RECOMENDACIÓN DE NORMA TÉCNICA "CARACTERÍSTICAS TÉCNICAS DE LA PLATAFORMA DE SERVICIOS INFORMÁTICOS BÁSICOS"

PRÓLOGO

A continuación se presenta la Recomendación de Norma Técnica asociada a las "Características Técnica de la Plataforma de Servicios Informáticos Básicos", que establece las especificaciones técnicas que deberían considerarse en la plataforma tecnológica a la hora de su instalación, implementación y mantenimiento, con la finalidad de impulsar la Gestión Gubernamental enmarcado en un modelo eficiente, de calidad y sustentable.

La plataforma de servicios informáticos constituyen uno de los principales instrumentos que apoyan la gestión de las instituciones mediante el manejo de grandes volúmenes de datos necesarios para la toma de decisiones y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance.

Con el propósito de coadyuvar con ese marco de control y procurar una mejor gestión de dichas tecnologías por parte de las instituciones del Estado, la presente Recomendación se constituye en una normativa más

ajustada a la realidad y necesidad de nuestro ámbito tecnológico actual, para la gestión y el control de las tecnologías de información.

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Generalidades

Esta Recomendación de Norma Técnica establece los principios fundamentales que deberían ser considerados como aspectos básicos para la implementación de la plataforma de servicios informáticos de cualquier Órgano o Ente de los Poderes Públicos de la República Bolivariana de Venezuela, todo esto enmarcado por lo establecido en el Decreto N° 3.390 publicado en la Gaceta Oficial N° 38.095 de fecha 28 de diciembre de 2004.

1.2 Aplicación

Los elementos descritos en esta Recomendación de Norma Técnica pueden ser aplicados por todos los Órganos y Entes del Poder Público, a los fines de mantener una estructura uniforme en su plataforma tecnológica que que permita a todos los ciudadanos el acceso rápido y oportuno a los recursos y servicios que ofrece el Estado venezolano.

2 RECOMENDACIONES

2.1 Condiciones Generales

Todo Órgano y Ente de la Administración Pública debería implementar una plataforma tecnológica que cumpla con:

2.1.1 Establecer políticas asociadas al uso correcto de la plataforma a nivel de seguridad (accesos, permisología, autenticación, entre otros), así como el cumplimiento de la Resolución 320 del Ministerio de Ciencia y Tecnología publicada en Gaceta Oficial el 02 de Enero de 2006.

2.1.2.Generar los productos y servicios de tecnología de información de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.

2.1.3. Responder adecuadamente a las amenazas que puedan afectar la gestión de la plataforma de servicios, mediante una gestión continua de riesgos que esté integrada a los planes actuales de recuperación y seguridad de la información.

2.1.4 Garantizar de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida.

2.1.5. Mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.

2.1.6. Mantener una continuidad razonable de sus procesos; su interrupción no debería afectar significativamente a sus usuarios.

2.1.7. Optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren.

2.1.8. Mantener una perspectiva clara del estado del arte en materia tecnológica, así como de la tendencia de las Tecnologías de Información Libres.

2.2 Implementación de la Plataforma de Servicios Informáticos

Todo Órgano y Ente de la Administración Pública debería implementar y mantener las tecnologías de información requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento podrá adquirir, instalar y actualizar la infraestructura necesaria para soportar las aplicaciones informáticas de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos por la organización.

2.3 Características Técnicas de la Plataforma de Servicios Informáticos

Todo Órgano y Ente de la Administración Pública debería implementar y mantener una plataforma informática que contemple los siguientes servicios: Correo de Contenido, DNS, DHCP, LDAP, Servicio de Impresión, Servicio de Archivo, Seguridad, Respaldo y Recuperación, NTP, Distribución de Configuraciones. Es conveniente que los servicios informáticos posean las características que se enuncian a continuación:

2.3.1. Características Técnicas de la plataforma de Correo electrónico

a) Poseer sistema de filtrado de correos no deseados (SPAM).

b) Acceso de lista negras de remitentes.

