Política de Desarrollo de Sistemas

1. INDICE

1. INDICE 2
2. OBJETIVO 4
3. ALCANCE 4
4. ROLES Y RESPONSABILIDADES 4
5. CONTROL NORMATIVO SSI 5
6. DEFINICIONES 7
6.1 PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS 7
6.1.1 Desarrollo interno de sistemas 7
6.1.2 Desarrollo por terceros 7
6.1.3 Procedimientos de Desarrollo Seguro 7
6.1.4 Principios de Ingeniería de Sistema Seguro 8
6.1.5 Separación de ambientes de Desarrollo 9
6.1.6 Pruebas de Seguridad en el Sistema 10
6.1.7 Entorno de Desarrollo seguro 10
6.1.8 Protección de la aplicación en redes Públicas 11
6.2 Definiciones sobre criptografía 12
6.3 Pruebas Funcionales 13
6.4 Implementación 14
6.5 Mantenimiento de Sistemas 14
6.6 Consideraciones Generales 15
6.7 Habilitación de Logs 15
6.8 Validación de datos 15
6.8.1 Validación de Datos de Entrada 16
6.8.2 Validación de Datos de Salida 17
6.9 Controles Criptográficos 17

6.10 Requisitos de protección de claves criptográficas 18
6.11 Requisitos de protección de otro material criptográfico 21
6.12 Métodos de protección de seguridad 21
6.13 Seguridad de los Archivos del Sistema 22
6.14 Procedimiento de Actualización de Software en Producción 22
6.15 Actualización de Software Base 23
6.16 Actualización de Software Interno 24
6.17 Procedimientos de gestión de las claves y contraseñas 25
6.18 Mecanismos de manejo de sesión 25
6.19 Estándares de implantación de tecnología criptográfica 26
6.20 Regulación de controles Criptográficos 27
7. Librerías y Frameworks 28
8. Licencias 28
9. ANEXOS 29
9.1 Anexo 1 29
9.2 Anexo 2 30
9.3 Anexo 3 31
9.4 Anexo 4 32
10. DIFUSIÓN 33
11. PERIODICIDAD DE EVALUACION Y REVISIÓN 33
12. FORMALIZACION EXTERNA 33
13. REGISTRO DE REVISION Y ACTUALIZACION HISTORICO. 34
14. FORMALIZACIÓN INTERNA 36

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.

El responsable para la gestión de claves, incluyendo la generación de claves y la operación de la infraestructura criptográfica es el Departamento de Informática. Éste puede delegar en otras unidades internas o externas, incluso en empresas, los aspectos de gestión de claves que estén justificados.

Todo funcionario del Servicio tiene estrictamente prohibido el uso de criptografía, a menos que haya sido autorizado por el Encargado de Seguridad

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.10.01.01	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
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 aplicaciones después de los cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se 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
A.18.01.05	Regulación de los controles criptográficos	Se deben utilizar controles criptográficos se debieran utilizar en que cumplan con todos los acuerdos, leyes y regulaciones pertinentes.

6. DEFINICIONES

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

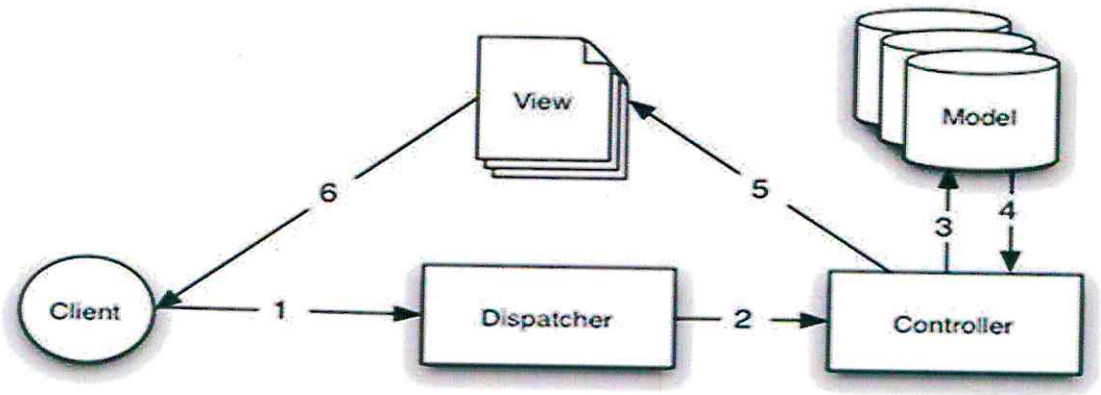
Se usan políticas de contraseñas seguras compuestas por caracteres alfanuméricos y números, minúsculas y mayúsculas, símbolos y al menos de 8 caracteres de largo. Esto para hacer una cultura de cuentas de personal seguras. Estas son encriptadas en base de datos criptográficamente por el algoritmo SHA1.

