INFORME TECNICO N° 2

RIESGOS QUE AFECTAN LA INTEGRIDAD Y AUTENTICIDAD DEL SISTEMA DE REGISTRO

Comisión de Estudios sobre Sistemas de Registro, su integridad y autenticidad documental

Contenido

I Alcance

La integridad y autenticidad de las operaciones económicas y financieras, incorporada en el Sistema de Registros a travésde su documentación respaldatoria, deben ser preservadas para que las registraciones sean eficaces como prueba ante un requerimiento legal.Para ello deberemos identificarel ciclo de vida de lasoperaciones, que se inicia con el hecho que les da origen:un correo electrónico, o un llamado deun vendedor o cliente (lo que antes se conocía como Libro de Correspondencia al ser recibido en soporte de papel), hasta el hecho económico-financiero que las finaliza. Todo el procesamiento manual o informatizado de las operaciones hasta su destrucción forma parte del Sistema de Registro, por lo tanto las dos características que se pidieron a las operaciones deben sostenerse en todo el ciclo de vida. Adicionalmente se deberá mantener la confidencialidad de los datos personales de terceros para cumplimentar la Ley 25.326.

Lo antes expuesto nos hace considerar que aquellos Sistemas de Registros cuyo tratamiento es informatizado pero con posteriorcopiatura a libros, debería asegurar la integridad y autenticidad en el proceso.

La normativa legal es clara en cuanto al cumplimientode las características de integridad y disponibilidad de la información contenida en el Sistema de Registro, pero no así en lo referido a las directivas sobre cómo **asegurar** estas obligaciones legales.

Esta situación provoca que la información que hoy damos por válida pueda no ser integra y, como hemos visto en varias oportunidades, no se encuentre disponible para los organismos de control como para los interesados en dicha información: Accionistas, Directores, Gerentes, Auditores, Clientes, Acreedores, Poder Judicial.

La falta de incorporación de controles relativos a la seguridad de la información en la normativa vigente, atenta contra la integridad de la información contenida en el Sistema de Registros, la cual puede verse afectada por eventos de seguridad originados en acciones intencionales o fortuitas, que modifiquen la información, no la procesen adecuadamente, no cumplan con la partida doble o no reflejen las operaciones económicas y financieras, como lo requiere la legislación aplicable.

Asimismo, la disponibilidad también se ve afectada por falta de normativa clara. Esta situación se ve reflejada en el proceso que se inicia conla incautación por parte del Poder Judicial y abarca la continuidad de las operaciones del ente, como por ejemplo las actitudes ilegales por parte de los responsables de los sistemas de comunicación y de información.

Por último, para que el cumplimiento legal sea efectivo,consideramos que deben darse normas claras y de fácil comprensión, basadas en buenas prácticas internacionales de la Seguridad de la Información y basados en los mismos pilares legales que la normativa aplicable a la información de los Sistemas de Registros. Deberán incluirse también la normas relativas a confidencialidad que exige la Ley 25.326 de Protección de Datos Personales, el Banco Central con la A4609 para las Entidades Financieras y el Estado Nacional a través de la Disposición 006 de 2005 y el Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional aprobada por la Decisión Administrativa 669/04 de la Jefatura de Gabinete de Ministros. (la cual es una copia de la versión 2000 de la ISO/IEC 17799 reenumerada en la versión 2005 a ISO/IEC 27002)

II Riesgos que afectan al sistema de registro

Cualquier actividad se enfrenta a riesgos, los cuales pueden ser administrados mediante un adecuado tratamiento llevándolos a los niveles aceptables para la Organización y en cumplimento de Normas Legales. El análisis de riesgos representa una cuestión que adquiere gran relevancia, ya que muchas empresas informatizadas no pueden afrontar fallas en sus equipos ya que las imposibilitan para proseguir su trabajo en forma manual.
El Sistema de Registro y su documentación respaldatoria, enfrenta, a lo largo de todo su ciclo de vida, riesgos relacionados con las áreas que explicaremos en los siguientes párrafos.

