DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA

APRUEBA POLITICA DE DESARROLLO DE SISTEMAS DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3054

SANTIAGO, 22 DIC 2017

VISTOS:

El Decreto Supremo N° 331/2017 del Ministerio de Interior y Seguridad Pública; las facultades que me concede el Artículo 24 letra ñ) de la Ley N° 19.175, Orgánica Constitucional de Gobierno y Administración Regional; el DFL N° 29 de 2004 del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, Estatuto Administrativo; el Decreto N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

1.- Que, el indicador de Seguridad de la Información es un instrumento de control de gestión en las instituciones públicas, para la exitosa implementación de un Sistema de Seguridad de la Información;

2.- Que, es importante considerar los lineamientos que establece la "Política Nacional de CiberSeguridad", la cual señala como esencial dentro de un Sistema de Gestión de la Seguridad de la Información (SGSI), la gestión del riesgo;

3.- Que, la gestión del riesgo permite la identificación de amenazas, valoración y priorización de controles que ayudan a mitigar los mismos, detectados en la institución;

4.- Que, siempre existirá un riesgo residual con el cual hay que convivir como institución, pero es importante establecer el número de controles que mitiguen éstos, hasta el nivel que el riesgo residual sea aceptable.

1617716

5.- Que, es decisivo que cada institución comprenda que el número de controles que decida implementar, será a partir del resultado del perfil de riesgos que cada servicio enfrenta;

6.- Que, un riesgo de seguridad de la información corresponde a una amenaza potencial que podría afectar activos de información, vinculados a los procesos de soporte institucional y/o a los procesos de provisión de Productos Estratégicos (bienes y servicios) establecidos en las definiciones estratégicas institucionales (Formulario A1 DIPRES), y por tanto causar daño a la organización;

7.- Que, los servicios deben determinar cuáles son los riesgos de seguridad que afectan sus productos estratégicos del formulario A1 DIPRES, ello permite priorizar qué controles de la Norma deberán ser implementados para mitigar éstos;

RESUELVO:

1.- DÉJESE sin efecto la Resolución Nº 2796 del 29 de diciembre del 2011, que aprobó el Procedimiento de Actualización de Seguridad y Validación de la Data y Procedimiento de Pruebas Funcionales del Gobierno Regional Metropolitano.

2.- APRUEBASE la Política de Desarrollo de Sistemas del Gobierno Regional Metropolitano de Santiago.

ANOTESE Y PUBLIQUESE

INTENDENCIA REGION METROPOLITANA
INTENDENTE

JUAN PABLO GOMEZ RAMIREZ
INTENDENTE (S)
REGION METROPOLITANA DE SANTIAGO

JFF/GEP/VGM/MRT/JIG

Distribución:
- Funcionario Gobierno Regional Metropolitano de Santiago
- Honorarios Gobierno Regional Metropolitano de Santiago
- Comité de Seguridad de la Información
- Oficina de Partes

Política de Desarrollo de Sistemas

1 INDICE

2 OBJETIVO

EL objetivo de esta Política es establecer las reglas para el Desarrollo de Sistemas en el Gobierno Regional Metropolitano, además de considerar el proceso formal de los procedimientos de las pruebas funcionales de los sistemas informáticos del Servicio el que se deberá realizar en forma periódica de acuerdo con lo establecido, para así poder asegurar y validar el correcto, íntegro y eficaz funcionamiento de toda la plataforma tecnológica (Equipos, Sistemas, Respaldos, etc.) que se utilizan en el Gobierno Regional Metropolitano de Santiago.

3 ALCANCE

Debido a que en la actualidad el Servicio cuenta con sistemas informáticos en operación, entre desarrollos propios, adquiridos y/o contratados a terceros, más los sistemas de orden gubernamental, entre computadores de escritorio y portátiles, es de gran importancia y criticidad la constante verificación de los sistemas informáticos en operación con el objeto de prevenir posibles fallas o contingencias que se puedan producir.