Para evitar vulnerabilidades primero que nada se debe actualizar el software base es decir 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.

6.2 Definiciones sobre criptografía

Los algoritmos criptográficos aprobados para el uso por el Gobierno Regional Metropolitano son los siguientes.

Algoritmos de resumen aprobados

- SHA-1,1 definido en la norma internacional ISO/IEC 10118-3 (2004): «Information technology -Security techniques - Hash functions - Part 3: Dedicated hash functions» y en la norma FIPS 180-2 (2002): «Secure Hash Standard».
- SHA-1 es el algoritmo más usado actualmente.
- SHA-384,4 definido en la norma FIPS 180-2 (2002): «Secure Hash Standard».
- SHA-512,5 definido en la norma FIPS 180-2 (2002): «Secure Hash Standard».

Algoritmos simétricos aprobados

- AES,6 definido en la norma FIPS 197 (2001): «Specification for the Advanced Encryption Standard (AES)».
- TDEA7 (por ejemplo, Triple DES), definido en la especificación NIST SP 800-67 (2004, revisado en 2008): «Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher», con la recomendación de emplear tres claves diferentes. Se recomienda utilizar los modos criptográficos de operación definidos en la especificación NIST SP 800-38A (2001): «Recommendation for Block Cipher Modes of Operation - Methods and Techniques».

Algoritmos asimétricos aprobados

- RSA,8 definido en la especificación técnica IETF RFC 3447 (2003): «Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1».
- DSA,9 definido en la norma internacional ISO/IEC 14888-3 (2006): «Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms» y en la norma FIPS 186-2 (2000): «Digital Signature Standard».
- EC-DSA,10 en sus dos variantes E(Fp) y E(F2m), definido en la norma internacional ISO/IEC 14888-3 (2006): «Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms».
- EC-GDSA, en sus dos variantes E(Fp) y E(F2m), definido en la norma internacional ISO/IEC 15946-2 (2002): «Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures».
- Algoritmos de establecimiento de claves aprobados

- Algoritmos DLC, definidos en la especificación NIST SP 800-56A (2007): «Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography».
- Algoritmo de transporte de claves RSA.

Algoritmos de envoltura de claves con clave simétrica

6.3 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

6.4 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.

6.5 Mantenimiento de Sistemas

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.

6.6 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.

6.7 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.

6.8 Validación de datos

Validación semántica, validación sintáctica, caja negra, deben ser hecho por el lado del servidor, nunca del lado del cliente
La validación de datos deberá utilizar librerías apropiadas, como por ejemplo HTML, Purifier Bleach u otras.
Esta validación no convierte a los datos inmediatamente en datos seguros, por lo que se debe utilizar en conjunto con otros elementos de defensa, escapado de datos, que es una técnica en la que se añade un carácter especial antes del dato a escapar

6.8.1 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

6.8.2 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

6.9 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.

6.10 Requisitos de protección de claves criptográficas

Las claves criptográficas deben estar disponibles operativamente tanto tiempo como lo requiera el servicio criptográfico correspondiente. Las claves pueden mantenerse en un equipamiento criptográfico mientras se utilizan, o pueden almacenarse de manera externa —con las medidas de seguridad adecuadas— y recuperarlas cuando sea necesario. Además, algunas de las claves se archivarán durante un plazo superior al inicialmente previsto para el uso del emisor.

La tabla siguiente indica, para cada tipo de clave, los requisitos de protección correspondientes.

Tipo de clave	Servicio de seguridad	Protección de seguridad	Datos asociados a proteger	Garantía requerida	Período de protección
Clave privada de firma	Autenticación Integridad Irrefutabilidad	Integridad Confidencialidad	Uso o aplicación Parámetros de dominio Clave pública de firma	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica
Clave pública de firma	Autenticación Integridad Irrefutabilidad	Archivo Integridad	Uso o aplicación Propietario del par de claves Parámetros de dominio Clave privada de firma Datos firmados	Validez	Desde su generación hasta que no sea necesario verificar los datos protegidos
Clave simétrica de autenticación	Autenticación Integridad	Archivo Integridad Confidencialidad	Uso o aplicación Otras entidades autorizadas Datos autenticados	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica
Clave privada de autenticación	Autenticación Integridad	Integridad Confidencialidad	Uso o aplicación Clave pública de autenticación Parámetros de dominio	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica
Clave pública de autenticación	Autenticación Integridad	Archivo Integridad	Uso o aplicación Propietario del par de claves Datos autenticados Clave privada de autenticación Parámetros de dominio	Validez	Desde su generación hasta que no sea necesario autenticar los datos protegidos