Personas que acceden

Todas las organizaciones, no importa si son con fines de lucro o no, grandes o pequeñas, privadas o estatales requieren de la intervención de personas para el registro de las operaciones que realizan. Las personas son el eslabón más débil en la cadena de seguridad de los datos registrables, ya que por desconocimiento, descuido, omisión de tareas, error y hasta la acción intencional, pueden poner en riesgo al Sistema de Registro.

Al hablar de personas, nos referimos tanto a empleados como a personal eventual, contratado, proveedores, clientes y todo aquel que puede, en forma directa o indirecta, tener acceso al espacio físico y/o lógico del Sistema de Registros. Ejemplos de estas situaciones, son variados y van desde el, acceso de personal no autorizado, accidentes del personal de limpieza (con sus productos) ante documentos que no están guardadas bajo llave, hasta el ingreso de una oferta económica, a través de sistemas con conexión remota, en un proceso licitatorio.

Un ejemplo similar se configura en el caso de un técnico que contratamos para arreglar una computadora, el cual tiene acceso a la información en ella debido a que el disco puede ser accedido por fuera de la computadora: se lo saca, lo ingresa en una caja especial que le provee por puerto USB la electricidad necesaria para que funcione y se lo accede desde otra computadora. De esta forma puede sustraer información del ente.

Por su parte, los propios empleados pueden sustraer información haciendo uso de dispositivos móviles, acceder a información restringida a su puesto de trabajo por prestarse claves, o bien terceros ajenos a la organización, que desarrollan sistemas para la misma, bien pueden “dejar puertas abiertas” para acceder a la información en ellos contenida.

Los que acceden a los soportes donde se almacena la información no solo pueden borrarla, destruirla definitivamente, sino que pueden modificarla.El riesgo puede derivar de la conducta, fraudulenta o no, del usuario, que altere cualquiera de las etapas del proceso: la entrada (información falsa), el procesamiento (programa fraudulento), el archivo, la conservación, la salida y la impresión de la información.

Entornos físicos y de las instalaciones

Los espacios físicos donde se procesa y guardan los Sistemas de Registros, así como las instalaciones pueden enfrentar riesgos relacionados con defectos de construcción, áreas inundables o zonas inseguras o afectables con tumultos y protestas, inexistencia de normalización en las instalaciones eléctricas, de provisión de gas, falta de matafuegos y fácil acceso a los espacios de procesamiento y guarda.

Equipamiento informático y soportes de resguardo

La lista de riesgos a los que se enfrentan los equipamientos informáticos y soportes de resguardo es larga, y va desde eldescuido y/o maltrato de los usuarios, falta de normalización en su fabricación,hasta la elección y mantenimiento de dispositivos de guarda que se corrompen con el tiempo (los viejos diskettes).Se carece de datos ciertos sobre la duración de los diversos soportes (magnéticos, ópticos, etc.), existiendo autorizadas opiniones técnicas que les asignan un lapso de perención, según el uso, lo que impediría su consulta después de dicho lapso.
Asimismo, las características físicas de los soportes (tamaño, homogeneidad, modos de individualización) posibilitan su pérdida y/o sustracción

Software de procesamiento

En este punto los riegos mayores están dados por tres aspectos muy importantes:

- la validación de los campos de los sistemas de procesamiento en la programación (código) que impidan errores en la carga,
- la falta de controles de acceso por tipo de usuario tanto a los sistemas como a las bases de datos, y
- la falta de sistema operativo legal y actualizado.

De allí la importancia de un adecuado sistema de diseño, revisión, documentación, testeo y aprobación, cuyo registro de tareas quede disponible para aquellos usuarios que se encuentren autorizados para su relevamiento.