Esta política busca resguardar Servidores, equipos fijos, portátiles y es aplicable a todo equipamiento computacional perteneciente al Gobierno Regional Metropolitano

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática a través de su Unidad de Desarrollo será quien estará detrás de todo Desarrollo, ya sea propio o tercerizado

La Unidad de Desarrollo se encargará de llevar en control sobre los códigos fuentes, permitiendo su acceso solo a personal autorizado.

La Unidad de Desarrollo, deberá analizar la situación que se presenta con un Cliente (funcionario o unidad demandante del software en desarrollo, de manera de diseñar el mejor modelo que se adapta a su necesidad, haciendo una maqueta de prueba y presentarlo para una aprobación en conjunto para finalmente ponerlo en prueba y luego en producción.

La Unidad de Desarrollo será responsable de hacer el seguimiento de sus propios progresos llevando un detalle de todo cambio o modificación. Además será responsable de ir documentando el o los códigos de manera de permitir a cualquier desarrollador explicar cosas que no resulten tan evidentes del código en sí.

El Encargado de la Unidad de Desarrollo será el responsable de ser contraparte técnica ante el desarrollo de sistemas externos en todas sus etapas, desde la planificación hasta su marcha blanca.

La Unidad de Desarrollo será quien finalmente capacite al usuario de cómo usar la aplicación resolviendo cualquier duda de este.

El cliente o el jefe de la unidad demandante deberán aprobar finalmente el proyecto dando por cerrado el ciclo de Desarrollo.

5 CONTROL NORMATIVO SSI

La siguiente política tiene por finalidad dar cumplimiento a los siguientes controles de la norma NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.09.04.05	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas.
A.12.01.02	Gestión de cambios	Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de la información, y los sistemas que afecten la seguridad de la información.
A.12.01.04	Separación de los ambientes de desarrollo, prueba y operacionales	Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.
A,14.01.01	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o en las mejoras para los sistemas de información existentes.
A.14.01.02	Aseguramiento de servicios de aplicación en redes publicas	La información relacionada a servicios de aplicación que pasa por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada.
A.14.01.03	Protección de las transacciones de servicios de aplicación	La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no-autorizada del mensaje.
A.14.02.01	Política de desarrollo seguro	Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.
A.14.02.02	Procedimientos de control de cambios	Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.
A.14.02.03	Revisión técnica de las	Cuando se cambian las plataformas de operación, se

	aplicaciones después de los cambios en la plataforma de operación	deben revisar y poner a prueba las aplicaciones críticas de negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.
A.14.02.04	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta.
A.14.02.05	Principios de ingeniería de sistema seguro	Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación del sistema de información
A.14.02.06	Entorno de desarrollo seguro	Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.
A.14.02.07	Desarrollo tercerizado	La organización debe supervisar y monitorear la actividad de desarrollo de sistemas tercerizada.
A.14.02.08	Prueba de seguridad del sistema	Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad
A.14.02.09	Prueba de aprobación del sistema	Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y o versiones nuevas.
A.14.03.01	Protección de datos de prueba	La datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa

6 DESARROLLO DE LA POLITICA

6.1 PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

6.1.1 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.

6.1.2 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.

6.1.3 Procedimientos de Desarrollo Seguro

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

En la fase de diseño de datos, deben definirse los procedimientos de seguridad, confidencialidad e integridad que se aplicarán a los datos:

- Procedimientos para recuperar los datos en casos de caída del sistema o de corrupción de los ficheros.

- Procedimientos para prohibir el acceso no autorizado a los datos. Para ello deberán identificarlos.

- Procedimientos para restringir el acceso no autorizado a los datos debiendo identificar los distintos perfiles de usuario que accederán a los ficheros de la aplicación y los subconjuntos de información que podrán modificar o consultar.

- Procedimientos para mantener la consistencia y corrección de la información en todo momento.

Existirán dos niveles de integridad: la de datos, que se refiere al tipo, longitud y rango aceptable en cada caso, y la lógica, que hace referencia a las relaciones que deben existir entre las tablas y reglas del negocio.