Clave simétrica de cifrado de datos	Confidencialidad	Archivo Integridad Confidencialidad	Uso o aplicación Otras entidades autorizadas Datos cifrados Datos en claro	No aplica	Desde su generación hasta la finalización de la vida de los datos o la finalización del período de validez criptográfica
Clave simétrica de envoltura de claves	Soporte	Archivo Integridad Confidencialidad	Uso o aplicación Otras entidades autorizadas Claves cifradas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que las claves envueltas no necesiten protección, el más largo de los dos períodos
Clave (simétrica y asimétrica) de generación de números aleatorios	Soporte	Integridad Confidencialidad	Uso o aplicación	Posesión de la clave privada, cuando se utiliza	Desde su generación hasta su reposición
Clave maestra simétrica	Soporte	Archivo Integridad Confidencialidad	Uso o aplicación Otras entidades autorizadas Claves derivadas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica o de las claves derivadas, el más largo de los dos períodos
Clave privada de transporte de clave	Confidencialidad Integridad	Archivo Integridad Confidencialidad	Uso o aplicación Claves cifradas Parámetros de dominio Clave pública de transporte de claves	Posesión	Desde su generación hasta la finalización del período de protección de todas las claves transportadas
Clave pública de transporte de clave	Confidencialidad Integridad	Archivo Integridad	Uso o aplicación Propietario del par de claves	Validez	Desde su generación hasta la finalización del período de su validez criptográfica
Clave simétrica de negociación de clave	Soporte	Archivo Integridad Confidencialidad	Uso o aplicación Otras entidades autorizadas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que no sea necesaria en relación con una clave determinada, el más largo de los dos períodos
Clave privada estática de negociación de clave	Soporte	Archivo Integridad Confidencialidad	Uso o aplicación Parámetros de dominio	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que

			Clave pública de negociación de clave estática		no sea necesaria en relación con una clave determinada, el más largo de los dos períodos
Clave pública estática de negociación de clave	Soporte	Archivo Integridad	Uso o aplicación Propietario del par de claves Parámetros de dominio Clave privada de negociación de clave estática	Validez	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que no sea necesaria en relación con una clave determinada, el más largo de los dos períodos
Clave privada efímera de negociación de clave	Soporte	Integridad Confidencialidad	Uso o aplicación Parámetros de dominio Clave pública de negociación de clave efímera	No aplica	Desde su generación hasta la finalización del proceso de negociación de claves, con destrucción inmediata
Clave pública efímera de negociación de clave	Soporte	Integridad	Uso o aplicación Propietario del par de claves Parámetros de dominio Clave privada de negociación de clave efímera	Validez	Desde su generación hasta la finalización del proceso de negociación de claves, con destrucción inmediata
Clave simétrica de autorización	Autorización	Integridad Confidencialidad	Uso o aplicación Otras entidades autorizadas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica
Clave privada de autorización	Autorización	Integridad Confidencialidad	Uso o aplicación Parámetros de dominio Clave pública de autorización	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica
Clave pública de autorización	Autorización	Integridad	Uso o aplicación Propietario del par de claves Parámetros de dominio Clave privada de autorización	Validez	Desde su generación hasta la finalización del período de su validez criptográfica

6.11 Requisitos de protección de otro material criptográfico

Tipo de material	Servicio de seguridad	Protección de seguridad	Datos asociados a proteger	Período de protección
Parámetros de dominio	Depende de la clave asociada a los parámetros de dominio	Autenticación Integridad	Uso o aplicación Claves privadas y públicas	Desde su generación hasta que no sean necesarios para generar claves o verificar firmas
Vectores de inicialización	Depende del algoritmo	No repudio Integridad	Datos protegidos	Desde su generación hasta que no sean necesarios para procesar datos protegidos
Secretos compartidos	Soporte	Confidencialidad Integridad	No aplica	Desde su generación hasta la finalización de la transacción Serán destruidos al finalizar el período de protección
Generadores de números aleatorios	Soporte	Confidencialidad Integridad	Uso o aplicación	Se utilizan una vez y se destruyen
Otra información pública	Soporte	Autenticación Integridad	Uso o aplicación Otras entidades autorizadas Datos procesados en relación con valores únicos de mensaje	Desde su generación hasta que no sean necesarios para procesar datos que dependen de ellos
Resultados intermedios	Soporte	Confidencialidad Integridad	Uso o aplicación	Desde su generación hasta que no sean necesarios, momento en el que tienen que destruirse

6.12 Métodos de protección de seguridad

Las dos tablas anteriores determinan diversas protecciones de seguridad con relación a las claves criptográficas y otros materiales:

- Integridad
- Confidencialidad
- No repudio
- Autenticación

A continuación se determinan los métodos aceptables para conseguir las protecciones de integridad y de confidencialidad, tanto cuando la información criptográfica está en tránsito como cuando está en su lugar de operación.

