para funcionar de sus sistemas aplicativos, bases de datos, redes de comunicaciones, procesos internos y las personas. Muchos de estos aplicativos no fueron diseñados y desarrollados para que sean seguros, debido a que el esquema de seguridad aplicado a los mismos era obsoleto o desconocido. La planificación del desarrollo de un aplicativo nos permite reducir lo desconocido. En el marco de la seguridad debemos realizar la planificación paralela que considere los diferentes controles de la protección de los activos de información.
La seguridad de la información es un proceso que evoluciona con toda la organización, si bien esta coordinada y centralizada por el personal especializado (IRM – Information Risk Management), involucra el compromiso de todas las personas de la empresa, incluso en muchos casos es extensivo a los clientes y proveedores de la misma, es decir, es un proyecto multidisciplinario aplicado a la cadena de valor completa. Si bien existen medios tecnológicos o técnicos que permiten mejorar la seguridad, actualmente no son suficientes por si solos. Debemos complementarlos con un detallado análisis e identificación de los puntos de riesgo, una cuidadosa planificación de los controles a realizar, una gestión de seguridad que involucre a todos y una adecuada implementación de procedimientos de acuerdo a lo relevado.

¿Para qué utilizar un estándar o buena práctica internacional?

A esta altura del artículo nos debiéramos preguntar ¿Somos concientes del esquema de seguridad que estamos aplicando a nuestros activos de información? ¿Somos competentes al realizarlo? Estas preguntas tienen como objetivo cuestionarnos que posición tenemos frente a la seguridad de la información. ¿Seremos ciegos al respecto?, es decir que no sólo no sabemos, sino que ni siquiera sabemos que no sabemos. ¿Seremos ignorantes?, esto es que sabemos que no sabemos. En este caso

somos concientes que no sabemos y debemos aprender, pasando de ser incompetentes a competentes, permitiéndonos ser aprendices de los conceptos de la seguridad de la información. Puede ser que algunos no quieran ser aprendices, y tomen la posición de la persona cretina, quien sabe que no sabe, pero finge saber…, esta posición no se las recomiendo debido a que no nos permite crecer como profesionales que somos.
Es inevitable que para ser aprendices de estos conceptos, y tener el grado de competencia que requiere la organización debamos compararnos. Podemos compararnos con otros profesionales, otros equipos de trabajo u otras organizaciones, pero siempre existirá una duda sustancial si la otra parte está realizando en forma correcta y efectiva la aplicación de la seguridad. Por ello existen estándares o buenas prácticas internacionales que son utilizadas como recomendaciones dentro de un esquema referencial a seguir, que nos permiten clarificar nuestro estado de conciencia y nos provee el conocimiento para aprender a ser más competentes al respecto. Las buenas prácticas se relacionan simplemente con “la mejor manera de realizar las cosas”.
En los últimos años el uso de la TIC, ha determinado un valor diferencial en las organizaciones. El conjunto de aplicaciones, bases de datos, redes de comunicaciones y equipamiento utilizado, determinan un aspecto crítico en el éxito de las actividades comerciales. La TIC determina una ventaja competitiva que permite mejorar la productividad y la calidad de la información circulantes en la organización. Pero también su aplicación implica riesgos. Estos riesgos debieran ser conocidos y controlados dentro de un esquema que conviva con las actividades normales de la organización. Las buenas prácticas determinan el esquema conceptual sobre las cuales debemos desarrollar las actividades relacionadas con la TIC.
Los estándares o buenas prácticas internacionales, determinan el camino que debemos seguir para alcanzar un objetivo puntual. No nos aseguran el éxito. Las buenas prácticas pueden ser comparadas con un mapa u hoja de ruta. Este mapa nos presenta un esquema con base conceptual y teórica que nos sirve de guía en las actividades que desarrollamos para alcanzar el objetivo propuesto. El mapa no nos anticipa lo que realmente puede presentarse en el territorio a recorrer. El mapa no es el territorio. Con el fin de acortar la brecha entre el mapa y el territorio (entre lo teórico y la realidad), es fundamental obtener de los recursos involucrados: compromiso, responsabilidad y aplicación del sentido común. Adicionalmente a estos factores, la persona que lidere este proceso, deberá apoyarse principalmente en su experiencia práctica dentro del esquema que presente la normativa en cuestión.
La efectividad y la excelencia se encontrarán condicionadas en como personalicemos las buenas prácticas a la organización, como las implementemos y posteriormente las mantengamos actualizadas. La efectividad y excelencia será resultado de la capacidad que posean el líder de este proceso en combinar los recursos humanos de la organización, el presupuesto económico, y la secuencia de objetivos intermedios y finales, frente a las recomendaciones que imparta las buenas prácticas de cómo hacer bien las cosas.

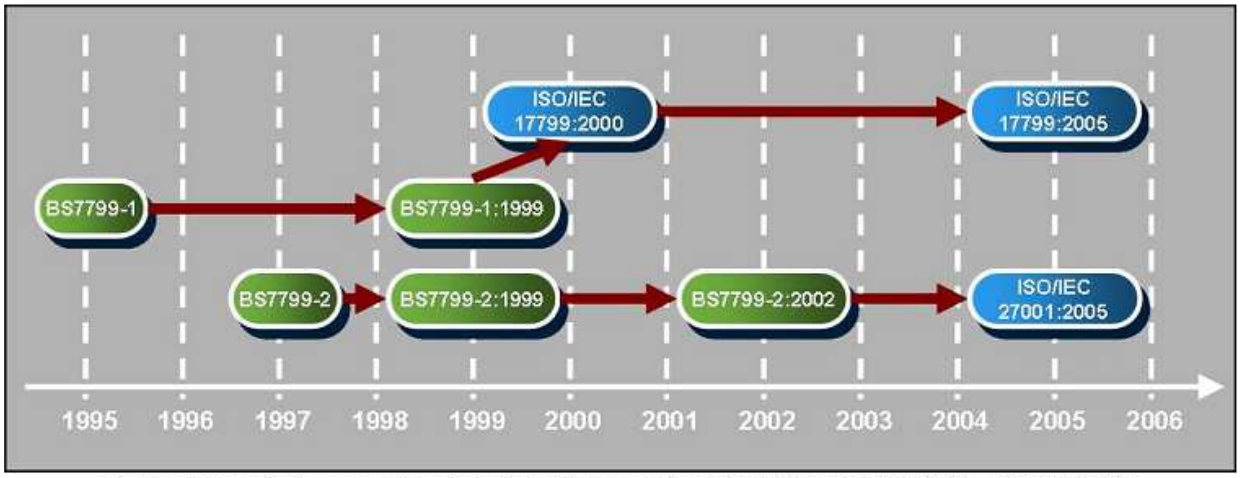
Beneficios de la aplicación de buenas prácticas

- Anula de los efectos negativos de “reinventar la rueda.
- Reduce la dependencia con los expertos tecnológicos internos o externos.
- Mejora el potencial del personal con menos experiencia del equipo de trabajo.
- Mejora y es mucho más fácil la colaboración con otros equipos de trabajo externos a la organización.

- Reduce los riesgos en términos de su frecuencia e impacto.
- Reduce la cantidad de errores.
- Mejora la calidad de la información utilizada.
- Mejora la calidad de los procesos de trabajo.
- Mejora las habilidades para gestionar y monitorear las actividades del equipo de trabajo.
- Reducen los costos operativos basándose en la estandarización incremental de los procesos.
- Mejora la confianza y confidencia, entre los integrantes del equipo la organización, socios, clientes y proveedores.
- Crea respeto ante las entidades reguladoras u controladoras externas.
- Protege y provee un valor diferencial para la organización.

Estándares aplicados a la seguridad de la información

En el año 1995, el Instituto Británico de Normas Técnicas (BSI) publicó las primeras normativas relacionadas con varios aspectos de la gestión de la seguridad informática. Connotaciones de gran importancia se sucedieron en los años subsiguientes, tales como la problemática del año 2000 (Y2K) y la unificación de la moneda europea o impacto económico en Europa frente a la consolidación en la moneda Euro. La primera edición del estándar BS 7799, no brindó los resultados esperados, transformándose en una normativa poco flexible y difícil de aplicar a conceptos básicos de la seguridad informática, que por aquel entonces no resultaba una necesidad importante y prioritaria. En este período los problemas de las funcionalidades de Internet, uso de correo electrónico, delitos informáticos, entre otros, no resultaban o no eran considerados graves, recién estaban conformando la base para lo que representarían años después en el concepto de riesgo e impacto.
En el año 1999, se desarrolla la segunda versión de la BS7799, dividiéndose en dos partes, totalmente mejoradas. La BS 7799-1:1999 (Parte 1) asociada a la tecnología de la información y códigos de prácticas para la gestión de la seguridad de la información, conteniendo el estándar con sus recomendaciones. La BS 7799-2:1999 (Parte 2) asociada a los sistemas de gestión de la seguridad de la información y especificaciones sobre guías de uso de la primera parte, puntualizando en la implementación de las recomendaciones y su certificación.



Estándares de la seguridad de la información: BS 7799, ISO 17799 y ISO 27001

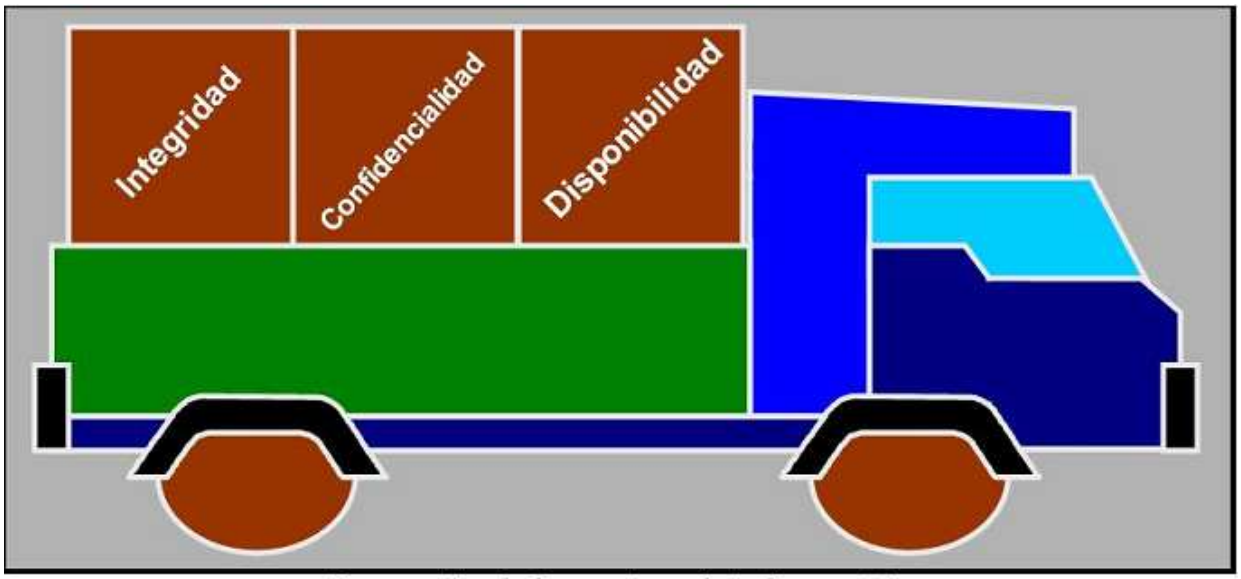
Durante esta transición, la Organización Internacional de Estándares (ISO) y la Comisión Electrónica Internacional (IEC) conforman un comité técnico con el fin de analizar en forma paralela la normativa técnica BS 7799. En el año 2000, la ISO/IEC

adopta y publica la primera parte bajo el nombre de ISO/IEC 17799:2000. El desarrollo efectuado por la ISO/IEC en esta normativa, recibió la aceptación que no tuvo sus predecesores, siendo reconocida y adoptada a nivel internacional. En Junio de 2005, la ISO/IEC 17799:2005, fue actualizada, particularmente en aspectos de análisis de riesgos, alineación de las políticas de seguridad con los requerimientos del negocio, monitoreos y control de accesos, administración de incidentes y finalmente sobre el entrenamiento y toma de conciencia de los usuarios finales sobre los aspectos de seguridad.
La segunda parte de la BS 7799, fue revisada en el 2002, y fue adoptada por la ISO en el año 2005, originando el estándar ISO/IEC 27001:2005 que referencia a la certificación de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

La ISO/IEC 17799 provee recomendaciones para la gestión de la seguridad de la información.