Comunicaciones

Dada la complejidad del tema este se desarrolla en el INFORME TECNICO N° 3CLOUD COMPUTING ASPECTOS LEGALES Y TÉCNICOS

III Medidas para minimizar los riesgos

Los marcos de buenas prácticas para minimizar los riesgos se describían en forma integrada por el **INFORME TECNICO N° 2INTEGRIDAD Y AUTENTICIDAD DEL SISTEMA DE REGISTRO CONTABLE.**

Como mínimo, se deben incluir los siguientes controles específicos:

Política de seguridad de los registros contables:

Cumplir con la Ley 25326 de Protección de Datos Personales y documentar la política de seguridad que por tratarse de un sistema de registro incluye los datos personales de los terceros ya relacionados con ellos, y se puede sumar al resto de los datos registrales contables

Organización de la Seguridad de los registros contables:

Firmar acuerdos de confidencialidad con los empleados y terceros que pueden acceder al Sistema de Registros, a el/os sistema/s operativo/s, acceso a la red local y remota, a los firewalls y los switches físicos y lógicos, de la/s Base de Datos.

Firmar Acuerdos de Nivel de Servicios con los terceros proveedores de tratamiento, o que pueden acceder al sistema de registros, a el/os sistema/s operativo/s, acceso a la red local y remota, a los firewalls, y los switches fiscos y lógicos, de la/s Bases de Datos que contenga las responsabilidades de ambas partes, responsables por cada parte, el detalle delos servicios incluido horarios y formas de contacto y las penalidades por incumplimiento.

Los responsables de los activos dedicados al tratamiento del sistema de registro contable deberánse entregar actualizada en sobres lacrados y firmados por los responsables al Directorio, al Síndico y a los Auditores Externos e Internos, y deberá contar con:

- Inventario versionado y actualizado de todos los equipos de computación (servidores computadoras, dispositivos móviles y todo soporte de procesamiento), soportes documentales, soportes de almacenamiento lógicos (discos externos, cintas, CD, DVD o cualquier otro dispositivo lógico móvil), sistemas y archivos que conformen el Sistema de Registros Contables con sus datos identificatorios (incluídos los números de serie y de placas de comunicación), los responsables de los activos y sus autorizaciones para el tratamiento de los mismos, ubicación física y lógica de cada ítem.
- Documentación detallada versionada y con fecha de vigencia de los permisos de logs que incluya los períodos de vigencia de las claves y la configuración del/los sistema/s operativo/s, de acceso a la red local o remota, de los firewalls, los swichts, de la/s base/s de datos y al sistema de registros contables.
- Las claves de acceso de los administradores del/los Sistemas Operativos, del acceso a la Red local y remota, a los firewalls, los switches, de la/s Bases de Datos y al Sistema de Registros Contables con su respectiva fecha de vigencia.
- Cada vez que se produzcan modificaciones deberán actualizarse las copias entregadas.Tanto el Directorio como el Síndico y los Auditores Externos e Internos deberán llevar un Registro de la documentación en depósito, con fecha de entrega y período de vigencia de las claves de los administradores y verificación de actualización de la entrega en tiempo y forma, así como la guarda en caja de seguridad con apertura restringida de dicha documentación.

Seguridad de los Recursos Humanos involucrados en la registración contable

Definir puestos y responsabilidades del personal que efectúa tratamiento del sistema de registros y régimen sancionatorio por incumplimiento. Toda esta documentación deberá ser firmado por el personal y guardada en su legajo.

Capacitar al personal periódicamente sobre toda la normativa legal involucrada en Sistema de Registros, dejando registro de la capacitación efectuada en sus legajos

Gestión de Comunicaciones y Operaciones de los recursos asociados con los registros contables

La configuración del servidor delos accesos remotos vía WEB (Red WAN) o vía conexión inalámbrica (Red WAN o LAN) o inalámbricas personales (Red LAN) , de forma tal que ante la petición de conexión, verifique con llamado de retorno la identidad del peticionante antes de autorizar la conexión, de forma de significar que el acceso se desarrolla sobre líneas y computadoras previamente reconocidas como de propiedad asignada al usuario además de la identificación del mismo.