6.1.4 Principios de Ingeniería de Sistema Seguro

Se designará un Administrador de Datos, ya que es importante centralizar en personas especializadas en el tema, las tareas de redacción de normas referentes al gestor de datos utilizado, definición de estándares y nomenclatura, diseño de procedimientos de arranque y recuperación de datos, asesoramiento al personal de desarrollo, etc.

Es importante la utilización de metodologías de diseño de datos. El equipo de analistas y diseñadores deben hacer uso de una misma metodología o Sistema de diseño, la cual debe estar en concordancia con la arquitectura de la Base de Datos elegida jerárquica, relacional, red, orientada a objetos, etc.

Debe realizarse una estimación previa del volumen necesario para el almacenamiento de datos basada en distintos aspectos tales como el número mínimo y máximo de registros de cada entidad del modelo de datos y las predicciones de crecimiento.

A partir de distintos factores como el número de usuarios que accederá a la información, la necesidad de compartir información, las estimaciones de volumen, etc. se deberá elegir el S.G.B.D. más adecuado a las necesidades de la empresa o proyecto en cuestión.

Se considerarán diversos aspectos en relación al uso de bases de datos:

- Registro de accesos y actividad (ficheros log). Los S.G.B.D. actuales suelen tener ficheros de auditoria, cuya misión es registrar las acciones realizadas sobre la base de datos, haciendo referencia a nombre de objetos modificados, fecha de modificación, usuario que ha realizado la acción, etc.

- Registro de modificaciones realizadas por la aplicación. Una aplicación bien diseñada debería grabar información necesaria para detectar incidencias o fallos. Estos atributos, también llamados pistas de auditoria, pueden ser la fecha de creación o de última modificación de un registro, el responsable de la modificación, la fecha de baja lógica de un registro, etc.

- Tunning periódico de la Base de Datos. Periódicamente, el Administrador de Datos debe controlar el crecimiento y la evolución de los ficheros de la base de datos a fin de tomar las medidas necesarias para mejorar el rendimiento del sistema.

- Mantenimiento de la Base de Datos. Dado que la base de datos es un objeto cambiante, periódicamente debe efectuarse su mantenimiento, ya que su estructura, volumen, etc., se modifican con el paso del tiempo. Asimismo, deben revisarse los roles de los usuarios para adecuarlos a los posibles cambios que se vayan produciendo.

6.1.5 Separación de ambientes de Desarrollo

Se implementa el uso de un ambiente de desarrollo Integrado llamado IDE como NetBeans que permite herramientas de construcción y depuración automáticas, además de la seguridad ante una eventual pérdida de las fuentes de los proyectos, ya que este nos permite hacer un rollback en cada archivo.

La metodología para el desarrollo de software y que permita crear productos de calidad y seguros es SCRUM, este es un método ágil para el desarrollo de software que se basa en la codificación del software más que en la documentación, obteniendo resultados en poco tiempo para presentar al cliente.

Uso de un lenguaje de programación de Alto Nivel como PHP, que nos permite depurar y encontrar errores tempranamente antes de poner en producción el software a construir.

6.1.6 Pruebas de Seguridad en el Sistema

En la fase de pruebas funcionales dentro del proyecto, se "testea" el software con escenarios no planificados, tales como: valores fuera de rango, tipos de datos incorrectos, acciones fuera de orden, etc. Estos datos son seleccionados y controlados y protegidos estrictamente para no producir alteraciones en las Bases de Datos.

Repositorio central manejado con subversión con usuario y contraseña solo para los desarrolladores del proyecto, a este podrán acceder a distintos artefactos que componen el proyecto, tales como: fuentes, imágenes, diagramas, etc.

Se implementa el software subversión para manejar el control de versiones de las fuentes y otros artefactos del proyecto.