6.13 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.

6.14 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.

6.15 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.

6.16 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.

6.17 Procedimientos de gestión de las claves y contraseñas

Se establecerán los siguientes procedimientos en relación con los siguientes aspectos:

- Generación de claves para diferentes sistemas criptográficos y aplicaciones.
- Generación y obtención de certificados de clave pública.
- Distribución de claves a los usuarios, incluyendo la activación una vez hayan sido recibidas.
- Almacenamiento de claves, incluyendo cómo obtienen acceso a las claves los usuarios autorizados.
- Cambio o actualización de claves, incluyendo normas sobre cuándo deben cambiarse o actualizarse, y cuál es el procedimiento aplicable.
- Gestión de claves comprometidas.
- Revocación de claves, incluyendo su retirada o desactivación.
- Archivo de claves, especialmente en caso de información cifrada que haya sido archivada.
- Destrucción de claves.
- Registro y auditoría de operaciones relativas a la gestión de claves.
- Deberá considerarse claves o contraseñas de al menos 8 caracteres con una combinación de números , letras, símbolos y el uso de mayúsculas y minúsculas

En caso de que haya terceros prestadores de servicios relacionados con la criptografía, se establecerán acuerdos de nivel de servicio que consideren de manera específica las cuestiones de responsabilidad, la fiabilidad de los servicios y los tiempos de respuesta garantizados.

6.18 Mecanismos de manejo de sesión

Para el manejo de las sesiones la Unidad de Desarrollo del Gobierno Regional Metropolitano, ha considerado lo siguiente:

- El identificador ha de ser único, aleatorio y de un largo suficiente.

- Se rotarán los identificadores de sesión durante la autenticación o re-autenticación.
- Se implementa un Time Out que fuerce el reingreso se autenticación del usuario cuando este se ausente por un tiempo prolongado o que el sistema no registre movimientos.

6.19 Estándares de implantación de tecnología criptográfica

Debe definirse e implantarse una infraestructura común y adecuada de tecnología criptográfica que preste servicios criptográficos identificados en esta política a las diferentes aplicaciones del Gobierno Regional Metropolitano.

- Hardware criptográfico dedicado

ISO 15408 (2005): «Information technology - Security techniques - Evaluation criteria for IT security», nivel EAL 4 o superior, de acuerdo con un objetivo de evaluación o perfil de protección adecuado al análisis de riesgo llevado a cabo.

- En concreto, se consideran adecuados los siguientes perfiles de protección:
    - CEN CWA 14167-2 (2004): «Cryptographic module for CSP signing operations with backup Protection profile - CMCSOB PP», en relación con las operaciones de firma de certificados y otros documentos, con copia de seguridad.
    - CEN CWA 14167-3 (2004): «Cryptographic module for CSP key generation services - Protection profile - CMCKG-PP», en relación con las operaciones de generación de claves.
    - CEN CWA 14167-4 (2003): «Cryptographic module for CSP signing operations – Protection profile - CMCSO PP», en relación con las operaciones de firma de certificados y otros documentos.
    - FIPS 140-2, nivel 3 o superior.

- Tarjetas y otros dispositivos criptográficos móviles, y software criptográfico
    - FIPS 140-2, nivel 3 o superior.
        - ISO 15408 (2005): «Information technology - Security techniques - Evaluation criteria for IT security», nivel EAL 4 o superior, de acuerdo con un objetivo de evaluación o perfil de protección adecuado al análisis de riesgo llevado a cabo.
        - En concreto, se consideran adecuados los perfiles de protección:

- CEN CWA 14169 (2004): «Secure signature-creation devices "EAL 4+", en relación con los dispositivos de firma electrónica.
- CEN CWA 14365-2 (2004): «Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices», en relación con el software de firma electrónica. En la definición de la infraestructura deben incluirse los siguientes aspectos:
- Identificación detallada de aplicaciones y servicios específicos que necesitan servicios criptográficos.
- Identificación del catálogo de requisitos criptográficos, que debe garantizar el cumplimiento de esta política. Debe considerarse de manera particular lo siguiente.
- El volumen de operaciones y la topología de red interna, a efectos del cálculo del número de equipos criptográficos necesarios.
- El análisis del cifrado para la protección de informaciones sensibles en tránsito o que estén fuera de las instalaciones de la UOC (transportadas mediante dispositivos móviles, con medios o dispositivos que pueden extraerse o por líneas de comunicación).
- El análisis del impacto del uso de la criptografía sobre los controles basados en la inspección de contenidos, como por ejemplo los programas antivirus.
- Desarrollo de una especificación de gestión de claves, que debe describir los componentes de gestión de claves requeridos para operar los dispositivos y las aplicaciones criptográficas durante su ciclo de vida. Su contenido debe considerar lo siguiente.
- La aplicación criptográfica para los dispositivos criptográficos
- El entorno de comunicaciones de los dispositivos criptográficos
- Los requisitos de los componentes de gestión de claves de los dispositivos criptográficos
- La distribución de los componentes de gestión de claves de los dispositivos criptográficos
- El control de acceso a los dispositivos criptográficos
- El registro de actividades relativas a la gestión de claves de los dispositivos criptográficos
- La gestión de compromisos y recuperación de los dispositivos criptográficos
- La recuperación de claves