Tanto los registros de logs como los registros del Sistema de Registros Contables y la documentación respaldatoria incorporada en el sistema de registros deberán:

- Estar en servidores ubicados físicamente en la jurisdicción o en su defecto que exista una registro espejo de la totalidad de las operaciones o un backup completo en la jurisdicción.
- Estar en servidor/es ubicado/s físicamente en área segura: edificación con materiales ignífugos, con acceso restringido al personal autorizado, controles de accesos que identifiquen a los que ingresan por medios magnéticos y en lo posible biométricos, con cableado eléctrico normalizado, estabilizadores de tensión, unidades de electricidad auxiliares que permitan autonomía de cierre de operaciones, extintores de incendio adecuados al tipo de mobiliario e instalaciones existentes, sin comunicación al exterior por ventanas, temperatura regulada en promedio no superior a 22^0 grados ni inferior a 18^0, restringir el acceso al personal no autorizado y no permitir el acceso de este personal autorizado con dispositivos móviles (teléfonos celulares, laptops, netbooks, tarjetas de memoria, pen drives, CD, DVD, etc.).
- Estar preservados del acceso de terceros en forma voluntaria o involuntaria mediante una ubicación lógica protegida y con acceso controlados por firewalls físicos, de ser posible en servidores dedicados uno para el alojamiento de logs y otro para el Sistema de Registros y la documentación respaldatoria incorporada en el Sistema de Registros. El sistema de registros no puede compartir servidor con ningún software de aplicativos, comunicaciones o de procesamientos ajeno al sistemas de registros.
- Realizarse Backup (copias de resguardo)bajo las siguientes normas:
  - Deberá realizarse un Backup diario.
  - El Backup deberá incluir el Sistema de Registro, sus bases de datos, los logs del sistema operativo, los logs del Sistema de Registros y los logs de la base por el mismo período de tiempo que el que abarca el Backup del Sistema de Registros.
  - La Responsabilidaddel Backup diario deberá ser de un área diferente al de operaciones de los sistemas y aplicativos.
  - El Backup deberá estar bajo las mismas condiciones de seguridad que el Sistema de Registros.
    - Deberán realizarse pruebas mensuales de recupero de la información que permitan verificar la buena conservación de las copias de respaldo y documentarse el resultado.
    - De producirse errores en el recupero se dará parte a los sectores involucrados y de control para recuperar la información siniestrada dejándose documentado todo lo realizado y las personas involucradas.
    - Deberán almacenarse en otra locación a una distancia no menor a 1 (un) km. del lugar central de procesamiento en un lugar con características de seguridad iguales que la del centro de procesamientos de datos.
    - Si se realiza transaccion en espejo (es decir del total de lo que contiene el disco de los computador y/o servidores) este deberá hacer mediante comunicación de fibra oscura y cifrada bajo modelo SHA512 o versiones posteriores por su mayor seguridad.
    - Si se realiza mediante soportes de almacenamiento, la información deberá ser encriptada, y los mismos deberán ser trasladados a la otra locación

