DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

RESOLUCION EXENTA Nº 2796

SANTIAGO, 29 DIC 2011

VISTOS:

Las facultades que me confieren el Decreto Supremo Nº 591/2011 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley Nº 19.175, Orgánica Constitucional de Gobierno y Administración Regional; el D.F.L. Nº 1/19.653, de 2.000, del Ministerio Secretaria General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Resolución Nº 1600, de la Contraloría General de la República; el DFL Nº 1/19.175, que fijó el texto refundido, coordinado, sistematizado y actualizado de la ley Nº 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; y

CONSIDERANDO:

1º Que, con el objeto de contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional, de manera de asegurar la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios/clientes/beneficiarios.

2° Que, es afán de este Gobierno Regional, responder a distintos requerimientos, y en particular, lo referente a seguridad de la información.

3º Que, este Servicio estima pertinente crear normas y procedimientos para asegurar y velar por la Seguridad de los Activos de Información.

4° Que, este Servicio considera necesario abarcar todos los Activos de Información, no realizando diferencias entre Activos Físicos y Tecnológicos.

5° Que, debido al valor de la información de este Servicio se requiere fijar normas especificas para evitar vulnerabilidades en la Seguridad de la Información.

RESUELVO:

1.- APRUÉBENSE las siguientes normas y procedimientos con el objeto de asegurar, velar, gestionar y fortalecer la Seguridad de la Información del Servicio, las cuáles se adjuntan y son parte constitutiva de la presente Resolución, la que entrará en vigencia a partir de la fecha de su total tramitación:

- Norma de Uso para los Equipos Tecnológicos Portátiles.
- Norma de Escritorio Limpio.
- Norma de Eliminación, Reutilización y Devolución de Activos de Información.
- Procedimiento de Actualización de Seguridad y Validación de la Data.
- Procedimiento de Pruebas Funcionales

11955484

2.- PUBLÍQUESE un ejemplar de la presente Resolución, Normas y Procedimientos adjuntos en el Banner de Seguridad de la Información de la Intranet Institucional.

ANÓTESE, REGÍSTRESE Y COMUNÍQUESE.

INTENDENCIA REGION METROPOLITANA
INTENDENTA

CECILIA PEREZ JARA
INTENDENTA
REGIÓN METROPOLITANA DE SANTIAGO

PUM/FRW/PSL/JGG/sbq

Distribución:
Gabinete Intendencia
Administración Regional
División de Análisis y Control de la Gestión
División de Planificación y Desarrollo
División de Administración y Finanzas
Departamento Jurídico
Unidad de Auditoría Interna
Unidad de Control Interno y Rendición de Cuentas
Unidad Regional de Asuntos Internacionales
Departamento de Gestión Institucional
Departamento de Gestión de Personas
Departamento de Gestión Documental
Departamento de Gestión de Abastecimiento
Departamento de Presupuesto y Contabilidad
Departamento de Servicios Generales
Departamento de Informática
Unidad de Desarrollo
Unidad de Soporte
Departamento de Control de Proyectos de Infraestructura y Obras Viales
Departamento de Actividades de Cultura, Deporte y Seguridad
Departamento de Transferencias de Capital
Departamento de Adquisición de Activos no Financieros
Departamento de Preinversión y Proyectos
Departamento de Planificación
Oficina de Partes.

PROCEDIMIENTO DE ACTUALIZACIÓN DE SEGURIDAD Y VALIDACIÓN DE DATA

1. INTRODUCCION

El presente documento tiene por finalidad regular el funcionamiento y mantención de los sistemas desarrollados internamente por el Servicio como también de los sistemas adquiridos y/o contratados a terceros.

2. PLANIFICACION Y ACEPTACION DE SISTEMAS

2.1. Desarrollo interno de sistemas

El Departamento de Informática efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para el Gobierno Regional Metropolitano.

El software diseñado por la Unidad de Desarrollo deberá ser analizado y aprobado por el Encargado de Seguridad, antes de su implementación.

2.2. Desarrollo por terceros

La aceptación del software se hará efectiva por las Jefaturas de División involucradas, previo análisis y pruebas efectuadas por personal del Departamento de Informática.

Únicamente se utilizará software certificado, o en su defecto, software previamente revisado y aprobado por personal de la Unidad de Desarrollo.

2.3. Especificación detallada de requerimientos

Identificar junto con los usuarios los requerimientos que ellos tienen con los activos, los procesos de negocio.

2.4. Planificación o diseño del sistema

a) Utilizar la herramienta MySql WorkBench para modelar la información.

b) Para la interfaz gráfica utilizar alguna de las herramientas provistas como DreamWeaver.

c) Las configuraciones y puesta en marcha de servicios serán en todos los casos normadas por el Departamento de Informática.

d) El personal responsable de los servicios llevará archivos de registro de fallas de seguridad del sistema, revisará estos archivos de forma frecuente y en especial después de ocurrida una falla.