6.1.7 Entorno de Desarrollo seguro

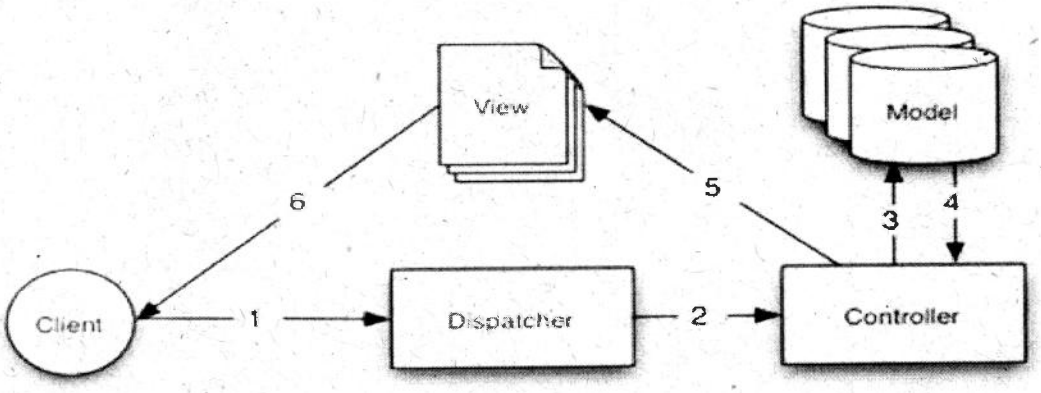
Se usan políticas de contraseñas seguras compuestas por caracteres alfanuméricos y números, minúsculas y mayúsculas, esto para hacer una cultura de cuentas de personal seguras. Estas son encriptadas en base de datos criptográficamente por el algoritmo SHA1.

Para evitar vulnerabilidades primero que nada se debe actualizar el software base ósea el sistema operativo actualizado, con un sistema de cortafuegos habilitado para filtrar el acceso indebido a este. También en las pruebas del software se realizan pruebas de seguridad a los métodos de la aplicación, evitando accesos indebidos sin autenticación, en esta etapa se encuentran posibles vulnerabilidades y se corrigen

6.1.8 Protección de la aplicación en redes Públicas

Se construye el diseño de autorización que nos permite definir: roles, permisos y privilegios de acceso a la aplicación. También proteger los accesos al software en caso de que este sea Desarrollo web a sectores prohibidos para los usuarios, para ellos se usan técnicas de protección de los métodos de la aplicación a través de un Framework.

Método de aplicación:



La figura 1 muestra un ejemplo sencillo de una petición [request] MVC. A efectos ilustrativos, supongamos que un usuario llamado Ricardo acaba de hacer clic en el enlace "¡Comprar un pastel personalizado ahora!" de la página inicial de la aplicación.

1. Ricardo hace clic en el enlace apuntando a http://www.ejemplo.com/pasteles/comprar, y su navegador hace una petición al servidor web.
2. El despachador comprueba la URL de la petición (/pasteles/comprar), y le pasa la petición al controlador adecuado.
3. El controlador realiza lógica de aplicación específica. Por ejemplo, puede comprobar si Ricardo ha iniciado sesión.
4. El controlador también utiliza modelos para acceder a los datos de la aplicación. La mayoría de las veces los modelos representan tablas de una base de datos, aunque también pueden representar entradas LDAP, canales RSS, o ficheros en el sistema. En este ejemplo, el controlador utiliza un modelo para buscar la última compra de Ricardo en la base de datos.
5. Una vez que el controlador ha hecho su magia en los datos, se los pasa a la vista. La vista toma los datos y los deja listos para su presentación al usuario. La mayoría de las veces las vistas vienen en formato HTML, pero una vista puede ser fácilmente un PDF, un documento XML, o un objeto JSON, dependiendo de tus necesidades.
6. finalmente la vista se devuelve al navegador de Ricardo.