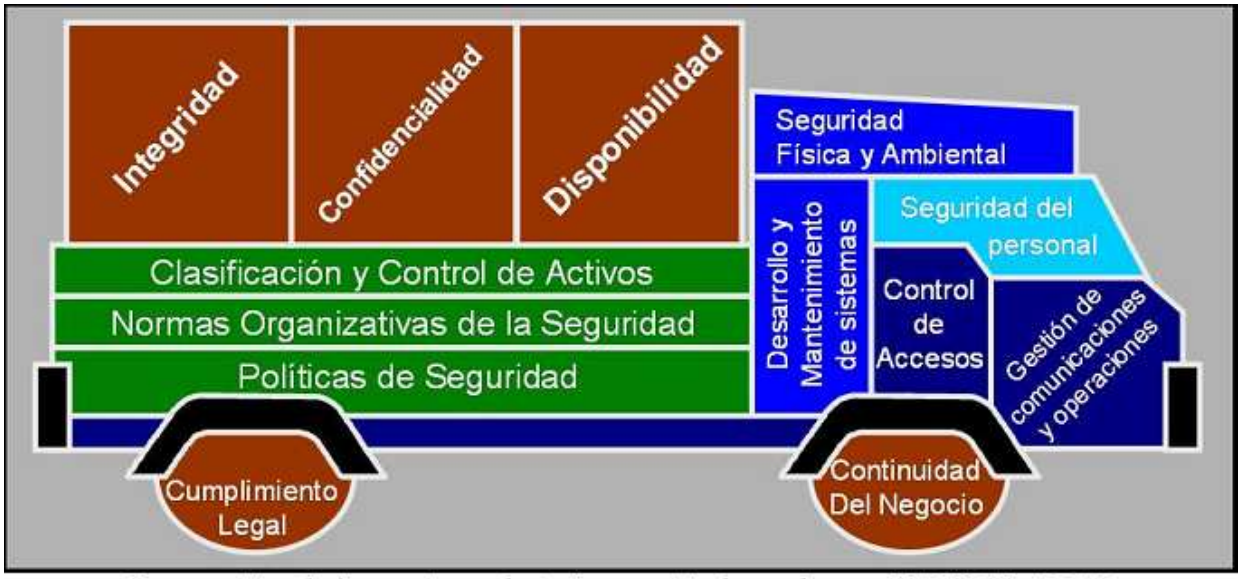
ISO/IEC 17799

ISO/IEC 17799 es un estándar internacional publicado por la Organización Internacional de Estándares y la Comisión Internacional Electrotécnica, con el fin de proveer un esquema estándar y un conjunto de recomendaciones que sirvan de guía a los responsables de la iniciación, implementación, mantenimiento y mejora de la gestión de la seguridad de la información. Es la normativa técnica de seguridad de la información más reconocida a nivel internacional. Su objetivo principal es proteger adecuadamente los activos de información de una organización. Esta normativa fue desarrollada en forma flexible, siendo neutrales a la tecnología (programas o equipamiento) a utilizar, de esta manera los conceptos en ella explicitados son fácilmente adaptables a los cambios tecnológicos que se producen en el mercado informático y a las diferentes plataformas que actualmente existen dentro de una misma organización.
Supongamos que debemos transportar algunos activos valiosos de información de nuestro interés. Estos son valorizados, como anteriormente indicamos, sobre los pilares de la integridad, confidencialidad y disponibilidad. Por ejemplo: el paquete de programas desarrollado finalmente para entregar a nuestro cliente, el conjunto de documentación de análisis y diseño de la propuesta de desarrollo que se realizará si este es aprobado, el conjunto de mis componentes y servicios de seguridad que son utilizados como base en cualquier desarrollo de aplicativos, o las lista de mis contactos de futuros clientes y los precios acordados a los cuales les venderé el software desarrollado. Todos estos son activos de información valiosos que significarán un paso clave en las tareas que estamos vinculados. En nuestro ejemplo los activos de información serán trasportados en un camión adecuado a nuestras necesidades costo/beneficio en materia de la seguridad.



Protección de los activos de información

Siguiendo con nuestro ejemplo, un camión puede estar conformado bajo las características que uno considere necesario, por lo tanto, las especificaciones del tipo de ruedas, motor, vidrios, como será la carrocería, equipos electrónicos y eléctricos, cabina, comodidades del conductor y acompañantes, entre otros. Cada uno de estos componentes es definido por una persona que toma bajo su responsabilidad la conducción de estos activos de información que son valiosos para nosotros. Asimismo debemos aclarar que el camión solo podrá funcionar si todas las partes que lo conforman se encuentran en completa armonía e integración. La rueda por si sola no es el camión, pero el camión necesita de la rueda para cumplir la función de camión. Si alguna de las partes no está presente, o bien alguna de ellas no funciona correctamente, el camión no podrá cumplir con la función para la cual es necesitado. Aplicando los conceptos básicos de la ISO/IEC 17799, el camión de nuestro ejemplo es transformado en un Sistema de Gestión de la Seguridad de la Información (SGSI), conformado por cada una de las partes que en este caso tiene el nombre de dominio de control. Estos están unidos integralmente y deben ser analizados en forma conjunta, consolidando los puntos de estudios de tecnología, procesos y personas.



Protección de los activos de información basados en ISO/IEC 17799

Estructuralmente la ISO/IEC 17799 se encuentra dividida en 10 dominios de control que cubren todas las necesidades de seguridad de la información en los diferentes niveles: estratégico, táctico y operativo. Dentro de estos dominios se establecen 36 objetivos de control y 127 controles propiamente dichos, establecidos mediante procedimientos, monitoreos, controles y rutinas prácticas que conllevan la mitigación o la reducción del nivel de riesgo que afronta las organizaciones.

Dominios de control

1.- Políticas de Seguridad.
2.- Normas Organizativas de la Seguridad.
3.- Clasificación y Control de Activos.
4.- Cumplimiento Legal.
5.- Control de Accesos.
6.- Seguridad del Personal.
7.- Seguridad Física y Ambiental.
8.- Desarrollo y Mantenimiento de Sistemas.
9.- Continuidad del Negocio.
10.- Gestión de Comunicaciones y Operaciones.

La seguridad de los activos de información (2)

Los información en torno al desarrollo de software tienen características especiales y su seguridad debe ser estudiada en forma particular con respecto a las personas, procesos y activos que están en juego.

La ISO/IEC 17799 nos permite cubrir las necesidades de seguridad de los activos de información dentro del alcance de 10 dominios de control, los cuales serán puntualmente desarrollados a continuación.

Análisis de la ISO/IEC 17799 orientado al desarrollo de software

Los dominios de control organizan el estándar internacional para cubrir todos los puntos que los responsables de la gestión de la seguridad deben tener en cuenta. Particularmente algunos de estos dominios tienen mas relación con las políticas estratégicas y los compromisos de la máxima autoridad responsable de la organización, otros dominios ponen foco en actividades tácticas o de supervisión y control, y un último conjunto de dominios aplican a rutinas operativas prácticas presentes en el día a día.

Pirámide de los dominios de control de la seguridad de la información

En esta sección desarrollaremos la ISO/IEC 17799 en cada uno de los objetivos de estos dominios, mencionando lo indicado en la normativa, y complementando con comentarios y ejemplos relacionados con nuestra experiencia. Dado que los lectores de la revista principalmente tienen un enfoque en relación a los desafíos que presenta el desarrollo, programación y mantenimiento de software, ahondaremos entonces en aquellos dominios u objetivos que directamente estén relacionados con este tema, y solo mencionaremos aquellos que indirectamente se encuentren asociados.

Las siguientes secciones están identificadas de acuerdo a esta asociación: (*) Directamente relacionada, (**) Indirectamente.

Políticas de Seguridad (**)

Este primer dominio tiene como objetivo impartir directrices sobre la administración y el soporte a la seguridad de la información. En tal sentido estas políticas establecen la prioridad e importancia que posee el concepto de la seguridad en toda la cadena de valor de nuestra organización o equipo de trabajo. Estas políticas son aplicadas como base para la toma de decisiones y determinan el accionar dentro de la organización, establecen como será el producto final que nuestros clientes tendrán en tal concepto, y cuales serán los requisitos mínimos que nuestros proveedores o servicio tercerizado deberán poseer para participar en nuestras actividades en relación a la calidad de la seguridad establecida. Este dominio en la práctica constituye un conjunto de documentos, conteniendo políticas, principios, y normas de seguridad, que reflejan las actividades en términos de seguridad dentro de la organización.
Es fundamental el compromiso y soporte de la máxima autoridad responsable de la organización, para que el espíritu de estas políticas sea parte de la práctica habitual en las actividades de los equipos de trabajo, a fin de obtener efectividad en la aplicación de estas medidas.