2.5. Implementación

a) Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso específicas para cada usuario del entorno operativo de la aplicación y definiendo las prestaciones de la aplicación.

b) Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

c) Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones antes de ponerlas en un entorno operativo real o en producción, con el objeto de evitar redundancias en las salidas de información u otras anomalías.

3. MANTENIMIENTO DE SISTEMAS

3.1. Responsabilidad

El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal de la Unidad de Desarrollo y de la Unidad de Soporte.

El software comercial licenciado al Gobierno Regional Metropolitano, es propiedad exclusiva de la Institución; la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

En caso de transferencia de software comercial a terceros, se harán las gestiones necesarias para su efecto y se acatarán las medidas de licenciamiento relacionadas con la propiedad intelectual.

El cambio de archivos de sistema no es permitido, sin una justificación aceptable y verificable por el gestor de seguridad.

Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

4. CONSIDERACIONES GENERALES

a) Las estaciones de trabajo, con procesamientos críticos no deben contar con medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información.

b) En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que ésta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a dicha información.

c) Toda oficina o área de trabajo posee, a una distancia moderada, herramientas auxiliares (extintores, alarmas contra incendios, luz de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.

d) El suministro de energía eléctrica será únicamente a través del circuito exclusivo provisto para los equipos computacionales (red magic), o en su defecto, el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

5. HABILITACION DE LOGS

a) Se deberá habilitar un registro mediante log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

b) Mediante el uso de una bitácora de dejará constancia de la revisión periódica de los eventos registrados en los archivos logs.

c) Si se detecta algún problema de acceso o algún evento que comprometa la seguridad de la información se deberá realizar la corrección inmediata de los respectivos permisos debiendo dejar registro de estos cambios.

6. VALIDACION DE DATOS DE ENTRADA

Los datos de entrada a las aplicaciones son validados en cada uno de los sistemas para asegurar que estos datos sean correctos y apropiados, debiendo asegurar la eliminación de datos redundantes y libres de errores de digitación.

De esta manera se consideran las siguientes directrices antes de su puesta en producción:

a) Entrada duplicada u otras comprobaciones de entrada, tales como :
   - Valores fuera de rango
   - Caracteres inválidos en campos de datos
   - Pérdida o datos incompletos
   - Exceder límites superiores e inferiores de volúmenes de datos
   - Datos de control no autorizados o incoherentes

b) La Unidad de Desarrollo revisará periódicamente el contenido de campos clave o archivos de datos para confirmar su validez e integridad, así como la inspección de documentos físicos de entrada ante cualquier cambio no autorizado.

c) Procedimiento para responder errores de validación.

d) Definición de responsabilidades de todos los usuarios involucrados en el proceso de ingreso de información a los sistemas.

e) Registro y almacenamiento de logs de actividades implicadas en el proceso de entrada de datos.

7. VALIDACION DE LOS DATOS DE SALIDA

La salida de datos de una aplicación se valida para asegurar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.

La veracidad de los datos debe evaluarse en las pruebas de instalación o actualización de sistemas en conjunto con la Unidad de Desarrollo antes de la puesta en producción de un sistema o actualización de éste, de manera de establecer un nivel de satisfacción ante la lectura de ésta en ámbitos de exactitud, entereza, precisión y clasificación de la información.

Es responsabilidad de cada usuario el uso o divulgación de la información obtenida del sistema.

Por cada sistema se definirán las responsabilidades de todo el personal implicado en el proceso de salida de datos, en conjunto con la jefatura de cada usuario.

Será responsabilidad de cada jefatura de unidad involucrada definir sus métodos de entrega de información con los roles de usuarios que les compete en cada sistema.

8. CONTROLES CRIPTOGRAFICOS

De modo de proteger la confidencialidad, autencidad o integridad de la información, se deben establecer controles criptográficos para las claves de acceso a los sistemas. Se ha determinado usar el estándar algoritmo SHA1 en la siguiente forma:

a) Todos los sistemas deben tener aplicada criptografía en las password.

b) Se evaluará en la etapa de desarrollo de la aplicación la posibilidad de aplicar este algoritmo a más información la que deberá determinarse de acuerdo a la criticidad y confidencialidad de los datos en conjunto con el Jefe del Departamento de Informática.

9. SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

La seguridad aplicada al acceso de los archivos de sistemas y al código original de programas será controlado, y estos podrán ser manipulados e instalados únicamente en las 2 estaciones de trabajo de la Unidad de Desarrollo.

Los accesos serán a través del software de control de versiones llamado "SUBVERSION" el que entrega clave para acceso al código que se encuentra centralizado en el servidor de desarrollo.

La entrega de estas claves será de responsabilidad única del encargado de la Unidad de Desarrollo y/o la Jefatura del Departamento de Informática.

Las bibliotecas de software o librerías deben ser documentadas cada vez que se realice alguna modificación. Esta modificación debe ser precedida por una copia de seguridad de la versión antigua indicando fecha de modificación, autor y motivo de la actualización.