6.20 Regulación de controles Criptográficos

Los servicios criptográficos tienen que emplearse de acuerdo con la legislación vigente en cada momento y deben ser considerados para el cumplimiento de los acuerdos pertinentes, leyes y regulaciones nacionales como internacionales, además de:

a) las restricciones a la importación o exportación de hardware y software para realizar funciones criptográficas;
b) las restricciones a la importación o exportación de hardware y software que está diseñado para tener funciones criptográficas añadidas;
c) las restricciones sobre el uso de encriptación;
d) los métodos de acceso de cumplimiento obligatorio o facultativo por las autoridades de los países a la información encriptada por hardware o software, para proveer la confidencialidad del contenido.
Se debe buscar asesoramiento jurídico para asegurar el cumplimiento de leyes y reglamentos pertinentes. De igual forma, se debe tomar asesoramiento jurídico previo a que la información encriptada o controles criptográficos sean movidos a través de las fronteras jurisdiccionales.

7. Librerías y Frameworks

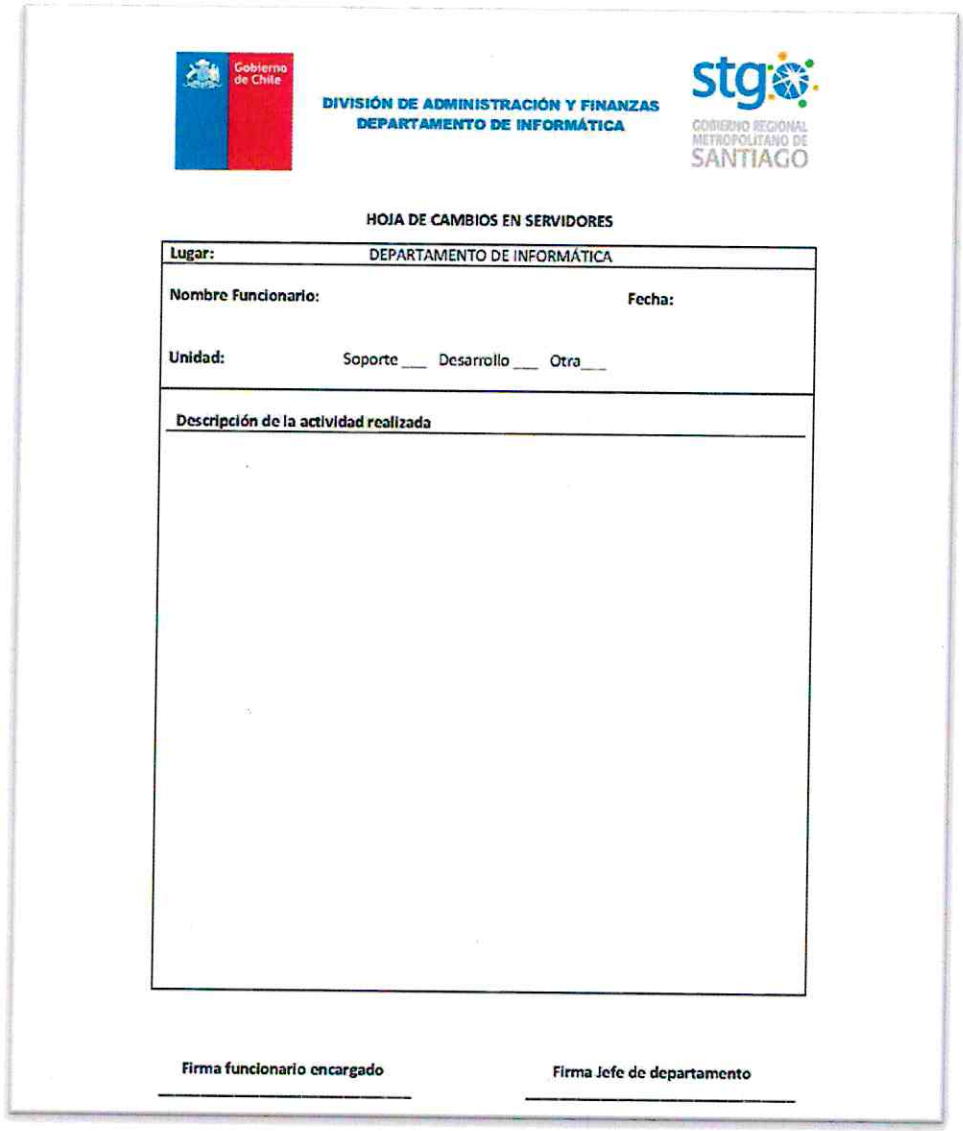
Se debe hacer un inventario y catalogar las librerías y Frameworks para mantenerlos actualizados y prevenir vulnerabilidades