Normas Organizativas de la Seguridad

Infraestructura de la Seguridad de la Información (*)
Tiene como objetivo el gestionar la seguridad de la información dentro de la organización. Considerando tanto a los responsables conductores y personas referentes, como a los procesos de comunicaciones y concientización de la seguridad de la información. La infraestructura requiere de una persona con desarrollo de actividades multidisciplinarias, dado que su objetivo es involucrarse en cada una de las actividades de los equipos de trabajo y trasladar con prácticas concretas la protección de los activos propios de cada una de las funciones de estás áreas funcionales.
En nuestra actividad de desarrollo de aplicaciones, una de las funciones que es necesaria definir es el rol de IRM, o responsable de la seguridad de la información. Dependiendo del tamaño del equipo de trabajo, podrá recaer en una sola persona o en un equipo con la consecuente división de tareas. Tendrá como responsabilidades las siguientes: definir las políticas, procedimientos y guías de seguridad, coordinar las implementaciones desde la perspectiva de seguridad y aplicar las buenas prácticas internacionales, identificar y analizar puntos de riesgos en los procesos y aplicaciones, proponer soluciones basadas en la mitigación o reducción del riesgo, estudiar vulnerabilidades de los sistemas aplicativos y programas de base utilizado, analizar las tendencias frente a los incidentes reportados actuando en referencia. Estas actividades podrán ser complementadas necesariamente con especialistas expertos frente a los avances del mercado tecnológico o en lo que a metodología y buenas prácticas se refiere.
Otros roles importantes que debemos destacar dentro del equipo de trabajo son: los responsables en los monitoreos de seguridad, administración de la seguridad (cuentas de usuarios, recursos informáticos y bases de datos), administración de sistemas, operadores del centro de cómputos, responsables de las bibliotecas o versiones de aplicativos, y propiamente el equipo de desarrollo.

Seguridad del acceso de un tercero (*)

Cuyo objetivo es mantener la seguridad del mecanismo de procesamiento de información y activos de información de la organización a los que acceden terceros. Tengamos presente dos ejemplos, el del camión y el de la casa propia. ¿A quién dejarían entrar a su camión durante el transporte de los activos? ¿En nuestras casas quienes tendrían permitido el ingreso? Ahora bien, no solo debemos definir el quién puede hacer que cosa, sin esto último, ¿Cuáles son las cosas a las que tendría acceso? La persona que ingrese a su casa, ¿podrá acceder y utilizar todos los elementos de todos los cuartos? El que acceda a la cabina del camión, ¿tendrá permitido conducir el mismo, manipular los mecanismos de la carga, o disponer de los controles de la consola? En particular debemos considerar ejemplos, sobre servicios técnicos de programación o de sistemas de bases de datos, cuyo personal externo muchas veces debe acceder desde nuestras computadoras o directamente desde el centro de cómputos a la información que consolida nuestras actividades. ¿Qué controles aplicamos en estos casos?
Tenemos que identificar todos los aspectos vinculantes a aquellas personas ajenas al equipo de trabajo, quienes tienen que acceder a las instalaciones de nuestra organización y a nuestros activos de información. Sobre estas terceras partes debemos aplicar los conceptos de seguridad sobre integridad, confidencialidad y disponibilidad, aún con mayor rigurosidad que con las personas de la propia organización. La identificación y evaluación del riesgo de las mismas, frente a los activos de información a los que podrían acceder, es el punto más prioritario que debemos tener en cuenta. Otros temas a considerar en este aspecto son los tipos de accesos físicos o lógicos, el para qué tendrá acceso, si el acceso será in-situ o virtual, como definiremos el contrato con la tercera parte en relación a la confidencialidad de la información a la que tenga acceso y la responsabilidad de sus actividades dentro de nuestras instalaciones, si los terceros tendrán o no posibilidad de copiar y utilizar la información propia fuera de la organización.

Contratación externa (*)

El objetivo en este caso es mantener la seguridad de la información cuando la responsabilidad en cuanto al procesamiento de información se encuentra a cargo de otra organización contratada. Supongamos que tenemos que transportar (proteger) más activos de información que lo que nuestro camión tiene capacidad. Una de las opciones permitidas sería contratar un camión a un tercero, con o sin conductor. ¿Qué características deberían cumplir cualquiera de estos camiones de terceras partes? Naturalmente la respuesta sería: las mismas o mejores que actualmente empleamos en nuestros camiones.
En nuestras actividades de desarrollo, la contratación externa es una de las actividades más comunes, dado que principalmente buscamos alcanzar un grado de especialización alto en lo que estamos desarrollando, en particular la especialización en el diseño y la programación. En términos comerciales este concepto resulta indiscutible, pero en términos de seguridad de la información debe tenerse los recaudos pertinentes, es decir, aplicar a las organizaciones contratantes, las mismas políticas de seguridad que nosotros empleamos en la nuestra.
Dos ejemplos muy comunes en la actualidad. El primero es la contratación de terceros para el desarrollo de módulos que no conforman el núcleo del sistema que estamos desarrollando. En este caso gran parte de los componentes de programación

y parte de la documentación técnica debe ser suministrada a estos terceros para que puedan desarrollar los requerimientos pedidos. El segundo es el almacenamiento de información propia en servidores de terceros o hosting. En este caso, es más notorio y explícito el traslado de los activos de información fuera de nuestra organización. Sobre estas contrataciones mencionaremos algunos puntos a tener en cuenta: revisión de las políticas de seguridad de las otras organizaciones, los acuerdos de confidencialidad entre ambas partes, contratos sobre responsabilidades, funciones, y nivel de acceso y uso de la información, mecanismos de control de la integridad y la confidencialidad de los activos de información, disponibilidad del servicio, tipo de servicio, horarios y fechas acordadas, niveles de seguridad, e incluir la posibilidad de ser auditados periódicamente.

Clasificación y Control de los Activos

Responsabilidad sobre los activos de información (**)
Cuyo objetivo es mantener la protección adecuada de los activos de la organización. Complementando los roles indicados en las secciones anteriores, dentro de la organización debemos definir roles acorde a los activos de información que se necesiten proteger. Estos roles pueden ser: dueños de los activos, custodios de los mismos y usuarios calificados propios de cada grupo de información. Los mismos tendrán asignados responsabilidades y controles a efectuar sobre dichos activos.
Para poder controlar los activos debiéramos tener un inventario donde indiquemos el activo de información en cuestión, el tipo, dueño y custodia, y clasificación del mismo (tema que desarrollaremos luego).

Tipos de los activos de información
Los activos de información están presentes en la organización de diversas formas conocidas por todos nosotros:
- Directorios, archivos o bases de datos.
- Aplicaciones o programas aplicativos.
- Sistemas o Redes de comunicaciones.
- Componentes de hardware.
- Correo electrónico.
- Medios removibles (Discos, cintas, discos ópticos, videos, pendrives, etc.)
- Soportes físicos escritos o impresos.

Clasificación de los activos de información (**)

Debemos asegurar que los activos de información se reciban en un nivel de protección adecuado. Una vez inventariado los activos, estos deberán ser clasificados, a fin de actuar y aplicar la seguridad correspondiente. Dentro del equipo de trabajo, una buena práctica es ordenar todos los componentes de programación clasificados y relacionarlos con los otros componentes. Particularmente existen algunos programas que son más importante que otros, en relación al conocimiento específico de las personas involucradas y a la importancia que tienen estos en el total del proyecto de desarrollo. Asimismo las bases de datos, contendrán tablas con información más importante que otras. Las tablas de clientes y transacciones tienen más prioridad e importancia, mientras que las tablas referenciales, las clásicas código-descripción, tienen menos importancia. La documentación no deja de ser un activo, y por lo tanto requiere de su clasificación, entendemos que los presupuestos con horas por recurso y

costos de los mismos, el plan estratégico de colocar un programa nuevo en el mercado, o la lista de actividades diarias, tienen diferente peso sobre el hecho de clasificarlas de mas a menos importante.
La información posee diferentes grados de sensibilidad y grados de importancia. Algunos activos pueden requerir un nivel de protección adicional o una administración particular. El esquema de clasificación que utilicemos debe definir claramente los diferentes niveles de estratificación de los activos, pudiendo identificarlos y relacionarlos con los esquemas de seguridad más adecuados, y en caso que fuera necesario medidas complementarias de su uso y control.

	Integridad	Confidencialidad	Disponibilidad
Menor Seguridad V V V	Pública	Nominal	Recuperable
	Restringido	Estándar	Manual
V V V Mayor Seguridad	Confidencial	Individual	Automático
	Secreta	Doble Intervención	Inmediata

Clasificación de los activos de información

Cumplimiento Legal (**)

Los puntos a resaltar sobre este concepto, es evitar la violación de cualquier tema legal, contractual u obligaciones entre partes en relación a los compromisos y responsabilidades de la organización. Uno de los puntos más importantes, es en relación a la propiedad intelectual de los programas desarrollados por el equipo de trabajo. Los programas y con ello los elementos que los componen (objetos, componentes, estructuras de base de datos, librerías, etc.), conforman el principal activo de información de los equipos de desarrollo y mantenimiento de sistemas. De acuerdo a los compromisos contractuales y los convenios impartidos por las licencias sobre los programas comercializados, debemos considerar los aspectos referidos al alcance de uso de nuestros programas. Esto incluye: copias de la seguridad permitida, limitaciones de uso máximo de acuerdo a los usuarios finales y/o usuarios concurrentes y/o máquinas y/o servidores, transferencia y uso de los programas por terceros, y copia de la información referida a los manuales de usuario, documentación funcional y técnica.

Control de Accesos

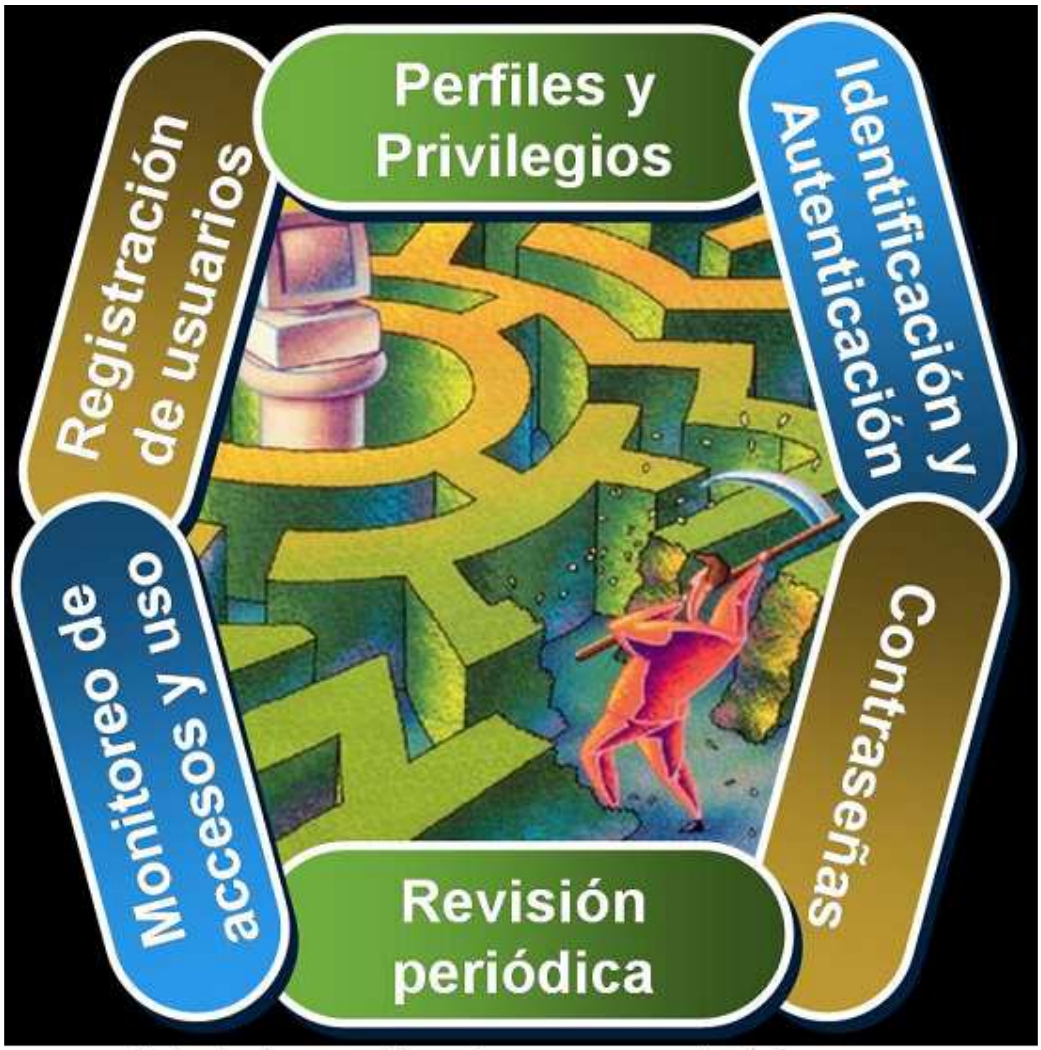
Administración del acceso del usuario (*)

El pilar de la integridad de la información es el más desatacado en este punto, basado en la esencia de impedir el acceso a las personas sin la autorización correspondiente.