10. PROCEDIMIENTO DE ACTUALIZACIÓN DE SOFTWARE EN PRODUCCION

Para reducir al mínimo el riesgo de corrupción en sistemas en producción, se consideran las siguientes directrices en el control de cambios de los sistemas en producción:

a) Los cambios serán aplicados únicamente por el encargado de la Unidad de Desarrollo, el encargado de la Unidad de Soporte o la Jefatura del Departamento de Informática.

b) Se utilizarán inicialmente servidores de prueba en todos los aspectos o capas de desarrollo.

c) Se utilizarán los datos de prueba obtenidos sobre copias de los sistemas en producción.

d) Se registrarán todas las pruebas en bitácoras de funcionamiento.

e) Se deben incluir pruebas sobre la utilidad, seguridad, efectos sobre otros sistemas y accesos de usuario.

f) La versión en ejecución del sistema en producción a modificar debe ser respaldada junto con la data y rotulada en cintas de respaldos indicando fecha, autor, sistema y motivo de la baja de la versión.

g) Si la actualización corresponde a un sistema de un proveedor externo esta acción debe:
   - Estar respaldada inicialmente con un contrato de mantenimiento con el proveedor.
   - Validar igualmente en los servidores de prueba del Servicio su funcionamiento antes de la puesta en producción de la modificación.
   - Los procesos de prueba en ningún caso serán mediante permisos de acceso en forma remota para el proveedor.
   - Todas las pruebas deben ser supervisadas por el encargado de la Unidad de Desarrollo, el encargado de la Unidad de Soporte o la Jefatura del Departamento de Informática.

h) Se identificarán 2 grandes grupos de software y de acuerdo a esto se determinarán los pasos de actualización.
   - Software base: Corresponde a aquellos programas que se entregan instalados en cada computador para uso o desarrollo de productividad de cada usuario, estos son: Sistema operativo, herramientas Microsoft, herramientas Adobe.
   - Software interno: es aquel desarrollado por el Gobierno Regional Metropolitano o para una cierta función específica adaptada a los procesos internos de este.

11. ACTUALIZACIÓN SOFTWARE BASE:

Esto aplica a todas las aplicaciones sometidas por proveedores de software a evaluaciones de vulnerabilidad y liberación de patch que deberán ser controladas en su instalación y distribución a los usuarios. También aplica a sistemas de servidor y soluciones de hardware/software. Lo anterior se llevará a cabo de la siguiente manera:

a) La Unidad de Soporte preparará un listado con todos los equipos computacionales que se verán afectados por la actualización.

b) Determinar el ámbito de seguridad comprometido al que interviene la actualización.

c) Registrar en bitácora la versión actual en funcionamiento y el o los objetivos de los cambios que aplican a la versión de actualización a instalar.

d) Se deben especificar los tipos de usuarios, software interno que utilizan y niveles de acceso de cada uno de éstos.

e) En uno o más equipos de pruebas realizar la instalación del software de actualización. El proceso se puede apoyar en el uso de máquinas virtuales.

f) Instalar los software internos utilizados por cada usuario conectados al servidor de base de datos de pruebas del Servicio.

g) Crear una cuenta de usuario de pruebas para cada uno de los tipos de usuarios detectados, se deben otorgar permisos similares a cada uno de los usuarios de prueba de los que serán afectados por la actualización.

h) Realizar cada una de las pruebas correspondientes a cada usuario ya sean en los software base y en los software internos realizando pruebas de ingreso, consultas, emisión de reportes o auditorías según corresponda. Se deben realizar pruebas de seguridad por cada acceso de usuario.

i) Instalar drivers de dispositivos periféricos de los usuarios de modo de realizar pruebas de compatibilidad.

j) Entregar los resultados de las pruebas al Jefe del Departamento de Informática quien determinará las acciones a realizar.

12. ACTUALIZACIÓN SOFTWARE INTERNO:

a) Registrar en bitácora la versión actual en funcionamiento y los cambios que aplican a la versión de actualización a instalar y a que equipos van a afectar.

b) Se deben especificar los tipos de usuarios, software interno que utilizan y niveles de acceso de cada uno de éstos.

c) En los servidores de aplicaciones y base de datos instalar las versiones de prueba del software a actualizar.

d) Crear una cuenta de usuario de pruebas para cada uno de los tipos de usuarios detectados, se deben otorgar permisos similares a cada uno de los usuarios de prueba de los que serán afectados por la actualización.

e) Realizar cada una de las pruebas correspondientes a cada usuario ya sean en los software base y en los software internos realizando pruebas de ingreso, consultas, emisión de reportes o auditorías según corresponda. Se deben realizar pruebas de seguridad por cada acceso de usuario.

f) Si se detecta algún error se deberá invalidar la actualización, registrar en la bitácora el problema, realizar todos los cambios respectivos y proceder nuevamente en el punto a), de modo de garantizar la operatividad y continuar con un procedimiento rollback que no interfiera la normal ejecución de los sistemas.

g) Instalar drivers de dispositivos periféricos de los usuarios de modo de realizar pruebas de compatibilidad.