mediante un procedimiento documentado donde se registre fecha, hora y responsable de la entrega del traslado y la recepción.
    - Los soportes deberán ser etiquetados con la identificación de su contenido.
    - Llevarse un registro de los Backup, su ubicación lógica y física, contenido y del etiquetado identificatorio.
    - Los soportes para realizar los Backup podrán ser cintas, discos, CD, DVD y demás soportes lógicos con probada perdurabilidad temporal al deterioro.
- Los relojes de todos los sistemas de procesamiento de información dentro de un ente se deben encontrar sincronizados de acuerdo a una fuente de tiempo precisa, previamente convenida y documentada en forma pública para los entes de control.
- Deberá llevarse una red protegida en todos sus accesos tantos físicos como lógicos mediante filtros, amplificadores, swiches y firewall físicos y lógicos, y con un sistema de monitoreo que permita controlar su estado y correcto funcionamiento, así como analizar y bloquear los intentos de intrusión.
- Toda información relacionada con el sistema de registros que se transmita deberá estar encriptada.
- Actualizar todos los sistemas y aplicativos (procesadores de textos, planillas de cálculo, etc.) cada vez que el fabricante emita un parche de seguridad y/o actualización.
- Tener sistema de prevención de código malicioso (virus, troyanos, robot espías).
- La salida de equipamiento que contenga información del Sistema de Registros deberá quedar registrada con la identificación de su contenido, del responsable, fecha y hora de retiro.
- La entrada de equipamiento y su contenido deberá quedar registrada con la identificación del responsable, fecha y hora de entrada.
- Estos registros de entrada y salida deberá guardarse por el mismo periodo que los sistemas de registros.
- Si el sistema de registros recibe transacciones provenientes del comercio electrónico deberán cumplirse con las siguientes pautas de control:
    - Si la información pasa por las redes públicas, se debe encontrar protegida de actividades fraudulentas, disputas de contrato, y divulgaciones y modificaciones no autorizadas.
    - La información involucrada en las transacciones en línea se debe encontrar protegida para prevenir transacciones incompletas, que sean erróneamente direccionadas, alteraciones no autorizadas de mensajes, divulgaciones no autorizadas, duplicación o repetición no autorizada de mensajes.
- Permitir la incorporación de la documentación respaldatoria en formato digital sólo si está firmada digitalmente por el responsable del registro.
- Administrar en forma controlada por software los dispositivos de almacenamiento que se conecten con las terminales o bien bloquear las conexiones de los puertos.

Control de Accesos a los registros contables:

Registro de logs (identificación) de los usuarios

Deberá existir un módulo de auditoría que permita la revisión de lasaltas,bajas, modificaciones,procesamiento yconsulta de operaciones con la respectiva identificación del usuario y la fecha y hora de acceso.
En todos los casos y más aún si se carece de un módulo de auditoría, el Sistema de Registros, deberá tener habilitado, por cada uno de los usuarios que tiene acceso,el registro de logs de identificación al Sistema Operativo y tener habilitado y guardado el registro de logs que el Sistema Operativo(XP, Vista, Windows7, Windows Server, Linuxs. Unix, OS de MAC:Leopard, Leon, OS de IBM, Solaris, Symbian,etc.) brindan. Esta información deberá estar adecuadamente resguardada y disponible para efectuar cualquier control posterior.
Asimismo, se deberá tener habilitadopor cada uno de los usuarios, los logs de acceso a las redes que permitan el acceso al Sistema de Registros..
Por último, se deberántener documentados y archivados todos los permisos de logs y mantenerlos actualizados.

- La identificación de los usuarios para el control de accesos deberá ser privativa del usuario,preferentemente deberá ser por Firma Digital. De no poder aplicarse ese tipo de identificación para el acceso a todos los sistemas: de registros, operativo, de red, de firewall, de switches, de base de datos, se procederá de la siguiente forma:
    - El sistema deberá permitir la generación de claves encriptadas.
    - El sistema deberá limitar a no más de tres intentos antes de bloquear la clave.
    - El sistema deberá permitir la renovación de las claves por parte del usuario.
    - Para el primer acceso de un usuario, el Administrador correspondiente generara una clave de no menos de 6 caracteres alfanuméricos y con caracteres con vencimiento dentro de las 48 horas de emitida.
    - El Administrador remitirá al usuario la clave y el sistema correspondiente obligará a cambiarla en el primer ingreso a cada sistema.
    - El Administrador ante bloqueo o necesidad de anulación de la clave deberá:
        - Si es por olvido, generar una nueva clave provisoria previa identificación fehaciente del responsable.
        - Si es por bloqueo, investigar el evento de seguridad antes de emitir la clave provisoria como en el punto anterior.
        - Si el usuario se desvincula, bloquear la clave al momento de la desvinculación.
        - Si la desvinculación fue por motivos de mal desempeño del usuario,realizar la investigación de los eventos de logs que pudieron ser incidentes de seguridad.
        - Si hubo intentos de acceso en horarios fuera de la operatoria de la empresa, bloquear la clave y entrevistar al usuario para determinar si el evento es un incidente de seguridad.
- Los registros de logs al Sistema de Registros Contables como al/los Sistema/s Operativo/s, a las bases de datos y a las redes de acceso, deberán permanecer en archivo por el mismo tiempo requerido al registro que le dio origen.