8. Licencias

Todo desarrollo dentro del Estado debe estar licenciado y en este caso el Gobierno Regional Metropolitano.

9. ANEXOS

9.1 Anexo 1



Gobierno de Chile

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

HOJA DE CAMBIOS EN SERVIDORES

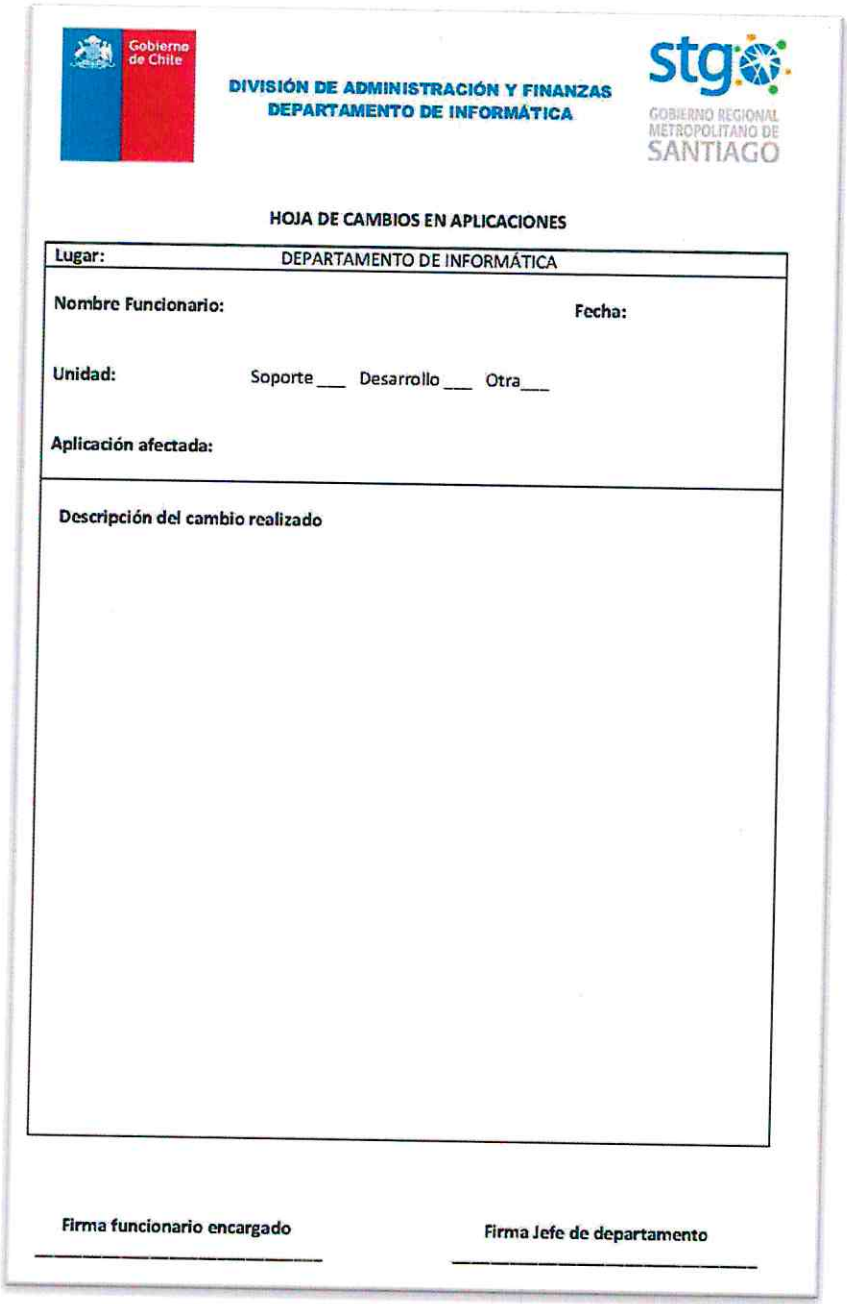
Lugar:	DEPARTAMENTO DE INFORMÁTICA
Nombre Funcionario:	**Fecha:**
Unidad:	Soporte ___ Desarrollo ___ Otra___

