Marco Normativo de IT

ES0101 – Estándar de Arquitectura para los Sistemas de Información e Infraestructura del Data Center

Agencia de Sistemas de Información

Gobierno de la Ciudad Autónoma de Buenos Aires

Índice

Antecedentes

1. Situación Actual

El desarrollo de aplicaciones sucede en un entorno tecnológico caracterizado por su diversidad y constante transformación. Las diferentes plataformas –sistemas operativos, servidores de aplicaciones y de bases de datos-, la variedad de lenguajes de desarrollo y la evolución de las tecnologías de integración, ofrecen mejoras y ventajas demandadas por los Desarrolladores quienes esperan con ellas brindar mejores servicios a los Usuarios de dichas aplicaciones.

Esta situación plantea también un desafío para los Arquitectos y los Administradores de Sistemas, quienes en caso de no haber tomado las decisiones adecuadas, enfrentarían el riesgo de encontrarse en el futuro lidiando con un conjunto heterogéneo de sistemas y aplicaciones.

2. Requerimiento

Dentro del marco de la Gestión de Procesos de TI de la Agencia de Sistemas de Información (ASI), es necesario diseñar e implementar un modelo de arquitectura de sistemas de información que considere la definición de los siguientes factores.

- → Plataformas operativas estándares y escalables.
- → Herramientas, servicios y recursos estándares, para soporte de las aplicaciones.
- → Entornos operativos que garanticen la disponibilidad de las aplicaciones y sistemas de información.
- → Un adecuado esquema que asegure la detección y diagnóstico de problemas de acuerdo a la necesidad de servicio requerida por la ASI.

3. Responsabilidad

La Agencia de Sistemas de Información (ASI) es la entidad rectora en cuanto a la implementación y operación de la infraestructura informática y de telecomunicaciones, los servicios tecnológicos y los sistemas de información en el ámbito del Gobierno de la Ciudad Autónoma de Buenos Aires.

En particular, en lo que respecta a la infraestructura informática, desarrollo y administración de sistemas, es responsabilidad de la ASI dotar a la Ciudad de una plataforma robusta, autosuficiente, razonable y bien definida en cuanto a recursos y procedimientos, que garantice la eficiencia y disponibilidad de los diferentes sistemas de información alojados en los Data Centers administrados por la ASI.

En tal sentido es la ASI la indicada para satisfacer el requerimiento expresado en el título anterior.

4. Objeto y Alcance

Este documento tiene por objeto formalizar y especificar el modelo de arquitectura aplicable a los Data Centers operados por la ASI, asegurando mediante una adecuada gestión tecnológica, su escalabilidad, agilidad y alta disponibilidad.

Todos los nuevos sistemas que se instalen en Data Centers operados por la ASI deberán respetar los criterios aquí descriptos. Los criterios establecidos en este documento serán también aplicables para los integradores que implementen todo tipo de sistemas desarrollados por terceros dentro de la infraestructura informática del GCABA en cumplimiento de contratos que así lo soliciten.

Estas implementaciones, deberán efectuarse respetando los criterios de arquitectura y entornos de desarrollo, homologación y producción descriptos en este documento de tal forma que los sistemas producto de la contratación puedan ser implementados en Data Centers del GCABA.

Arquitectura de Sistemas

1. Arquitectura Física

La arquitectura de los sistemas y la topología de las redes de servidores de todos los ambientes proporcionados por la ASI donde se alojen los sistemas y Bases de Datos en el Data Center de la ASI son iguales.

Las aplicaciones que residan en los servidores de la ASI (en adelante, "servidores de aplicaciones"), serán accedidas por los usuarios desde los distintos navegadores homologados (ver Anexo 2), en el esquema de desarrollo de invocación de servicios.

En estos servidores de aplicaciones residirá la lógica de presentación, es decir la que se comunica con los navegadores utilizados por el Usuario, y parte o toda la lógica de negocio. Por lo tanto, en los navegadores no debe residir ningún dato, tabla, archivo o documento excepto durante el tiempo que dure una transacción. Toda información deberá ser almacenada en servidores específicos.

Los servidores de aplicación serán agrupados bajo el esquema de Granjas, permitiendo la escalabilidad de los sistemas primero en forma horizontal, través del incremento de la cantidad y capacidad de los servidores físicos, y en segundo plano a través del aumento de la capacidad de los servidores en los cuales residan los motores de Bases de Datos.

2. DMZs

Una DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS. El esquema denominado, Granja de Servidores de Aplicaciones, se localiza dentro de una DMZ (ver Anexo 1).