Acceso restringido a la base de datos del Sistema de Registros

Las bases de datos donde se registran las operaciones deberán estar cerradas al acceso de terceros para las altas, bajas, modificaciones y procesamiento por fuera del Sistema de Registros.Asimismo, se deberá restringir la cantidad de administradores autorizadosy mantener actualizado el listado de quienes tienen acceso y los perfiles de cada uno. Por último, el módulo de auditoria que mencionamos anteriormente deberá estar activo de manera que permita consultar las operaciones a los que se sometió a la base.

Los registros de logs al Sistema de Registros Contables como al/los Sistema/s Operativo/s, a las bases de datos y a las redes de acceso, deberán permanecer en archivo por el mismo tiempo requerido al registro que le dio origen.

Adquisición, desarrollo y mantenimiento de Sistemas de Información asociados a los registros contables

Documentación del sistema

Los entes deberán tener la documentación del sistema bajo las siguientes condiciones:

- Si han diseñado el sistema: especificación detallada de requisitos funcionales y no funcionales, requisitos de infraestructura, la interfaz del usuario, modelo estáticos y de comportamiento, arquitectura, código, casos de uso como pruebas funcionales y de aprobación del usuario a través de la cual se pueda verificar el cumplimiento de esta normativa. Si no existe documentación, el ente deberá crear un usuario de control que pueda realizar pruebas para validar el sistema por fuera de la base de datos de registros a través de un ambiente de prueba con las mismas características que elsistema en uso (producción).
- Si han adquirido el sistema: requisitos funcionales y no funcionales, cumplimiento de requisitos de infraestructura, modelo de comportamiento y ciclo de vida.
- Toda modificación y mantenimiento del sistema de registro deberá quedar adecuadamente documentado.

Controles obligatorios en el diseño del Sistema de Registros

- El diseño del control de accesos debe tener una adecuada segregación de funciones para que solo el personal autorizado acceda a procesar las altas, bajas, modificaciones, consultas y procesamientos.
- Impedir la anulación definitiva de los registros.
- Tener documentado su ciclo de vida y una vez finalizado, permaneceren estado operativo a fin de poder acceder a la información procesada en su período de vida.
- Cumplir con la normativa de las Leyes 25.326 de Protección de Datos Personales, y de la Ley 11.723 de Propiedad Intelectual y su modificación sobre el derecho en el Software Ley 25.036

Ambientes de prueba fuera del sistema con las mismas características del ambiente de producción, que permitan generar casos de uso para probar la seguridad del Sistema de Registros Contables tanto en sus accesos, como en la posibilidad de realizar altas, bajas, modificaciones y procesamientos. Estos ambientes de prueba deberán ser usados antes de poner en producción las altas, modificaciones y mantenimiento del sistema cuyo proceso debe estar documentado y aprobado por el usuario responsable.

Cumplimiento de obligaciones legales, contractuales y de normativa interna relacionada con los registros contables

IV Control de la integridad y autenticidad

La forma de controlar como terceros (auditores o peritos)el Sistema de Registros se encuentra muy bien desarrollada en las Normas de Auditoria Interna conocidas como “Guía de Auditoria de Tecnología Global” (GTAG) emitida por TheInstitute of InternalAuditors.