La administración de los accesos de los usuarios, podemos analizarlo de acuerdo a las características de las funciones que agrupan:

- Registración de usuarios: Deben existir los procedimientos formales que nos permita registrar formalmente, las autorizaciones de los accesos de los usuarios. Los formularios de accesos, junto con toda la información particular del mismo, es uno de los reportes que naturalmente es pedido en las aplicaciones.
- Perfiles y Privilegios: Los tipos de acceso a un activo difieren de persona a persona. La habilitación de acceder no implica pleno acceso al activo en cuestión, sino que por el contrario, cada persona tendrá definido algunos privilegios de actividades y/o acciones que puede realizar. Cuando estos privilegios o acciones permitidas, se agrupan para poder ser asignadas a más de una persona, se las integran en lo que llamamos perfiles. La funcionalidad de asignación individual de privilegios, el armado y asignación de perfiles, los reportes de vinculación entre acciones y usuarios, son puntos a tener en cuenta en cualquier desarrollo de aplicaciones desde la perspectiva de seguridad de la información.
- Identificación y Autenticación: ¿Quiénes somos? ¿Cómo nos identificamos dentro? ¿Cómo nos reconocen? Los controles de accesos deberían poder contestar en forma sistémica estas preguntas. La identificación del usuario en forma unívoca, con el fin de poder realizar los controles y monitoreos pertinentes. El proceso de autenticación, permite corroborar que la persona que dice que es, verdaderamente es. Este proceso puede llevar acompañado un método de encriptación o tecnología aplicada en tarjetas inteligentes.
- Contraseñas: La gestión de contraseñas en cualquier contexto de aplicación, es un tema muy extenso, para lo cual solo mencionaremos los puntos a ser considerados en un aplicativo o programa. Las características funcionales a resaltar son: la configuración de longitudes de contraseñas, determinación y validación, cantidad de intentos fallidos, cantidad de contraseñas históricas no repetitivas, período de vencimiento y cambio de contraseñas, funciones de encriptación utilizado.
- Monitoreo de accesos y uso: Este punto consolida dos conjuntos de actividades: la registración en las bases de datos y la explotación de esta información a través de reportes puntuales requeridos por las áreas de seguridad de la información o de auditoria. La registración la basamos en desarrollar las funciones de almacenamiento y la incorporación de estas funciones en el programa en cada uno de los eventos que necesitemos capturar del usuario. Ejemplos válidos son: el ingreso y egreso del sistema, el cambio de la contraseña, el acceso a la ventana de administración de usuarios, el bloqueo de usuario debido a superar la cantidad de accesos fallidos o exitosos. Cada una de las actividades importante del sistema le corresponde una registración, con la información necesaria, en una o varias tablas de la base de datos. La información ahí consolidada nos brinda un conjunto de datos homogéneos que pueden ser explotados y de gran soporte para analizar las actividades desarrolladas por los usuarios dentro de los sistemas.
- Revisión periódica: La revisión periódica de las actividades registradas en los sistemas, frente a los privilegios y perfiles que tienen asignado cada uno de los usuarios, nos permite evaluar periódicamente la veracidad y necesidad de mantener los accesos actuales. Para ello debemos desarrollar un conjunto de

reportes dentro del aplicativo que permitan realizar este proceso de manera eficiente.



Principales consideraciones en un control de acceso

Control de acceso a las aplicaciones (*)

El acceso a las aplicaciones es un caso particular del control de accesos. No solo nos focalizamos en el acceso en sí, sino en la información contenida en los sistemas. Cuando planificamos el desarrollo de un sistema, esquemáticamente lo dividimos en módulos o grupos funcionales. Un grupo de módulos están relacionados directamente con el núcleo principal del negocio en cuestión, mientras que muchos otros son módulos comunes a todos los sistemas. Ejemplo de estos últimos son: administración de tablas de relleno (tablas clásicas de código y descripción), las funciones de ayuda del sistema, y sobre lo que estamos investigando el módulo completo de seguridad. Un módulo de seguridad perfectamente alineado a las normativas de la ISO/IEC 17799 y con la flexibilidad necesaria para estar tranquilos en el desarrollo de cada uno de nuestros proyectos informáticos. Generalmente, dejamos el módulo de seguridad para la última fase del proyecto, cuando los recursos y los tiempos se

volvieron escasos, originando un desarrollo pobre, con recortes de funcionalidad, obteniendo un producto fuera de lo que necesariamente requiere nuestro cliente responsable de la seguridad de la información. Un módulo de seguridad alineado a normativas estándares internacionales, nos brinda una ventaja competitiva y un valor agregado, para cualquier otro producto que proyectemos, considerando reducción de costos, sobre la inversión de dinero y tiempos de realizarlo una única vez.

Un módulo de seguridad alineado a normativas internacionales nos brinda una ventaja competitiva y un valor agregado al producto final

Anteriormente nos preguntamos ¿A quién dejarían entrar a su camión durante el transporte de los activos? ¿Cuáles son los privilegios a los que tendría acceso? El que acceda a la cabina del camión, ¿tendrá permitido conducir el mismo, manipular los mecanismos de la carga, o disponer de los controles de la consola? Estos son preguntas simples que generalmente no son tenidas en cuenta en el desarrollo de un proyecto.

La seguridad de los activos de información (3)

La seguridad operativa del desarrollo del software requiere que apliquemos conceptos y tomemos conciencia que existen situaciones de riesgo que pueden impactar en nuestra actividad diaria, en consecuencia, debemos saber como actuar.

Finalizado el marco estratégico y táctico, debemos estudiar los factores operativos que impactan en las actividades del desarrollo del software. Esta es la primera parte de los dominios operativos.

Seguridad del Personal

Seguridad aplicada a los recursos humanos (**)

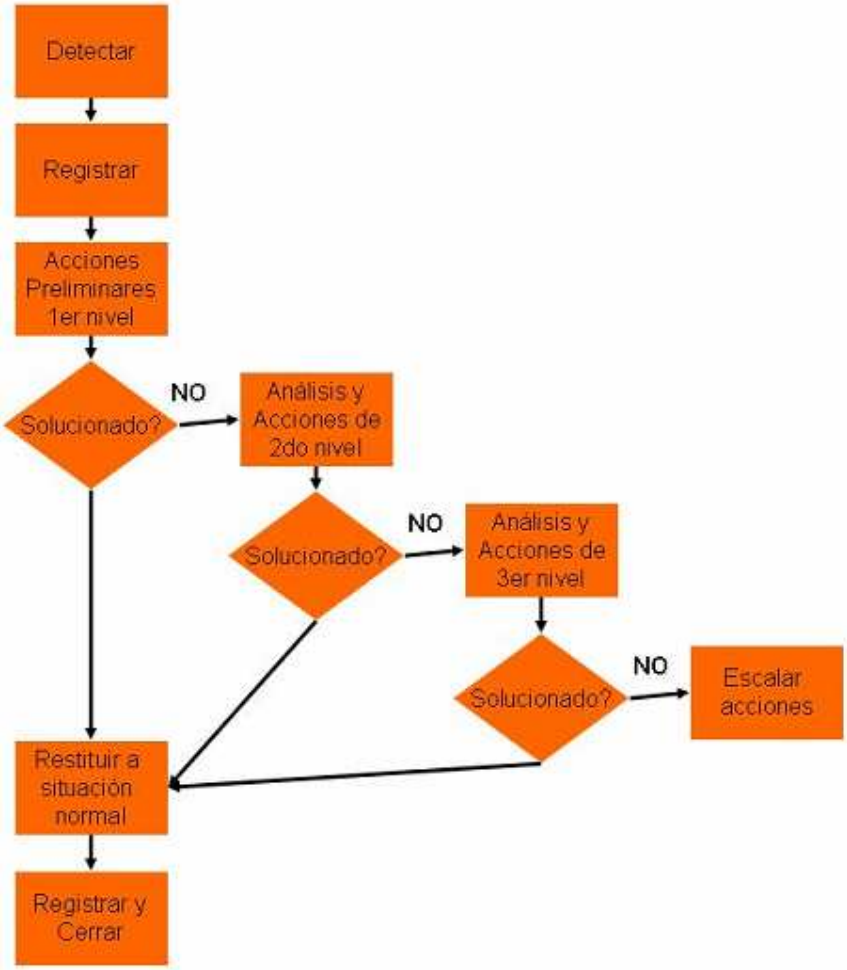
En los contextos actuales donde creemos que casi todo se resuelve con las aplicaciones de los beneficios de la TIC, muchas veces dejamos de lado los factores que esencialmente permiten explotar y dar uso a esta tecnología: los recursos humanos. Reducir el riesgo debido a errores humanos, mal uso de los sistemas, o delitos ocasionados por intermedio de estos servicios, es un factor que se origina necesariamente por la intención real o desconocimiento de las personas.
Por un lado en esta sección se aplica todas las consideraciones de revisión y selección del personal que se realizamos en la incorporación de un nuevo recurso al equipo de trabajo. Adicionalmente si este recurso es contratado, se aplican las cláusulas relacionadas con la confidencialidad en relación a toda la información propia que el equipo de trabajo produce, y los límites de responsabilidades que hablamos en otras secciones anteriores.
Por otro lado, la falta de entrenamiento específico en los sistemas, o bien, la falta de conciencia aplicada a seguridad de la información, puede disparar incidentes de seguridad en perjuicio económico y/o comercial de nuestra organización. ¿Cuántas veces nos enojamos porque nuestros usuarios o clientes no poseen el conocimiento para desarrollar tal o cual actividad en los sistemas desde sus puestos de trabajos? ¿Cuánto es el tiempo invertido en forma personal con cada uno de nuestros clientes sobre consultas de nuestro sistema que pueden ser impartidas a toda la población en conjunto? ¿Consideramos que la pregunta de un usuario es aplicada a varios otros? ¿Consideramos que uno que pregunta formula una consulta para varios que callan? Mejorar el conocimiento de nuestros clientes, nos permite mejorar la calidad de nuestros aplicativos, dado que serán nuestros clientes los que nos requieran nuevas funcionalidades que mejoren las actuales de nuestros sistemas.

