GOBIERNO REGIONAL DE LOS LAGOS

Acción de Futuro

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO "ASEGURAMIENTO DE SERVICIOS DE APLICACIÓN EN REDES PÚBLICAS"

CÓDIGO	**SSI-A.14.01.02**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	26-11-2019	
RESPONSABLE	Encargado de Sistemas de Seguridad de la Información.			

Historial de modificaciones

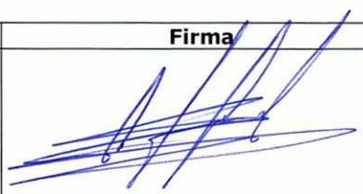
Creación/Modificaciones del Documento

Versión	Fecha de modificación	Autor	Motivo	Páginas modificadas	Firma
1.0	24-09-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	Creación de la primera versión del procedimiento	Todas	

Revisiones

Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	26-09-2019	Eduardo Madrid Osorio, Encargado Unidad de Informática	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	05-11-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	
1.0	05-11-2019	Alejandro Montaña Ampuero, Administrador Regional del Gobierno Regional de Los Lagos	

Distribuciones

Versión	Fecha	Encargado	Observaciones
1.0	06-12-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	Enviado por correo electrónico e instruida la publicación en intranet a la Unidad de Informática

Contenido

1. Objetivo

Proteger la información involucrada en los servicios de aplicación que pasan a través de redes públicas contra la actividad fraudulenta, la disputa de contratos y la información y modificación no autorizada.

2. Alcance o ámbito de aplicación interno

El presente procedimiento, establecerá la forma de garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas.
Este procedimiento es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros, es decir, proveedores, que presten servicios al Gobierno Regional de Los Lagos.

3. Roles y Responsabilidades.

ROLES	RESPONSABILIDADES
Encargado de Seguridad de la Información	• Es responsable de la elaboración de la presente política, de su actualización y velar por el cumplimiento de sus disposiciones. • Supervisar la implementación de la presente política. • Además, para efectos de la presente política, deberá definir la lista de sistemas de información clasificados como "críticos" para el Servicio y sus programas. • Los sistemas clasificados como críticos, pueden ser de desarrollo o empaquetados.
Encargado de la Unidad de Informática	• Es responsable de coordinar la creación de los procedimientos e instructivos correspondientes y de que se cumplan los respectivos requisitos de esta política. • Hacer cumplir con las disposiciones de esta política para todo sistema desarrollado para el Servicio. • Mantener vigente conjunto de estándares de diseño que consideran aspectos de seguridad para los nuevos sistemas. • Autorizar, validar y documentar los requerimientos funcionales y de seguridad, tanto para desarrollos externos como consultores, quienes deben velar por el cumplimiento de los hitos comprometidos.

4. Procedimiento

Seguridad de las aplicaciones en redes públicas y Protección de las transacciones.

Las aplicaciones deben cumplir con controles de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad, integridad y disponibilidad de la información y acceso a ella.

Encriptar las comunicaciones de los servicios expuestos en redes públicas.

Requerir el uso de métodos fuertes de autenticación para las aplicaciones core del Servicio expuestas a redes públicas.

El sistema debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.

El sistema debe permitir la implementación de certificados digitales tanto en software como en hardware.

Las aplicaciones deben implementar mecanismos de firma o validación o autorización de documentos mediante firma mecánica o digital.

El sistema debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.

El sistema debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).

Implementar controles para evitar la pérdida o duplicación de información de las transacciones.

Control de cambios en sistemas y ambientes de desarrollo seguro.

Aplicar el procedimiento de control de cambios vigente en el Servicio.

Probar el nuevo software en un ambiente separado tanto de los ambientes de producción como de desarrollo.

Pruebas de aceptación y seguridad de sistemas.

Nuestros implementadores de sistemas de información o tercerizados deben usar herramientas para el análisis de código y escáner de vulnerabilidades y deben corregir los defectos encontrados antes de entregar el sistema a las instancias de pruebas y producción.

Programa detallado de actividades y entradas de las pruebas y salidas esperadas en una variedad de condiciones.

Las pruebas se deben hacer en un ambiente de pruebas realista, para asegurar que las pruebas son confiables.

Se debe evitar el uso de datos operacionales que contengan información de datos personales o cualquier otra información confidencial para propósitos de prueba. Si esta información de datos personales u otra información confidencial se usa para propósitos de las pruebas, todos los detalles y contenido sensibles se deberían proteger

eliminándolos o modificándolos, la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.

Debe haber una autorización separada cada vez que se copia información operacional a un ambiente de pruebas.

Se deben tener ambientes de pruebas, desarrollo y producción.

El sistema debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.

El implementador del sistema de información, debe suministrar las evidencias de que se han hecho pruebas suficientes para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.

Diseño.

Las aplicaciones deben poder ejecutarse sobre las dos versiones más recientes en todos sus componentes (software base, bases de datos, frameworks de desarrollo, etc.) y se debe garantizar dentro de los acuerdos de niveles del servicio con los proveedores el soporte para al menos las dos versiones de software siguientes a su salida a producción.

Se debe establecer un control de versiones para cualquier tipo de aplicaciones. (Team Foundation Server).

Asegurarse de que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, por ejemplo, en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet.

La coordinación de aplicaciones junto con el procedimiento de control de versiones debe permitir realizar la trazabilidad de los cambios realizados en las mismas y el control estricto de las versiones en los diferentes ambientes (desarrollo, pruebas y producción)

El acceso a los diferentes ambientes (desarrollo, calidad o pruebas y producción) deben estar completamente segregados y los proveedores y/o desarrolladores no deben tener acceso al ambiente de producción, en caso de ser requerido el acceso al ambiente de desarrollo este deberá estar justificado por el Encargado de la Unidad de Informática y su acceso será controlado y supervisado por el Encargado de Seguridad de la Información, bajo ninguna circunstancia se realizaran ajustes al ambiente de producción sin pasar por los otros dos ambientes ni por el procedimiento de control de versiones respectivo.

Todo intercambio de información realizado entre aplicaciones se realizará de manera automática desde las mismas aplicaciones, con el fin de reducir las posibilidades de error humano y la pérdida de confidencialidad e integridad de la información, para ello se usará el protocolo XML y sus características de seguridad.

Es requerido que todas las aplicaciones sean desarrolladas de manera nativa sobre el estándar IPv4 y/o con compatibilidad para IPv6.

4.1. Documentos de referencia

En la siguiente tabla, se presentan los documentos que se han utilizado como referencia, para la formulación del presente manual de procedimientos.

Código	Descripción
SSI-A.05.01.01	Política de Seguridad de la Información
NCh-ISO 27001	Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información.
NCh-ISO 27002	Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información.

4.2. Registros de control del procedimiento.

a) Certificados SSL de los sitios web del Gobierno Regional de Los Lagos.
b) Pantallazos sitios web Gore Los Lagos con sus certificados instalados (https).

5. Validez y gestión de documentos

Este documento es válido desde la fecha de su aprobación.

El responsable de este documento es el Encargado de la Unidad de Informática, que debe verificar, y si es necesario actualizar el documento, por lo menos una vez cada tres años.

Aprobado Por
GOBIERNO REGIONAL - ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN - Región de Los Lagos GOBIERNO REGIONAL - COMITÉ DE SEGURIDAD DE LA INFORMACIÓN - Región de Los Lagos
Oscar Alejandro Oyarzo Pérez **Encargado de Seguridad de la Información**
05 de Noviembre de 2019