c) Permitir implementar acciones a los mensajes de correo electrónico de acuerdo a la clasificación deseada: eliminar, rechazar mensajes.

d) Manejo de filtros bayesianos.

e) Manejo de cuotas de almacenamiento de buzón.

f) Manejo de IMAP seguro (cifrado).

g) Opciones de configuración de listas grises.

h) Bloqueo de remitentes.

i) Manejar lista de control de acceso.

j) Permitir frases y bloqueo de frases.

k) Permitir enviar mensaje a grupos de personas utilizando listas de correo electrónico.

l) Seguimiento exacto y en tiempo real de los resultados de las acciones emprendidas por el servidor de correo (LOGs).

2.3.2.Características Técnicas DNS

a) Recibir y resolver peticiones relacionadas con el sistema de nombres.

b) Traducir su nombre de dominio en una dirección IP

c) Traducir de dirección IP a nombre de dominio.

d) Asignar nombres a todas las máquinas de una red y trabajar con nombres de dominio en lugar de direcciones IP.

e) Permitir la transferencia de Zona y el soporte de transferencias de zona incremental (IXFR), donde un servidor de nombres sólo descargue las porciones actualizadas de una zona modificada en un servidor de nombres maestro. El proceso de transferencia estándar requiere que la zona completa sea transferida a cada servidor de nombres esclavo hasta por el cambio más pequeño.

f) Permitir la integración con DHCP.

g) Atender a las peticiones hechas por los distintos programas que acceden a Internet y resolver la dirección IP asociada al dominio consultado.

h) Compatibilidad con normas RFC (Peticiones de comentarios) producidas por el Grupo de Trabajo de Ingeniería de Internet (IETF).

i) Integración con LDAP.

j) Interoperabilidad con otras implementaciones del servidor DNS.

k) Vistas múltiples, a través del uso de la declaración "view" en "named.conf". BIND puede presentar información diferente dependiendo de quién esté realizando la petición.

l) Soporte de número de métodos diferentes para proteger la actualización y zonas de transferencia, en los servidores de nombres maestro y esclavo.

m) Permitir firmar con caracteres criptográficos zonas con una clave de zona, a través de DNSSEC.

n) Permitir que una transferencia desde el maestro al esclavo sea autorizada sólo después de verificar que una clave secreta compartida existe en los servidores maestro y en el esclavo, utilizando TSIG.

ñ) Soporte de TKEY.

2.3.3.Características Técnicas DHCP

a) Proporcionar configuración de forma dinámica a través de un servidor del protocolo. Se debería proporcionar los siguientes datos: dirección IP, máscara de red, dirección de broadcast, características del DNS, entre otros.

b) Acelerar y facilitar la configuración de ordenadores en la red local, evitando en gran medida los posibles errores humanos.

c) Configurar un único servidor para entregar números IP para clientes de red.

d) Disminución de las tareas administrativas, eliminación de conflictos de red y direcciones duplicadas.

e) Proveer una configuración robusta, estable, confiable.

2.3.4.Características Técnicas LDAP

a) Permitir el acceso a un servicio de directorio ordenado y distribuido para realizar consultas en un entorno de red.

b) Consolidar información para toda la organización dentro de un repositorio central usando para ello el LDAP, dado que éste soporta la Capa de Conexión Segura (SSL) y la Seguridad de la Capa de Transporte (TLS), además de que se pueden proteger los datos confidenciales.

c) Soportar un número de bases de datos administrativas en las que se guarden directorios. Esto permite que los administradores tengan la flexibilidad para desplegar la base de datos más indicada para el tipo de información que el servidor tiene que diseminar.

d) Configuración de servidor de replicación.

e) Soporte LDAPv3 — OpenLDAP soporta la Capa de Autenticación y Seguridad (SASL), la Seguridad de la Capa de Transporte (TLS) y la Capa de Conexión Segura (SSL), entre otras.

f) LDAP sobre IPC — OpenLDAP se puede comunicar dentro de un sistema usando Comunicación Interproceso (IPC), lo que mejora la seguridad al eliminar la necesidad de comunicarse a través de la red.