7 Pruebas Funcionales

Las pruebas funcionales a los sistemas son fundamentales a la hora de implementar, evaluar y poner un sistema a producción. Estas pruebas se harán bajo condiciones de trabajo y carga real para el sistema, sin embargo se deben tener en cuenta las siguientes consideraciones:

a) Se realizarán las pruebas y evaluaciones de funcionamiento en los servidores de prueba del Servicio, es decir en ningún caso utilizar los servidores de bases de datos con sistemas en producción.

b) En los servidores de prueba se deben emular dos mismos controles de acceso que existen en los sistemas.

c) Nunca exponer los sistemas de prueba a la red pública.

d) Se debe realizar una copia autorizada de la base de datos de producción al sistema de pruebas.

e) Realizar pruebas de aceptación con datos de prueba en el sistema de pruebas.

f) Una vez finalizada la operación se borrarán todos los datos de prueba de la aplicación testeada. Nunca se mantendrán datos de sistemas en producción en los servidores de prueba que no estén en proceso de actualización.

g) Se realizarán respaldos completos de las bases de datos a utilizar, de los cuales uno quedará guardado como respaldo maestro y otro se utilizará para cargar la data en los servidores de prueba.

h) Se dejará constancia del respaldo efectuado por medio de una bitácora de respaldo, en la que se registrará, la base de datos respaldada, sistema al que corresponde, fecha de respaldo, quien lo realizo el respaldo y observaciones en el caso que hubiesen, tal como lo incida el anexo 1

i) Una vez finalizado el proceso de pruebas funcionales y que el sistema se encuentre en producción en forma estable y que no se requiera realizar nuevas modificaciones al sistema, los datos serán borrados de los servidores de prueba, dejándose constancia de este proceso por medio de una bitácora de pruebas en la que se registraran a lo menos los siguientes datos: Pruebas realizadas, nombre del servidor de prueba, sistema al que corresponde, base de datos de prueba, fecha de borrado de datos, quien realizó la eliminación de la data y observaciones en el caso que hubiesen, según lo indica el anexo 2

8 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.

9 Mantenimiento de Sistemas

9.1 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.

10 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 al 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.

11 Habilitación de Logs

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.

Mediante el uso de una bitácora se dejará constancia de la revisión periódica de los eventos registrados en los archivos Logs, tal como lo indica el anexo 3

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.

12 Validación de Datos de Entrada

Los datos de entrada a las aplicaciones son válidos 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:

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

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.

Procedimiento para responder errores de validación.

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

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

Se implementan gestores de bases de datos relacionales que cumplan con el acrónimo A.C.I.D que significa Atomicidad, Consistencia, Aislamiento y Durabilidad de los datos.

A.C.I.D se describe en la norma ISO/IEC 10026-1 de 1992 sección 4 donde esta debe asegurar la atomicidad de los datos, esto quiere decir que las transacciones ocurren por completo o nada.

Los siguientes gestores de bases de datos cumplen con esta norma, estos son:

- Microsoft SQL SERVER
- MySQL
- PostgreSQL

13 Validación de Datos de Salida

La salida de datos de una aplicación se válida 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 la unidad involucrada definir sus métodos de entrega de información con los roles de usuarios que les compete en cada sistema

14 Controles Criptográficos

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

Todos los sistemas deben tener aplicada criptografía en las contraseñas.

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.

En las aplicaciones Web se implementan certificados TLS/SSL donde los datos ingresados en formularios de usuarios viajan por un canal encriptado entre el navegador Web y el Servidor, logrando la privacidad y seguridad de los datos. Se puede apreciar al conectar con una aplicación web el protocolo HTTPS.

15 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 "SUBVERSIÓN" 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.

16 Procedimiento de Actualización de Software en Producción

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, como lo indica el anexo 2

E. Se deben incluir pruebas sobre la utilidad, seguridad, efectos sobre otros sistemas y accesos de usuarios.

F. La versión en ejecución del sistema en producción a modifica debe ser respaldada junto con la data y rotulada de 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:
   a. Estar respaldada inicialmente con un contrato de mantenimiento con el proveedor.

b. Validar igualmente en los servidores de prueba del Servicio su funcionamiento antes de la prueba en producción de la modificación.
c. Los procesos de prueba en ningún caso serán mediante permisos de acceso en forma remota para el proveedor.
d. 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 e Informática.
e. Se identificarán 2 grandes grupos de software y de acuerdo a esto de determinarán los pasos de actualización:

1. 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.

2. Software interno: Es aquel desarrollado por el Gobierno Regional Metropolitano o para una cierta función específica adaptada a los procesos internos de este.