Resumidamente, tales normas establecen cómo debe instrumentarse la revisión de la documentación de la que hablamos en los puntos anteriores. Esta documentación se refiere a los registros documentados de cumplimiento de los procesos administrativos y operativos que impactan sobre el Sistema, como es la privacidad de los datos, la documentación de la arquitectura del Sistema de Registros en todo su ciclo de vida, incluidos parches y modificaciones, los contratos y los servicios de terceros con sus correspondientes niveles de cumplimento de los servicios, controles de acceso y las pruebas o situaciones en que se llevó adelante la gestión de continuidad del negocio ante eventos que impidieron la continuidad de las operaciones relacionadas con el Sistema.

A continuación se detallan losGTAGs

- Controles de Tecnología de la Información (TI)
- Control de Gestión de Parches y Cambios: cruciales para el éxito de la Organización
- Auditoria Continua: Implicancias para el aseguramiento, la supervisión y la evaluación de riesgos
- Gestión de la Auditoria de Tecnologías de la Información
- Gobernanza de la Seguridad de la Información
- Auditando los Usuarios-desarrolladores de Aplicaciones
- Prevención y Detección de Fraudes en un mundo automatizado
- Auditando Proyectos TI
- Desarrollo de Plan de Auditoria en TI
- Gestión de la Continuidad de Negocios (BCM sus siglas en ingles)
- Gestión de Identidades y accesos
- Auditar controles de las Aplicaciones
- Tercerización de tecnologías de la información
- Gestión de Auditoria de Puntos Vulnerables de TI
- Gestión de Auditoria de Riesgos de Privacidad

Como mínimo y para aquellos que prefieran una guía rápida, consideramos que el profesional que deba verificar que la información contenida en el Sistema de Registros es íntegro y auténtico deberá tener en cuenta las siguientes revisiones previas:

La evaluación de riesgos: de existir una evaluación de riesgos de Seguridad de la Información, analizar las constancias de cumplimiento del tratamiento dado a los riesgos y en el caso de riesgos aceptados por la máximas autoridades de la Organización que los mismos no sean contrarios a las leyes vigentes (ej. asumir el riesgo de no cumplir con una Ley).

El cumplimiento legal: verificar se cumpla con la legislación vigente sin dejar de lado la que más se relaciona con la Seguridad de la Información: Ley 25.326 de Protección de Datos Personales, Ley 26.388 de Delitos Informáticos.

Las auditorías de seguridad de la información y las de la ley 25.326 de Protección de Datos Personales: verificar la existencia de estas auditorías que son exigibles a partir del tratamiento de datos de niveles intermedios y verificar si las observaciones han sido regularizadas o si las mismas están pendientes de regularización.

La existencia del manual de procesos y procedimientos de Seguridad de la Información requeridos por la ley 25.326 de Protección de Datos Personales. Verificar la existencia del manual y el cumplimiento de cada uno de los controles que en él se detallan por muestreo significativo.

Los recursos humanos: capacitación, asignación de funciones y responsabilidades: verificar mediante la documentación, que se instrumentó el nivel de capacitación y concienciación del personal, al igual que la existencia del diseño de funciones y responsabilidades del personal y el pleno conocimiento del personal acerca del mismo.

La división de funciones: verificar los documentos que demuestran la separación de tareas de las áreas de diseño, desarrollo, testeo y usuarios de los aplicativos. En los casos de que el servicio lo presten terceros, documentos que registren que la organización realizó o exigió el testeo de funcionamiento dentro de laorganización.

La seguridad de los ambientes físicos: verificar los niveles de seguridad de las áreas de tratamiento de la información en función a la normativa legal de seguridad para empleados y que la misma se aplique a los espacios de guarda y archivo y al traslado de información.

Los controles de accesos físicos: verificar el cumplimiento de la normativa de restricción de acceso a instalaciones y a información mediante los registros que debe llevarsedel acceso de personas.