Respuestas ante incidentes de seguridad y malfuncionamientos (**)

Cuando desarrollamos nuestros proyectos, tenemos tres puntos básicos donde el cliente expone sus requerimientos frente a sus necesidades funcionales con respecto a lo que actualmente le ofrecen los sistemas aplicativos. El primero punto es la definición del pedido formal, sobre lo que necesita. El segundo cuando el cliente realiza la prueba del producto desarrollado frente a los pedidos realizados. Y finalmente cuando el producto se encuentra funcionando en el ambiente de producción, durante el día-a-día productivo de su organización. El riesgo que puede provocar un incidente o un error del sistema en este tercer punto, puede ser importante de acuerdo al rol que ocupa el sistema en la cadena de actividades de la

organización. Por tal motivo debemos desarrollar canales administrativos de comunicación de estos incidentes, a fin de encontrar una solución rápida de acuerdo a las prioridades acordadas. El objetivo de la aplicación de este estándar es reducir al mínimo el daño efectuado por incidentes de seguridad y errores de mal funcionamiento, sumando a la tarea de realizar el seguimiento y aprendizaje de tales incidentes.

El establecimiento de un procedimiento de recepción, seguimiento, resolución y aprendizaje de los incidentes o errores encontrados por nuestros clientes en nuestros sistemas, demuestra profesionalismo y consistencia metodológica en nuestro equipo de trabajo. Estos procedimientos establecen los roles que ambas partes tendrán (nuestra organización y nuestro cliente) y contactos o personas referentes en caso de aparecer un incidente. Incluye la manera y el contenido en que debe ser reportado el incidente, a fin que la otra parte tenga toda la información para resolver el malfuncionamiento, eliminando cualquier mala interpretación o inferencia cuando uno no cuenta con la información suficiente. La respuesta y velocidad de resolución estarán de acuerdo al contrato de mantenimiento acordado. Una etapa importante que generalmente dejamos de lado, es el aprendizaje producto de los incidentes que surgieron en una etapa definida. El aprender de nuestros errores, suena más teórico que práctico, en particular si no es utilizado frecuentemente. El hombre es el animal que se tropieza dos veces con la misma piedra, pero ¿cuántas veces le dedicamos unas horas a analizar los errores cometidos? La aplicación de mecanismos estadísticos o de estudio detallado de los errores incurridos por nuestros sistemas, permiten determinar la existencia de incidentes concurrentes o de alto impacto. Nos permite focalizar en las causas de estos efectos que son expuestos por nuestros clientes, de esta manera nos permite mejorar la funcionalidad de nuestro sistema, y reducir costos operativos y administrativos de nuestro equipo de trabajo.



Workflow para la resolución de incidentes

Seguridad Física y Ambiental (**)

Tiene como objetivo el impedir el acceso sin autorización, daños, pérdidas, robos e interferencias a las instalaciones de la organización y a su información. La protección física de nuestros activos la debemos considerar desde aquellos terceros no autorizados que buscan acceder a nuestra información, como así también, considerando los factores ambientales que pueden suceder y afectar el uso de nuestros activos. Nuestro equipamiento tecnológico debe estar protegido físicamente de las amenazas del medio ambiente, esto es, hacer frente a contingencias provocadas por fuego, humo, agua, polvo, productos químicos, vibraciones, robo, explosivos, vibraciones o temblores, interferencias electromagnéticas o suspensión del suministro de la energía eléctrica. Cada una de estas amenazas implica la aplicación de una resolución claramente expuesta en un plan de acción. Por ejemplo la falta de energía eléctrica la podríamos subsanar con equipos de baterías o grupos electrógenos. Las alternativas para afrontar estas amenazas son varias, y se encuentran en el rango de unos pocos pesos a miles de millones de inversión. En relación al valor de los activos de información, debemos identificar los riesgos en los mismos y cual será la protección que queremos implementar, decidiendo los riesgos que mitigaremos y cuales no.

El resto de los temas de esta sección no aplica necesariamente a temas relacionados con el desarrollo de sistemas, igualmente debemos destacar dos temas importantes en relación a la información confidencial que cada uno de nosotros utiliza en la jornada laboral y que fácilmente puede dejar de proteger debido a la falta de conciencia en seguridad de la información. Estos dos temas son políticas de escritorios limpios y pantallas limpias. La política de escritorios limpios conlleva que antes de retirarnos de nuestra organización, o bien cuando nos ausentamos de forma prolongada de nuestro escritorio, controlemos que no exista información confidencial en nuestro puesto de trabajo. Un documento impreso, un disco óptico, o un disquete puede ser tomados por un tercero y provocando la pérdida de dicha información. ¿Cuántas veces controlamos nuestro escritorio y guardamos en un lugar seguro la información confidencial que nosotros utilizamos diariamente? La política de pantallas limpias, tiene la misma esencia que la de escritorios, pero aplica a la activación del protector de pantalla (con contraseña) a fin que un tercero no tenga acceso a la información que tenemos a través de la computadora. Una persona que pueda acceder a nuestra computadora, previo a que nosotros hayamos ingresado nuestra identificación y contraseña, implica que esta persona puede actuar como si fuéramos nosotros, con los riesgos que ello implica. En caso de producirse un incidente la persona responsable por dichas actividades no será otra que nosotros mismos. La implementación de un protector de pantalla con contraseña en cada una de las estaciones de trabajo requiere una inversión casi nula y de un alto beneficio para la organización, solo requiere que las personas sean concientes de que deben bloquear sus computadoras antes de dejar su puesto de trabajo. Esto último no es tarea fácil.

Activos de información que deben ser resguardados bajo la política de escritorios limpios

Continuidad del Negocio (**)

Nos proponemos realizar un viaje con el camión de nuestro ejemplo. Cargamos

nuestros activos de información y nos disponemos a encender el motor. Primer intento fracasa. Segundo intento, ni siquiera se escucha ruido. Es el único camión que tenemos para realizar el trasporte seguro y dadas las circunstancias nos encontramos estancados en un incidente no contemplado del negocio. No tenemos desarrollado un plan contingente que le permita dar continuidad a nuestro desarrollo comercial. El estándar dentro de esta sección busca contrarrestar las interrupciones en las actividades de la empresa y proteger procesos del equipo de trabajo críticos frente a grandes fallas o desastres.
Lo mismo puede ocurrirnos en nuestro entorno laboral. Cualquier amenaza que impacte directamente en nuestra infraestructura impidiendo la continuidad de nuestro negocio, la debemos identificar y formular en un plan de acción, canalizado bajo un plan de contingencia. Este plan integrará toda la información, contacto, roles y acciones a seguir en caso que existan interrupciones de gravedad. Asimismo controles preventivos y actividades de recuperación deberán ser incluidos, para anticipar las amenazas y para restablecer el normal funcionamiento una vez sobrepasado el hecho de gravedad. La velocidad de activación del sitio alternativo de contingencia dependerá de los activos de información involucrados y la inversión en tecnología disponible. Podemos pensar en la mejor propuesta, es decir, tener un sitio alternativo contingente igual a que poseemos en las instalaciones donde trabajamos cotidianamente incorporando una replicación en línea de toda la información que se modifique o se agregue por cada una de las personas. Otra alternativa es contratar a un tercero las facilidades de tecnología requeridas para el caso que ocurra una situación contingente, donde debemos indicar las características y disponibilidad de los servicios necesarios. Existen como estas diferentes alternativas a ser consideradas y depende exclusivamente de las clasificaciones de los activos de información, los posibles riesgos identificados y los tiempos de demora de inicio de actividades que considerando las políticas del negocio. Cualquier alternativa que decidamos, deberá ser mantenida actualizada y probada periódicamente (al menos una vez al año) a fin de controlar que nuestro sitio alternativo contingente se encuentra bajo las condiciones suficientes para ser utilizado en caso de una emergencia.

Gestión de comunicaciones y operaciones

Procedimientos y Responsabilidades Operativos (*)

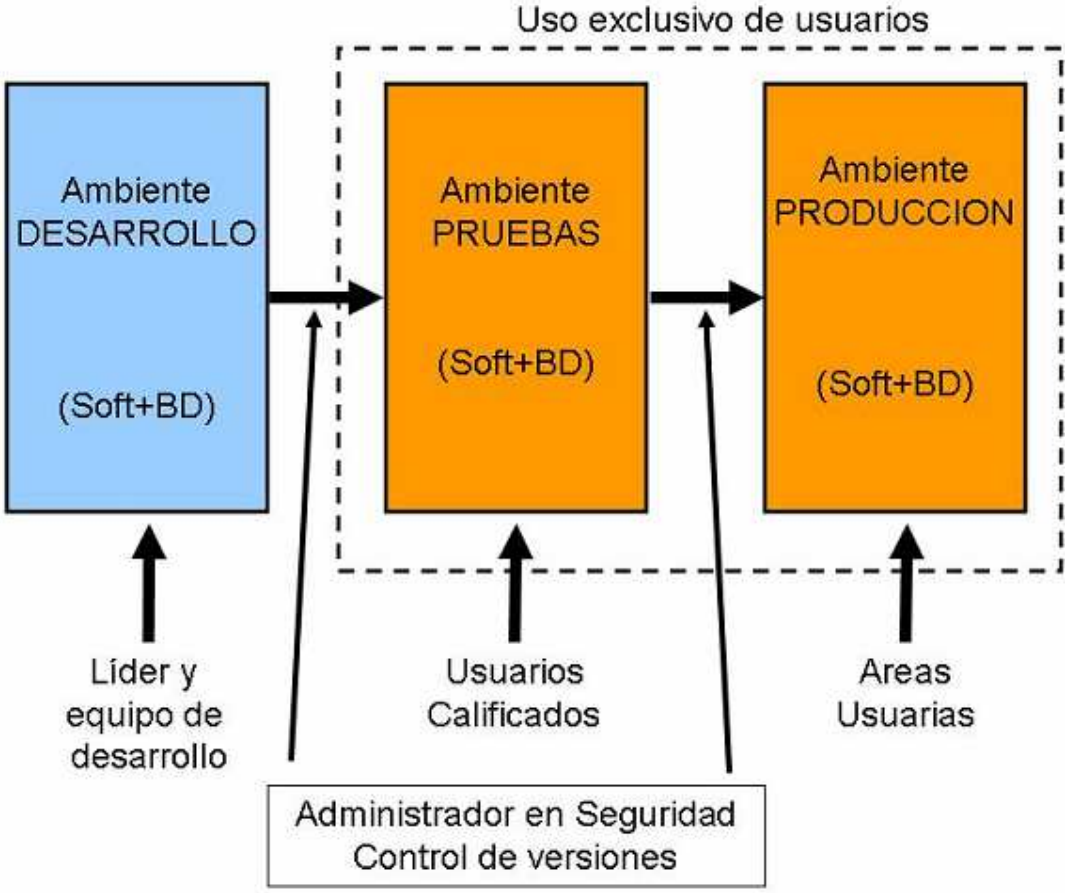
El centro operativo informático en una organización recae en el centro de cómputos propiamente, en las funciones y actividades que aquí se desarrollan. Los procedimientos y responsabilidades establecidos en esta área, se formulan para garantizar el funcionamiento correcto y seguro de los sistemas de procesamiento de la información.
Cada uno de los procedimientos contendrá el detalle de instrucciones y los pasos a seguir en cada una de las actividades que se desarrollen en el centro de cómputos. Estos procedimientos respaldan y sirven de soporte en caso de ausencias de operadores o responsables de dichas actividades. La información que debemos incluir en estos procedimientos, debe ser tal que pueda contestar los interrogantes de cualquier otra persona que desarrolle la actividad en cuestión. Parte de la información relacionada puede estar compuesta por: lista de tareas paso-a-paso, contactos de proveedores, direcciones y teléfonos de emergencias, alternativas de posibles soluciones sobre ciertos problemas, reportes antes, durante y después de realizar las tareas (dependiendo del caso).