g) Soporte LDIFv1 — Provee compatibilidad completa con el formato de intercambio de datos, Data Interchange Format (LDIF) versión 1

2.3.5.Características Técnicas Servicio de Impresión

a) Gestionar los trabajos y tareas de impresión.

b) Soporte de impresión de red utilizando el Protocolo estándar de Impresión en Internet (IPP)

c) Soporte de procesamiento PPD.

d) Permitir la auto-detección de impresoras de red.

e) Disponer de una herramienta basada en Internet para la configuración y administración.

f) Permitir segmentación por grupo de usuarios.

g) Manejar asignación de cuotas de impresión.

2.3.6.Características Técnicas Servicio de Archivo

a) Compartir archivos entre ordenadores de una misma red local.

b) Implementación de código abierto usando el protocolo NFS

c) Identificar e Implementar mecanismo de seguridad.

2.3.7.Características Técnicas Seguridad Cortafuegos (Firewall)

a) Definir políticas de seguridad claramente especificadas, de acuerdo a sus sistemas y servicios de red, sólo el tráfico definido en estas políticas es permitido.

b) Identificar e implementar mecanismo de seguridad.

c) Todo el tráfico de la red desde adentro hacia afuera, y viceversa, debe pasar a través de él.

d) Poder definir filtrado de paquetes: entrada y salida.

e) Bloqueo de puertos.

f) Política por defecto en DROP, (Bloqueado sólo permito los accesos validos)

2.3.8. Características Técnicas Respaldo y Recuperación

a) Definir políticas de respaldo y recuperación.

b) Administración centralizada del servicio.

c) Disponer de un catálogo centralizado.

d) Programación interna para ejecución automática y simultanea de trabajos por prioridades.

e) Permitir la administración y supervisión de todos los trabajos.

f) Flexibilidad a la hora de definir qué respaldar.

g) Permitir la recuperación de información en cualquier punto del tiempo.

h) Garantizar optimización de ancho de banda.

i) Permitir respaldos completos, diferenciales e incrementales.

j) Permitir copiar y restaurar ficheros dañados o perdidos.

k) Permitir comunicaciones encriptadas.

2.3.9 Características Técnicas NTP

a) Permitir sincronización con servidores de horas de otros proveedores.

b) Permitir la requisición de hora local a sistemas clientes.

c) Compatible con SNTP

2.3.10. Características Técnicas Servicio de Distribución de Configuraciones

a) Actualización de paquetes de forma centralizada.

b) Correlación en las versiones y paquetes instalados.

c) Distribución de configuraciones a múltiples computadoras.

d) Soporte de comunicación cifrada.

2.4 Administración y Operación de la Plataforma

Todo Órgano y Ente de la Administración Pública debería mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas, para ello tendrá que considerar:

a) Establecer y documentar los procedimientos y las responsabilidades asociadas con la operación de la plataforma.

b) Contar con un sistema de monitoreo que le permita la visualización en tiempo real de la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.

c) Identificar eventuales requerimientos, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de tecnología de información solicitados, tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.

d) Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (equipos y aplicaciones informáticas), custodiar adecuadamente las versiones de las aplicaciones informáticas y realizar verificaciones físicas periódicas.

e) Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.

f) Mantener separados y controlados los ambientes de desarrollo y producción.

g) Brindar el soporte requerido a los equipos principales y periféricos.

h) Controlar los servicios e instalaciones realizadas por terceros.

2.5 Seguridad de la Plataforma

a) Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.

b) Disponer de una herramienta que permita a los administradores de la plataforma ejecutar programas con los privilegios de seguridad de otro usuario de manera segura.

c) Garantizar el acceso remoto a los servidores, mediante sesiones seguras a través de canales cifrados, con la posibilidad de definir puertos de accesos aleatorios.

3 REFERENCIAS

[1] Decreto N° 3390, publicado en Gaceta Oficial N° 38.095 de fecha 28 de Diciembre de 2004.