Descripción de la actividad realizada

Firma funcionario encargado _____

Firma Jefe de departamento _____

9.2 Anexo 2



Gobierno de Chile

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

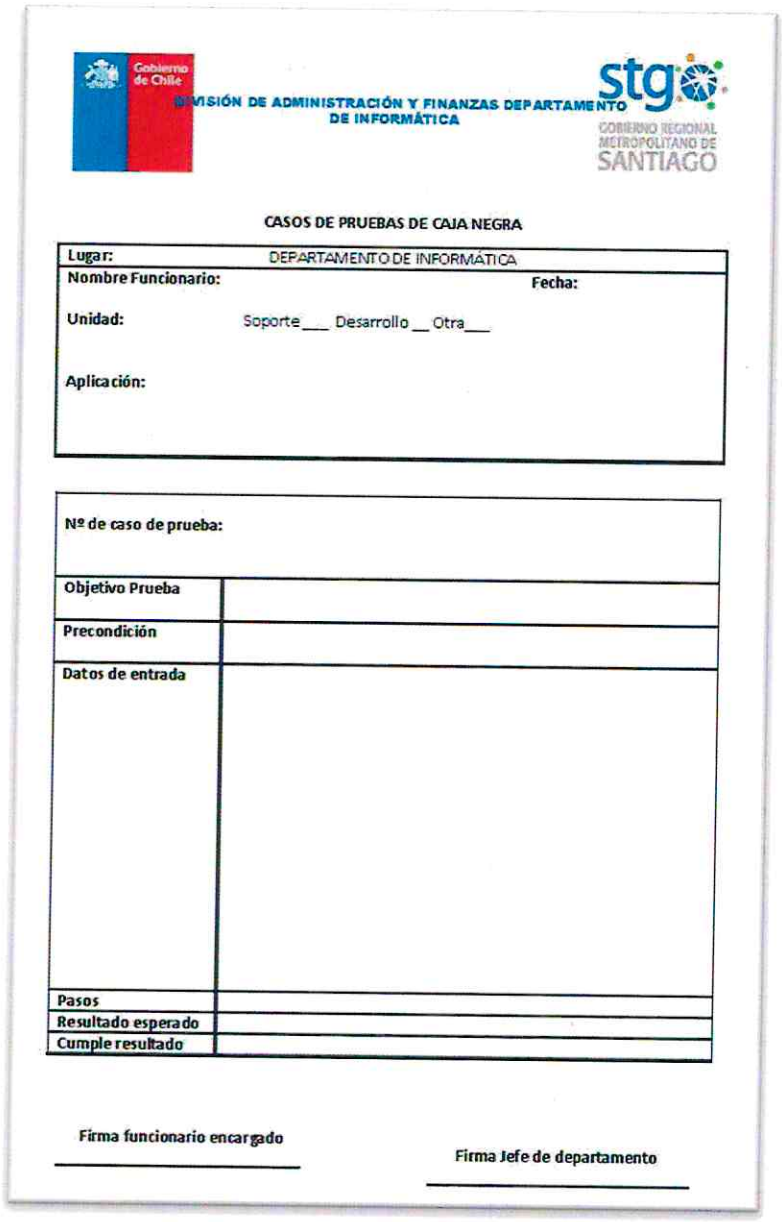
HOJA DE CAMBIOS EN APLICACIONES

Lugar:	DEPARTAMENTO DE INFORMÁTICA
Nombre Funcionario:	**Fecha:**
Unidad:	Soporte ___ Desarrollo ___ Otra___
Aplicación afectada:	
Descripción del cambio realizado	

Firma funcionario encargado _____

Firma Jefe de departamento _____

9.3 Anexo 3



DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS DEPARTAMENTO DE INFORMÁTICA