El seguimiento de control de cambios de equipamiento y programas de base o sistemas operativos, es uno de los procedimientos particulares que debemos tener en cuenta. El análisis, implementación y control de las nuevas incorporaciones tecnológicas, (servidores, equipos de comunicaciones, sistemas operativos, programas para la administración de bases de datos, nuevas versiones de programas de base, etc.) deben ser documentados a fin respaldar el conjunto de cambios de este tipo de actividades.
Un conjunto de actividades se agrupan bajo el concepto de la protección contra programas ilícitos, esto es desde el punto de vista del licenciamiento de programas que utilizamos o introducen ilícitamente los usuarios, como así también, en lo relacionado con virus informáticos, gusanos de red, bombas lógicas y troyanos. Los procedimientos implicarán instrucciones preventivas como correctivas, en lo que a estos puntos se refieren. La incorporación de parches o actualizaciones de antivirus, sistemas de base o sistemas operativos, son de vital importancia a fin de anular o mitigar las vulnerabilidades que ellos puedan presentar.
Anteriormente mencionamos que es importante desarrollar mecanismos de seguimiento de incidentes para con nuestros clientes, lo mismo ocurre en el centro de cómputos si realizamos una vista interna del proceso. Debemos tener un procedimiento en relación a informar cualquier tipo de incidente que ocurra y debemos tener el plan de acción a seguir frente a los mismos, o bien la cadena de llamados con los referentes a quién tenemos que recurrir para desarrollar la resolución correspondiente.

La reducción de actividades ilícitas implica la separación de deberes de administración de los de ejecución, y los de control de los operativos.

La estructura del equipo del centro de cómputos, debe estar organizada de forma tal de considerar la separación de deberes, con el fin de separar la administración de la ejecución, o las tareas de control de las tareas operativas. De esta manera podemos reducir las oportunidades que puedan presentarse de modificación no autorizada o uso inapropiado de la información o de los servicios. Por ejemplo, un operador nocturno que tiene acceso a las tareas de cierre de día de una organización, no debería poder tener acceso a ingresar datos referenciales de clientes, cotizaciones o ingreso de transacciones operativas, dado que si así fuera esta persona podría ingresar transacciones para su beneficio y ejecutar el cierre de día haciendo efectiva la operación. La persona que realiza los procesos con cintas de resguardo, no debería ser la misma que quién controla si el proceso fue realizado correctamente, dado que un error operativo puede implicar una falla en el resguardo de la información a causa de una negligencia del operador. Al separar las tareas de administración de las de ejecución y las operativas de las de control, cualquier acto ilícito contra la seguridad de la información, deberá implicar una asociación ilícita con más de una persona.
La separación de deberes relaciona directamente personas con responsabilidades.
Existe otra separación relacionada con los ambientes de trabajo informáticos. Esta separación de ambientes implica aislar los entornos de desarrollo o programación, de los de prueba y los de producción, unos de otros. Los objetivos de los equipos de trabajo en cada uno de estos ambientes o entornos, son diferentes y en muchos casos programas deben informar errores e incidentes, los cuales deben ser corregidos por el equipo de desarrollo, los cuales les interesaría ingresar directamente al entorno de prueba y realizar las modificaciones directamente a fin de que dichos errores no sean informados a su líder de proyecto. Lo mismo ocurre en el ambiente de producción,

pero el impacto es mayor dado que los sistemas son los utilizados para soportar el negocio comercial en el día-a-día. Un acceso a este ambiente no controlado, podría provocar una ruptura del sistema ocasionando la discontinuidad del mismo, o peor aún, la generación y almacenamiento de información errónea en sus respectivas bases de datos, con el efecto de propagación a otros sistemas en efecto cascada. La separación de ambientes implica que tendremos asignada responsabilidades a una persona, que deberá ser la encargada de realizar el pasaje de las actualizaciones entre los diferentes ambientes y mantendrá controlado las versiones correspondientes.



Ambientes de Desarrollo, Prueba y Producción

La separación del ambiente de desarrollo, prueba y producción es necesaria a fin de reducir el riesgo de cambios accidentales de los programas o de los activos de información.

Planificación de la capacidad de los Sistemas (*)

Los proyectos de sistemas tienen centrada sus actividades en el desarrollo de la estructura lógica requerida por nuestros clientes. En particular nuestros clientes, sean estos externos o internos, nos requerirán contemplar dos consideraciones importantes:

- el conjunto de equipamiento y programas necesarios para poder ejecutar el sistema por nosotros desarrollado;
- la proyección de capacidad necesaria para soportar nuestro sistema a corto, mediano y largo plazo.

Muchas veces nos ocurre que todos los programas desarrollados desde nuestra computadora en nuestra organización funcionan correctamente, pero en el momento de realizar la instalación en nuestro cliente el comportamiento del mismo programa es errático o difiere sustancialmente. Por ello, debemos realizar el análisis y la documentación correspondiente del entorno en el cual nuestro sistema se implementará, a fin de poder realizar las pruebas en un contexto igual, pudiendo de esta manera estudiar su comportamiento previo a la entrega final a nuestro cliente. Debemos incluir como componentes del entorno, el equipamiento que se utilizará en las estaciones de trabajo, los servidores, los programas (con sus versiones y actualizaciones) complementarios a nuestro sistema para que este funcione correctamente, los servicios activos en las comunicaciones de red, las configuraciones en relación a la zona geográfica (tipo de fecha, como, punto decimal, etc.), privilegios de seguridad activos en los puestos de trabajo y en los servidores, entre otros.
Una vez en funcionamiento el sistema, debemos analizar la proyección de expansión de la información y el equipamiento necesario para su procesamiento. Esto implica analizar el crecimiento de los archivos y/o bases de datos, y la incorporación de nuevo equipamiento de almacenamiento o de servidores de procesamiento. Este crecimiento conlleva que debamos realizar un análisis conjunto entre el cliente y nosotros, a fin de determinar las estimaciones de proyección del negocio y en consecuencia el crecimiento del sistema en sí. Este crecimiento del sistema lo podremos realizar más fácil o más difícil de acuerdo al conocimiento documentado que tengamos del negocio en relación al aspecto técnico del sistema desarrollado. El crecimiento de una base de clientes o proveedores en un sistema difiere en general del crecimiento de las transacciones que pueden proyectarse de acuerdo al plan del negocio. Un módulo contable implicará un crecimiento en registros de acuerdo a las políticas regulatorias contables y en relación a las transacciones que la empresa realice diariamente. Las proyecciones sobre los requerimientos futuros del negocio nos permiten reducir el riesgo de sobrecarga del sistema, su mal funcionamiento o su no operatividad.

Resguardo y restauración de la información (*)

La estrategia relacionada con las copias de seguridad tiene como objeto, mantener la integridad y disponibilidad del procesamiento informático y los servicios de comunicación. La discusión que formalizamos en este punto es sobre la frecuencia en la que debemos realizar un resguardo de la información y por cuánto tiempo debo mantener la misma protegida en un lugar seguro. La relación costo y beneficio, debe ser estudiada y decidir una alternativa óptima en relación a la cantidad de información administrada y el tipo de actividades que desarrollamos. Por el lado del costo, debemos considerar las cantidades de soportes magnéticos u ópticos utilizados, que tipo de resguardo se realizará (completo o incremental) y el tiempo en horas del operador que realiza el proceso. Desde la perspectiva del beneficio, debemos analizar la frecuencia con la que necesitaríamos utilizar una copia de seguridad debido al riesgo de una pérdida o requerimiento de restauración de alguna información anterior.

La clasificación de los activos de información nos determina la importancia del pilar de la disponibilidad, donde nos indica cual es la frecuencia e historial de resguardo que debemos mantener. A mayor disponibilidad mayor frecuencia de resguardo y mejores mecanismos de restauración, donde pasaríamos de los clásicos resguardos en

cintas a procesos inmediatos por medio de clusters. Dependiendo de cómo se estructure el trabajo y de los condicionantes externos, clientes, proveedores y entidades regulatorias, la cantidad de resguardos almacenados históricamente variará de organización en organización.

El estudio de la ISO/IEC 17799, nos determina nuevos conceptos de seguridad aplicados en nuestros equipos y nuestro producto. En la próxima y última entrega desarrollaremos el dominio con nombre propio: desarrollo y mantenimiento de software.