17 Actualización de 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 preparara 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 softwares 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 softwares base y en los software interno realizando pruebas de ingreso, consultas, emisión de reportes o auditorias 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 realiza pruebas de compatibilidad.

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

18 Actualización de 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 softwares base y en los software interno realizando pruebas de ingreso, consultas emisión de reportes o auditorias 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.

19 REGISTRO DE CONTROL

La Unidad de Desarrollo deberá emitir un informe que dé cuenta de los siguientes controles:

- A.09.04.05 Informe sistemas de protección de código fuente
- A.12.01.02 Informe de registro de cambios y pruebas de cambio
- A.12.01.04 Informe de Separación de los ambientes de desarrollo, prueba y operacionales
- A.14.01.01 Informe de identificación y administración de requisitos de seguridad en los procesos de los proyectos de sistemas de información.
- A.14.01.02 Informe de sistemas de protección para redes publicas
- A.14.01.03 Informe de protección de transacciones en los sistemas de aplicación
- A.14.02.01 Informe de técnicas de programación segura
- A.14.02.02 Informe de sistemas de control de cambios.
- A.14.02.03 Informe de revisión y prueba a las plataformas de operación con cambios.
- A.14.02.04 Informe de cambios en paquetes de software
- A.14.02.05 Informe de sistemas de seguridad en los niveles de la arquitectura de desarrollo
- A.14.02.06 Informe de la seguridad en los entornos de desarrollo
- A.14.02.07 Informe de monitoreo y supervisión de desarrollo externalizado
- A.14.02.08 Informe de pruebas de seguridad durante el desarrollo
- A.14.02.09 Informe de aceptación de pruebas de desarrollo
- A.14.03.01 Informe de control de acceso al entorno de Desarrollo

El informe deberá ser enviado al Encargado de Seguridad de manera semestral.

Todo documento deberá venir formalizado por quienes sean responsables del proceso (Debe contener logo del Servicio, fecha de creación, nombre, cargo y firma del responsable)

20 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

21 REVISIÓN

La siguiente Política será revisada, evaluada y/o actualizada según corresponda una vez al año por el Comité de Seguridad de la Información, en cuanto a su funcionamiento y correcta aplicación en la Institución.

22 ANEXOS

Anexo 1

Bitácora de Respaldo de Datos

Base de datos respaldada	Sistema al que corresponde	Fecha del respaldo	encargado	observaciones

Anexo 2

stgo

Bitácora de pruebas

Pruebas realizadas	Servidor de Pruebas	Sistema	Base de Datos de Prueba	Fecha de borrado de Datos	encargado	Observaciones

Anexo 3

stgo

Registro de Logs

Registro de LOGS						
Aplicacion	usuario	errores de conexión	horas de conexión	intentos fallidos	Fecha y hora	terminal desde donde se conecta
OBSERVACIONES						

23 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Héctor Salinas Murúa. Encargado de unidad de Desarrollo	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Carlos Hernández A.** Analista Departamento de Informática **Carolina Hidalgo M.** Jefa Departamento de Gestión Institucional	**Mayuri Reyes Torres** Presidente Comité de Seguridad

24 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Héctor Salinas	todas	12-07-17	Creación documentos
02	Mauricio Marín	todas	19-10-17	Se cambia formato y se actualiza documento. Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI • Se incorpora registro de control

Acta de Reunión
Comité de Seguridad de la Información

Asistentes:

- Sra. Mayuri Reyes Torres - Jefa División de Administración y Finanzas
- Srta. Carolina Hidalgo Mandujano – Jefa Departamento de Gestión Institucional
- Sra. Valentina Guerra Monsalve - Jefa Departamento Jurídico
- Sra. María Macarena Miranda Nuñez - Jefa Departamento de Gestión Documental
- Sr. José Ignacio Gutiérrez - Encargado de Seguridad de la información
- Sr. Hector Salinas Murúa – Jefe (s) Departamento de Informática
- Sr. Carlos Hernández Arancibia – Analista Departamento de Informática
- Sr. Mauricio Marín Vera – Analista Departamento de Informática
- Srta. Paulina Vilches Vásquez– Encargada Unidad de Transparencia
- Sr. Juan Catalán Farías – Depto. Servicios Generales
- Sr. Ariel Lagos Vásquez – Prevencionista de Riesgos