CASOS DE PRUEBAS DE CAJA NEGRA

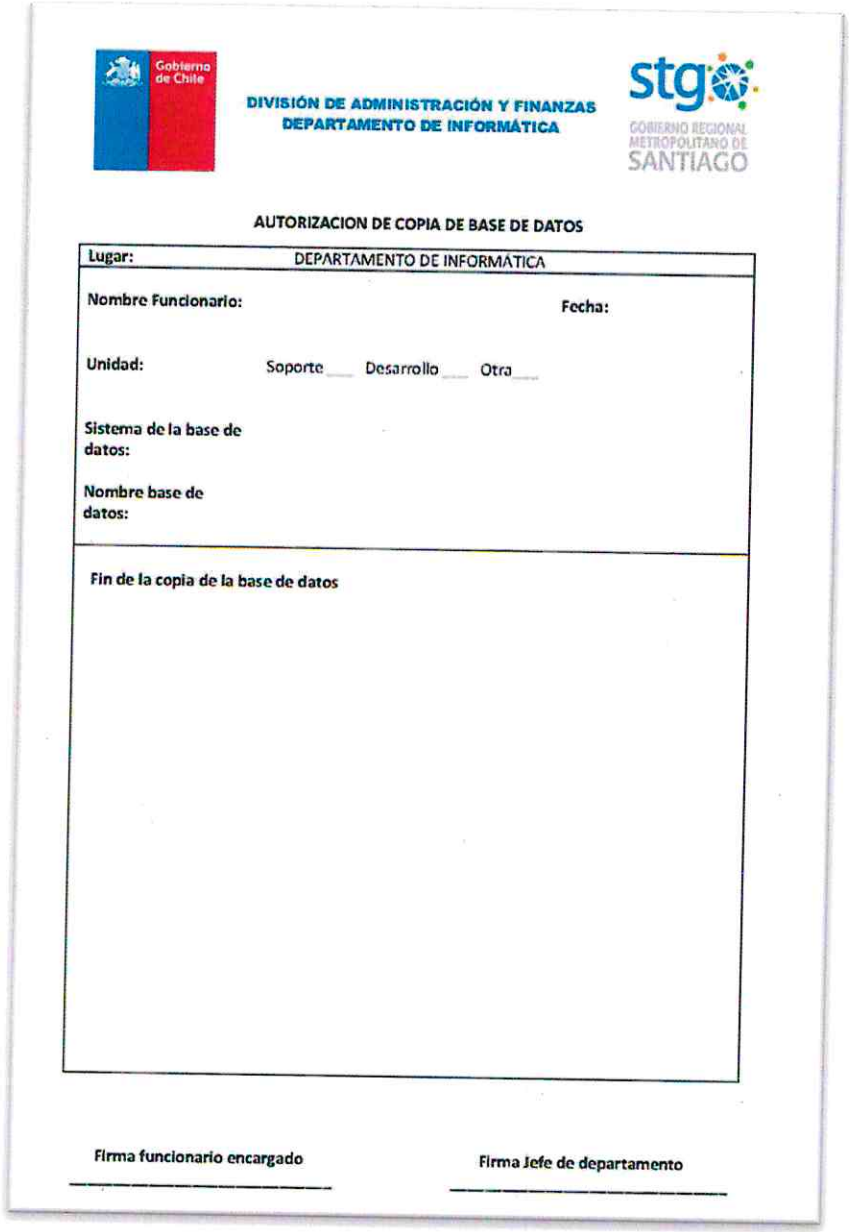
Lugar:	DEPARTAMENTO DE INFORMÁTICA
Nombre Funcionario:	**Fecha:**
Unidad:	Soporte___ Desarrollo __ Otra___
Aplicación:	

Nº de caso de prueba:	
Objetivo Prueba	
Precondición	
Datos de entrada	
Pasos	
Resultado esperado	
Cumple resultado	

Firma funcionario encargado

Firma Jefe de departamento

9.4 Anexo 4



Gobierno de Chile

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

stg GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

AUTORIZACION DE COPIA DE BASE DE DATOS

Lugar:	DEPARTAMENTO DE INFORMÁTICA
Nombre Funcionario:	**Fecha:**
Unidad:	Soporte___ Desarrollo___ Otra___
Sistema de la base de datos:	
Nombre base de datos:	

Fin de la copia de la base de datos

Firma funcionario encargado _____

Firma Jefe de departamento _____

10.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.

11.PERIODICIDAD DE EVALUACION Y REVISIÓN

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

12.FORMALIZACION EXTERNA

Mediante el acta fecha 12 de julio año 2019, se aprueba por parte del Comité de Seguridad de la Información, la Política de Desarrollo de Sistemas

13.REGISTRO DE REVISION Y ACTUALIZACION HISTORICO.

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
03	Mauricio Marin V.	19	2/08/2018	Se agrega en Registro de Control el siguiente párrafo: En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo.
04	Mauricio Marín V.	21, 22, 23, 24	2/8/2018	Se agregan nuevos anexos Se cambia título 6 " Desarrollo de la Política por " Definiciones" Se cambia título de "Registro de Control" por "Registro de Operaciones" Se cambia título de "Revisiones" por "Periodicidad de evaluación y revisiones"
05	Mauricio Marin	todas	29-01-19	Se fusiona esta política con la Política sobre el uso de controles criptográficos
06	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.

07	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Política de desarrollo de sistemas año 2019.

14.FORMALIZACIÓN INTERNA

Elaborado por	Revisado por	Aprobado por
Ricardo Cortes F. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Carlos Hernández A.** Analista Departamento de Informática **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Alejandro Segura B.** Presidente Comité de Seguridad