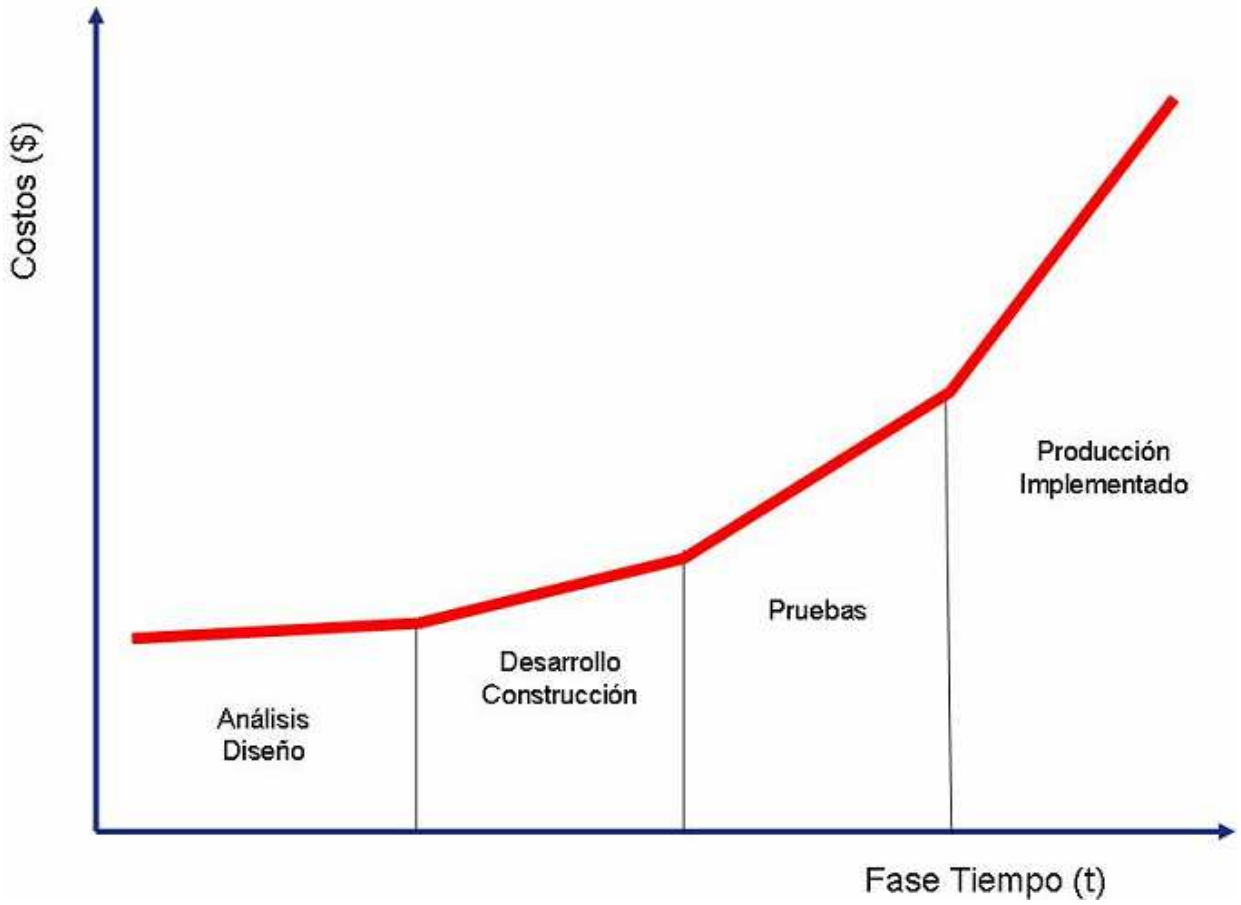
La seguridad de los activos de información (4)

La norma ISO/IEC 17799 tiene un dominio de control exclusivo sobre actividades del desarrollo de software, el cual nos permite conceptualizar en nuestras mentes un mapa de requerimientos de seguridad, previos a cualquier inicio de un proyecto.

En el desarrollo de cada uno de nuestros proyectos, los activos de información más importantes se relacionan con el software creado en todas sus variantes. Con esto concluiremos la ISO/IEC 17799.

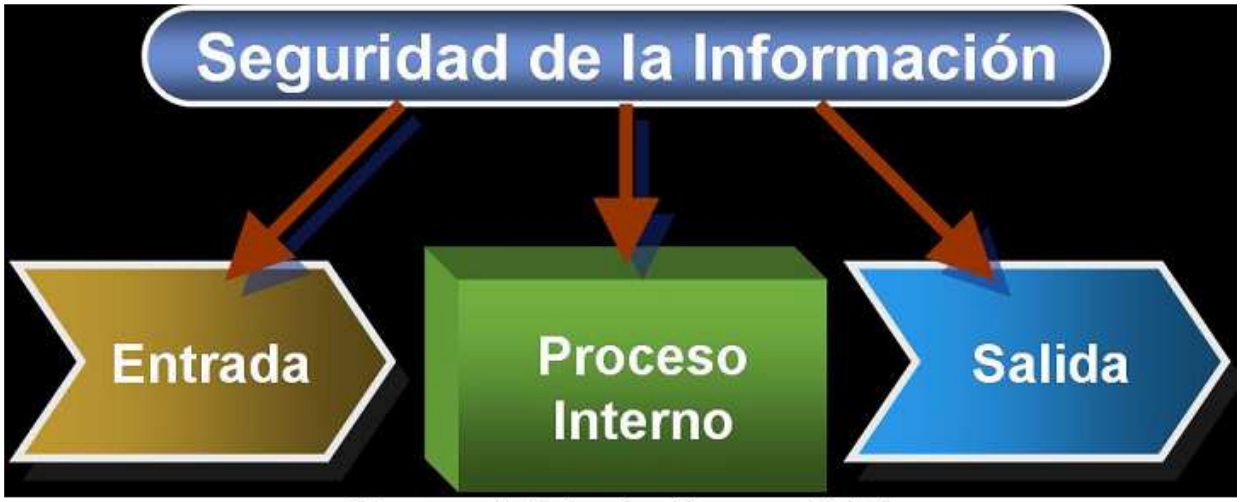
Desarrollo y Mantenimiento de Sistemas

Requisitos de seguridad de los sistemas (*)
Los requerimientos de seguridad de los sistemas deben ser garantizados cualquiera fuera el alcance que posea nuestra aplicación: para clientes externos, para clientes internos o aplicaciones complementarias. El conjunto de requerimientos funcionales sobre seguridad dependerá del análisis característico de la organización que utilice el sistema, los activos de información que serán protegidos y de la identificación de los riesgos que debamos mitigar. Las políticas de seguridad de la organización, en este punto juegan un papel de importancia dado que determinan el marco natural sobre la cual se basarán los desarrollos de seguridad. Como resultado del análisis indicaremos una lista de controles y monitoreos, que debemos reflejar dentro del sistema desarrollado, los cuales serán las herramientas del área de seguridad y/o de las áreas de auditoria. Si poseemos un módulo de seguridad completo, significará un diferencial a la hora de compararnos con otros sistemas. El costo de incorporar los requerimientos de seguridad en el primer paso de diseño es considerablemente menor, que al hacerlo luego de la fase de implementación, por tal motivo, considerar los aspectos de seguridad en su fase inicial implica no solo el valor agregado en el producto, sino también una visión integra a un costo desde el inicio bajo.



Seguridad en los sistemas de aplicaciones (*)

Las aplicaciones son utilizadas para administrar y almacenar información particular de cada una de las áreas de la organización. Esta información debe ser integra, confidencial y debe estar disponible frente a las necesidades de cada una de las personas que la requieran. Por eso uno de los objetivos en el desarrollo de programas es impedir pérdidas, modificaciones o uso indebido de datos de los usuarios con nuestros sistemas aplicativos. Para ello debemos incorporar controles, validaciones y registros de actividades que nos permita asegurar y proteger la integridad de la información.
Como diagrama clásico utilizaremos el esquema de Entrada – Proceso – Salida, donde indicaremos conceptos de validaciones y controles que debemos analizar en cualquier desarrollo de sistemas.



Esquema de Entrada – Proceso – Salida

El ingreso de datos en cualquier aplicativo, lo debemos validar y controlar, permitiendo incorporar información consistente a nuestro sistema. Estos datos de entrada pueden ser ingresados a través de las pantallas de los usuarios o capturados por interfaces automáticas o semiautomáticas desde otros sistemas. Para ello podemos incorporar validaciones a fin de mitigar los conceptos que a continuación detallamos:

- Datos incompletos o faltantes: por ejemplo la incorporación de datos obligatorios en el ingreso de una ficha de un cliente.
- Fuera de rango: por ejemplo cuando debemos ingresar una calificación de 0 a 10 y alguien ingresa un 12. Particularmente en estos casos se utilizan de acuerdo al lenguaje utilizado, los llamados combos o drop down, donde se despliega la lista de valores posibles.
- Caracteres inválidos: por ejemplo, el uso de algunos signos particulares cuando ingresamos una contraseña.
- Incongruencias transitivas entre datos ingresados: en este caso la validación se relaciona por efecto transitivo entre dos o mas datos ingresados, por ejemplo, si validamos que la fecha de nacimiento debe ser menor que la fecha de finalización de la escuela primaria y esta menor que la finalización de la secundaria.
- Dígitos verificadores, por ejemplo, el código de control en los números de CUIT (documentos personales) donde el último dígito se calcula aplicando u fórmula matemática sobre los otros primeros números.
- Momento de la validación. El proceso de validación lo podemos realizar cuando ingresamos el dato, o bien, al final cuando ejecutamos un evento específico.

El último paso de control es la salida de los datos procesados. Si consideramos que la entrada se encuentra correctamente validada y el procesamiento interno fue el correcto, naturalmente la salida deberá ser correcta. Igualmente existen algunos controles o conceptos adicionales que podemos emplear en las validaciones de salida:

- Aplicación de las validaciones símiles a las de la entrada de datos. Por ejemplo, si mostramos la ficha de un cliente podemos aplicar las validaciones utilizadas anteriormente al momento del ingreso, a fin de controlar la calidad de los datos almacenados.

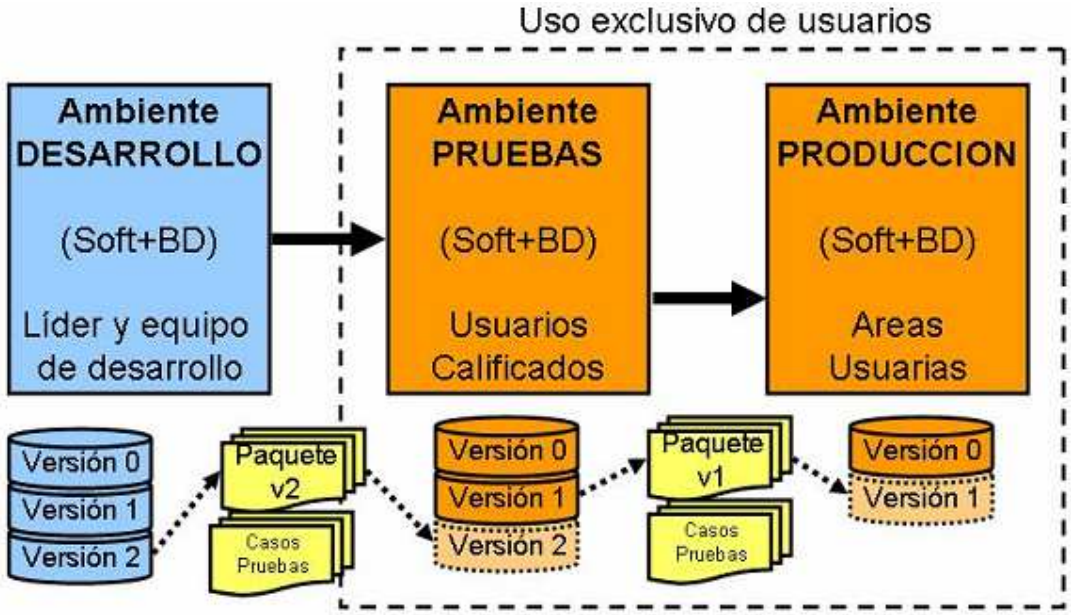
- Conciliación de la salida de información versus otra fuente de información, o un procesamiento diferente de los datos de entrada.
- Control de totales de cantidades, suma de saldos u otro tipo de numerales que nos permitan determinar si la información de salida es producto de los datos provenientes de la entrada.
- En muchos casos, la implementación lógica del sentido común frente a los datos de salida, es importante como control. En la medida que el lenguaje nos permita trasladar el sentido común a las validaciones de salida, más rica será la información suministrada.