Tabla:

1. Se ratifica al Jefe del Departamento de Informática como Encargado de Seguridad de la Información.

2. Se acuerda incorporación a este Comité de los siguientes funcionarios:
   a. Jefe Departamento de Servicios Generales
   b. Jefe Departamento de Gestión de Personas
   c. Prevencionista de Riesgos Institucional

3. Se revisa y evalúa la correcta ejecución de los contratos de mantenimiento del Gobierno Regional Metropolitano (GORE RM).

4. Se revisan y validan por parte de este Comité los siguientes documentos:

   - Política General de Seguridad de la Información
   - Resolución Encargado de Seguridad de la Información
   - Resolución de nombramiento Comité de Seguridad de la Información
   - Instructivo Correctivo Preventivo
   - Manual de Gestión de Archivos
   - Norma de Acceso a la Red
   - Norma de Eliminación de Activos
   - Norma de Seguridad de la Información para la Gestión de Proyectos
   - Norma de Uso Outsourcing
   - Norma de Trabajo Remoto
   - Norma de Uso Instalación Legal de Software
   - Norma de Uso Identificación y Autentificación

- Norma de Uso Navegación por Internet
- Norma de Uso para los Equipos Tecnológicos Portátiles
- Norma de Reutilización y Devolución de Activos
- Plan de Emergencia Institucional
- Política de Clasificación de Activos
- Política de Acceso físico
- Política de Correo Electrónico
- Política de Desarrollos de Sistemas
- Política de Dispositivos Móviles
- Política de Escritorios y Pantallas Limpias
- Política de Gestión de Incidentes de Seguridad
- Política de Gestión de la capacidad
- Política de la Seguridad Informática
- Política de Respaldo de la Información
- Política Gestión de Claves
- Política Manejo de Activos
- Política para la Privacidad y Protección de la Información e Identificación Personal
- Política sobre el Uso de Controles Criptográficos
- Política y Proceso de Selección de Personal
- Procedimiento de Control de las Vulnerabilidades Técnicas
- Protocolo de Control y Tratamiento de SSI
- Reglamento sobre Infracciones al SSI

5. Se toma conocimiento y valida el informe "Procesamiento y Confidencialidad de los Activos de Información", elaborado por el Encargado del Seguridad de la Información, el cual da cuenta de la no ocurrencia de incidentes de seguridad durante el período 2017.

6. Se informa por parte del Encargado de Seguridad de la Información respecto de la participación en distintas instancias en materias relativas al Sistema de Seguridad de la Información:

   - Exposición para el Sector Público de Expertos en materia de Seguridad informática (Subsecretaría del Interior)
   - Reunión bipartita GORE RM-Red de Expertos
   - Jornada de Capacitación Indicador SSI (Ministerio Secretaría General de la Presidencia)

7. Se dan a conocer por parte del Encargado de Seguridad de la información las medidas de difusión del Sistema de Seguridad de la Información a través de:

   - Correo electrónico a todo el personal.
   - Banner corporativo en Intranet Institucional.

8. Se acuerda que el Comité de Seguridad tenga una próxima sesión durante el primer semestre del próximo año para evaluar lo reportado durante 2017 y revisar los compromisos 2018.

Aprueban:

Sra. Mayuri Reyes Torres
Jefa División de Administración y Finanzas

Srta. Carolina Hidalgo Mandujano
Jefa Departamento de Gestión Institucional

Sra. Valentina Guerra Monsalve
Jefa Departamento Jurídico

Sra. María Macarena Miranda Nuñez
Jefa Departamento de Gestión Documental

Sr. Hector Salinas Murúa
Jefe (s) Departamento de Informática

Srta. Paulina Vilches Vásquez
Encargada Unidad de Transparencia

Sr. José Ignacio Gutiérrez García
Encargado de Seguridad de la Información