Los controles de accesos lógicos: verificar mediante los módulos de auditoría de los sistemas tanto operativos como los aplicativos y las bases de datos en los que se soportan, que se cumpla la normativa de derechos de acceso respecto a la limitación de tareas según funciones (perfiles de usuarios) y el tratamiento dado a los eventos de seguridad en el acceso que puedan ser considerados incidentes de seguridad.

La documentación de los sistemas de desarrollo propio: verificar la documentación de los desarrollos propios que permitan determinar el procesamiento que se realiza, los casos de uso, la arquitectura del sistema, los controles para evitar la carga de datos incorrectos, incompletos, incoherentes o inexistentes, la existencia de módulos de auditoría que permitan verificar los accesos, tratamientos, y eventos de seguridad, el registro de quienes realizaron cada una las tareas de desarrollo desde el análisis hasta la puesta en funcionamiento.

La documentación de los sistemas desarrollados por terceros: verificar como mínimo la documentación de los procesamientos que realiza, los controles para evitar la carga de datos incorrectos, incompletos, incoherentes o inexistentes, la existencia de módulos de auditoría que permitan verificar los accesos, tratamientos, y eventos de seguridad, el registro de quienes los realizaron.

La seguridad de las comunicaciones y de las operaciones: verificar que la información que se transmite interna y externamente sea Firmada Digitalmente según lo requiere la Ley 25.506 como ya lo detallamos en el cumplimiento legal y verificar el no repudio de dichas firmas. Verificar que el procedimiento de backup y de recupero esté documentado así como también los registros de su cumplimiento y las pruebas de su recupero. Verificar la existencia, uso y actualización del sistema operativo, aplicaciones, antivirus, firewall.

V Bibliografía

- El Código de Comercio.
- Resolución 07/2005 de la Inspección General de Justicia
- Informe COSO II
- IRAM/ISO/IEC 27002Código de práctica para la gestión de la seguridad de la información
- COBIT 4.1
- MERCOSUR/ISO/IEC 27005:2008 Gestión del riesgo de seguridad en la información, 2010
- ISO/IEC 27004:2009 Information security management -- Measurement, 2009
- IRAM 17550 Sistema de gestión de riesgos. Directivas generales, 2005
- Ley 25.326 de Hábeas Data, 2000
- Decreto Reglamentario 1.558, 2001
- Disposición de la Dirección Nacional de Protección de Datos Personales 11/2006, 2006
- Michael Juergens y David Maberry "Gestión de auditoría de tecnología de la información" GTAG N° 4 (2006). Ed. Instituto de Auditores Internos, 247 MaitlandAvenue, Altamonte Springs, Florida.

VI. Autores

Este Informe fue preparado por un grupo de trabajo integrado por los Doctores:

Iglesias, Silvia G.
Lopez Aranguren, Jorge (miembro de la Comisión hasta 2012)
Mitroff, Maximiliano E.(miembro de la Comisión hasta 2012)

Versión resumida, revisada y actualizada por los Doctores Braga, Graciela I. e Iglesias Silvia G. del Capítulo Eficacia probatoria de la Contabilidad Informatizada del Libro Derecho Contable Aplicado ERREPAR

Las autoridades de la ***Comisión de Estudios sobre Sistemas de Registro, su integridad y autenticidad documental***, son los Doctores

Iglesias, Silvia G.- *Presidente*
Braga, Graciela I. - *Vicepresidente*
Valsangiacomo, Guillermo F. - *Consejero Coordinador*

El trabajo fue aprobado en la reunión plenaria del 10 de Junio de 2014 por los miembros presentes en la ocasión:

Avalos, Gustavo
Diaz, Oscar
Maggi, Marta
Mazzitelli, Esteban C.
Osso, Maria C.
Pavicich, María C.

Pavichevich, Gladys
Vera, Alejandro M.

Buenos Aires, 10 de Junio de 2014.