Seguridad de los archivos y documentos del sistema (*)

Los programas y con ello los elementos que los componen (objetos, componentes, estructuras de base de datos, librerías, etc.), conforman el principal activo de información de los equipos de desarrollo y mantenimiento de sistemas.

Adicionalmente incorporamos a estos activos, toda la documentación de respaldo del análisis funcional y de diseño que nos permitió crear el aplicativo en cuestión. Por ello debemos garantizar la protección de los proyectos informáticos y sus actividades complementarias, de manera de restringir a las personas no vinculadas en este proceso y a controlar la utilización de los activos de información mencionados.
Cuando analizamos las actividades operativas, mencionamos la separación de ambientes determinados entre desarrollo, prueba y producción. En esta situación existía un responsable por el pasaje de las versiones de los programas entre cada uno de los ambientes. El foco que ahora queremos darle, es sobre la protección del conjunto de programas que estamos desarrollando antes de realizar el pasaje a la instancia siguiente. En el momento del desarrollo de un proyecto, establecemos conjuntos de requerimientos determinados por actividades de programación en común. A cada uno de los equipos de desarrollo les entregamos dichos requerimientos, junto con los programas iniciales para realizar el mantenimiento o bien para crear una nueva versión sobre estos. Las actualizaciones o mejoras son desarrolladas por los programadores y luego son integradas por una persona, quien será la responsable por controlar que versión fue entregada, que número de versión tendrá la actualizada y que conjunto de programas todavía tienen en su poder los programadores. El conjunto de estos códigos fuentes son responsabilidad de la metodología de desarrollo implementada y los controles de integridad y consolidación complementarios. Esta metodología nos permitirá mantener un orden del progreso del proyecto y un registro de auditoria de las actividades desarrolladas.
Los procesos de compilación, generación de códigos objetos, archivos ejecutables, son considerados otras instancias de esta metodología y deberán ser controlados y monitoreados de la misma manera. Particularmente los archivos ejecutables serán el último paso, que luego de pasado el control de calidad por intermedio de las pruebas unitarias del sistema, determinará un paquete o librería generando una versión del entregable. El historial de las versiones anteriores las debemos mantener de acuerdo a la política de resguardo acordada, acompañada con la documentación técnica que nos permita determinar que instancia del desarrollo aplica a cada una de las versiones resguardadas.
El acceso de terceros (clientes y proveedores), al conjunto de activos deberá ser restringido de acuerdo a la necesidad de acciones y los compromisos contractuales establecidos entre ambas partes. Este punto lo desarrollamos anteriormente cuando

cumplimiento legal, contrataciones externas y accesos de terceros.
Cuando elaboramos el proceso de control de calidad de los aplicativos, necesariamente tenemos que definir casos de pruebas que permitan encontrar falencias en el desarrollo. Una buena prueba de calidad no es aquella que no genere errores, sino todo lo contrario. Para ello es necesario armar casos de pruebas reales, donde muchas veces se utilizan copias de los ambientes de producción que determinan muy acertadamente las distintas combinaciones requeridas para las pruebas de sistemas. En tal caso medidas de confidencialidad deberán ser tomadas para preservar la información utilizada y para permitir que la misma no sea utilizada por terceros no autorizados. El copiado de la información del ambiente de producción al ambiente de prueba deberá ser autorizado por los dueños de esta información, a fin de que ellos evalúen el riesgo de utilización de la misma, documentando este proceso correctamente. Una vez que el conjunto de información copiado y procesado no es utilizado más, el mismo deberá ser borrado y debemos efectuar el control correspondiente.



Protección de los programas (versionado) y casos de pruebas (control calidad)

Seguridad en los procesos de desarrollo y de soporte (*)

La seguridad aplicada en los procesos de desarrollo y soporte, apunta a proteger los programas del sistema en cada uno de los ambientes, la información propia en cada uno de ellos y que cualquier cambio que realicemos no impacte en el resto del mapa de aplicaciones de la organización. La manera de aplicar un esquema seguridad es mediante la inclusión de procedimientos y de equipos interdisciplinarios donde intervienen responsables de las áreas usuarias y de informática. Estos equipos trabajan en forma conjunta analizando cada pedido de cambio y cada instalación de nueva versión, este sea en el ambiente de prueba como en el ambiente de producción. Donde aseguraremos la calidad de los programas instalados en el ambiente de prueba, y reduciremos el riesgo de toda implementación en el ambiente de producción. El conjunto de procedimientos, conlleva una serie de documentos y roles de personas que nos permitan realizar los controles y el seguimiento correspondiente asegurando

la integridad de los activos de información tanto del equipo de desarrollo como del resto de la organización.

Información necesaria aplicada al control de cambios de programas
- Referentes, dueños o responsables usuarios del aplicativo en cuestión.
- Referentes o responsables del área de desarrollo del aplicativo en cuestión.
- Identificación del aplicativo, versión, módulo, y detalle de la actualización o mejora instala.
- Detalle de programas, componentes, servicios y bases de datos que serán actualizados.
- Número de identificación y sobre que ambiente fue realizada.
- Aprobación formal de la prueba realizada por el área de desarrollo.
- Aprobación formal de la prueba realizada por el área usuaria.
- Casos de pruebas, resultados esperados y resultados obtenidos de dichas pruebas.
- Documentación de respaldo de las pruebas realizadas.
- Autorización del equipo multidisciplinario de la instalación o no, en cuestión.
- Conjunto de incidentes solucionados o no, luego de la prueba realizada.
- Detalles del entorno o consideraciones particulares al momento de la instalación.

Conclusión de la ISO/IEC 17799

Concluyendo sobre lo expuesto de este estándar internacional, debemos centrarnos en una posición de compromiso y responsabilidad frente a la seguridad de la información y determinar cual es el nivel de nuestro equipo de trabajo u organización frente a este tema. Los niveles adquieren relevancia dentro del marco estratégico, táctico y operativo de nuestra organización o equipo de trabajo.
Para ello hemos preparado 20 disparadores autoevaluadores que nos permitirá repasar rápidamente los dominios de la normativa y los objetivos más importantes en cada uno de ellos. Queda para cada uno de nosotros la decisión de quedarse en el estado de comodidad actual, o bien, dar el paso de llevar el conocimiento a la práctica, buscando aprender y mejorar el nivel de seguridad en lo que a nuestras actividades se refiere. El análisis efectuado sobre esta normativa tiene por objeto conocer los temas que anteriormente no sabíamos que existían y salir de nuestra ceguera en los temas de seguridad de la información, para poder ir creciendo profesionalmente, siendo mas competentes en la implementación a pasos escalonados de una normativa de estas características.

Disparadores Autoevaluadores

1.- ¿Cuáles son las políticas de seguridad que protege las actividades de nuestro equipo de trabajo u organización? ¿Consideramos que la máxima autoridad responsable de la organización se encuentra comprometida con estas políticas?
2.- ¿Quién es la persona referente en gestionar los aspectos de la seguridad de la información dentro de nuestro equipo de trabajo? ¿Cómo se encuentran conformados los roles dentro de nuestro equipo de trabajo? ¿Para qué están cada uno de ellos?
3.- ¿Para qué debe acceder un tercero a los activos de información de nuestro equipo de trabajo? ¿De qué tercero estamos hablando? ¿Cuáles son los mecanismos de control que utilizamos cuando accede un tercero?
4.- ¿Las actividades contratadas externamente cumplen las mismas o mejores políticas de seguridad que la de nuestra organización?
5.- ¿Cuáles son los activos de información más relevantes con los que tenemos contacto? ¿Qué clasificación poseen? ¿Cómo están siendo protegidos?

6.- ¿Cómo es protegida la propiedad intelectual de los programas que desarrollamos? ¿Cómo está estructurado el licenciamiento de nuestros desarrollos?
7.- ¿Tenemos un módulo de seguridad totalmente probado y alineado a las mejores prácticas internacionales? ¿Cómo hemos implementado la administración de privilegios y perfiles dentro del aplicativo? ¿Qué características distintivas puedo indicar sobre el concepto de contraseñas en nuestros desarrollos? ¿
8.- ¿Cuáles son los controles y monitoreos que son propuestos a través del módulo de seguridad de nuestro aplicativo? ¿Qué reportes o informes ofrece? ¿Qué actividades de seguridad del usuario estamos registrando?
9.- ¿Cada cuánto realizamos un entrenamiento de nuestros sistemas a todos nuestros clientes? ¿Y sobre los aspectos aplicados a la seguridad de los activos de información? ¿Nuestros clientes nos piden el entrenamiento o nosotros realizamos el pedido en forma periódica? ¿Nuestros clientes saben lo que no saben o no saben que no saben?
10.- ¿Cuál es el circuito administrativo con que cuenta nuestro equipo de trabajo, para la recepción, seguimiento, resolución y aprendizaje de los incidentes o errores encontrados por nuestros clientes?
11.- Antes de que nos retiremos de nuestro escritorio ¿Bloqueamos la pantalla de nuestra computadora a fin de que ninguna persona pueda acceder a nuestra información?
12.- Antes de retirarse de la organización ¿Controlamos que la información que queda en nuestro escritorio no sea confidencial y sea fácilmente accedida por un tercero?
13.- ¿Cuál es nuestro plan de acción en caso de ocurrir una emergencia en las instalaciones de nuestra organización que impida darle continuidad al negocio?
14.- ¿Nuestro equipo de trabajo posee separado las funciones de control de las operativas, y las administrativas de las de ejecución?
15.- ¿Se encuentran separados los ambientes de desarrollo, prueba y producción?
16.- ¿Con qué frecuencia realizamos copias de resguardos de nuestra información? ¿Por cuánto tiempo son resguardadas?
17.- ¿Cómo se definieron los requerimientos de seguridad del módulo de seguridad de nuestro aplicativo? ¿Desarrollamos un módulo único o distinto por cada uno de los aplicativos desarrollados?
18.- ¿Con qué validaciones cuenta el ingreso de datos de nuestro aplicativo? ¿Qué controles de proceso interno posee? ¿Qué controles conciliatorios implementamos en la exposición de datos de salida?
19.- ¿Qué metodología utiliza nuestro equipo en la protección de los programas y bases de datos utilizados en nuestros desarrollos? ¿Quién es la persona responsable de la protección y seguimiento de estos activos de información?
20.- ¿Cómo determinamos los riesgos y el momento oportuno de la instalación de paquetes de programación en los diferentes ambientes de prueba y producción? ¿Cómo es el proceso de control y validación?