Cada DMZ contiene un balanceador de carga de capa 7 (load balancer), quien será el encargado de distribuir las peticiones entre los distintos servidores de aplicaciones, a fin de poder distribuir la carga de transacciones entre los distintos servidores que atienden a los Usuarios, y al mismo tiempo contar con la facilidad de efectuar el mantenimiento en caliente de las aplicaciones.

La ASI contará con cuatro DMZs:

- → **DMZ de Producción para Usuarios Externos**: Utilizada únicamente para alojar aplicaciones en producción que necesiten ser accedidas desde fuera de la Red del GCABA.
- → **DMZ de Producción para Usuarios Internos**: Utilizada únicamente para alojar aplicaciones en producción que necesiten ser accedidas desde dentro de la Red del GCABA.
- → **DMZ de Homologación para Usuarios Externos**: Utilizada para alojar las aplicaciones que se encuentren en etapa de homologación, y necesiten ser accedidas desde fuera de la Red del GCABA.
- → **DMZ de Homologación para Usuarios Internos**: Utilizada para alojar las aplicaciones que se encuentren en etapa de homologación, y necesiten ser accedidas desde dentro de la Red del GCABA.

Esta arquitectura/topología será idéntica tanto para los sistemas que implementan transacciones desde Internet por Usuarios externos al GCABA, como para las aplicaciones accedidas por personal del GCABA desde la red interna del Gobierno.

3. Entornos

El Data Center de la ASI contará con los siguientes Entornos:

- → Entorno de Desarrollo.
- → Entorno de Testing.
- → Entorno de Homologación.
- → Entorno de Producción.

Todos los entornos serán idénticos en términos topológicos y en cuanto a las funcionalidades en ellos implementadas. Todos los ambientes contarán con balanceo de carga.

Ningún Usuario, externo o interno, accederá directamente a servidores que no están en alguna de las DMZ.

La responsabilidad y administración de los entornos mencionados será siempre de la ASI.

En el Entorno de Desarrollo y Testing residirán los servidores utilizados para el desarrollo y prueba de las aplicaciones, hasta alcanzar la madurez de la las mismas.

4. Arquitectura Lógica

Todas las aplicaciones deberán tener claramente separados sus Servidores de Aplicación de sus Servidores de Bases de Datos.

En ningún caso la ASI será responsable por la pérdida de información persistente; es decir archivos temporales, logs, datos no propios del sistema; que las aplicaciones pudiesen generar en los servidores mencionados.

La ASI podrá modificar la configuración del esquema de granjas (cantidad de servidores, mecanismos de persistencia de sesión y balanceo de carga) sin necesidad de dar previo aviso a los Usuarios, a los Desarrolladores o al Personal de Soporte, siempre que esto sea trasparente para los afectados.

Los Servidores de Aplicación no tendrán direcciones IP externas y solo recibirán solicitudes HTTP.

Los Servidores de Aplicación que formen parte de una Granja serán entre sí totalmente independientes, es decir que no emplearán ningún mecanismo de acoplamiento entre ellos.

Como mecanismo de balanceo de carga se utilizará la metodología *Round-Robin*.

Para establecer la comunicación entre los Servidores de Aplicación, las Bases de Datos, el sistema de gestión de documentos y otros servicios tales como el E-Mail, deberán utilizarse únicamente los puertos estándar definidos para dichos servicios.

En el caso de las Bases de Datos se otorgará a la aplicación un Usuario de Base de Datos con los mínimos permisos necesarios para ejecutar las transacciones.

Las Bases de Datos de todos los Entornos serán creados por la ASI.

Todas las aplicaciones que tengan que hacer referencia a un servidor deberán hacerlo por su nombre DNS, jamás por su dirección IP. La relación entre nombres y direcciones IP podrá ser cambiada por la ASI tantas veces como sea necesario sin aviso previo a los Usuarios, a los Desarrolladores o al Personal de Soporte, siempre que esto sea trasparente para los afectados.

Todas las aplicaciones deberán cumplir con lo definido en el *PC0901 - Proceso de Control de Cambios para Organismos*.

Para evitar posibles problemas de compatibilidad entre los diferentes Entornos, la ASI pondrá a disposición de quienes lo requieran, las imágenes virtuales de las configuraciones homologadas.

La ASI será la responsable de administrar las configuraciones de los Servidores de todos los Entornos (Desarrollo, Testing, Homologación y Producción).

El espacio en dónde correrán las aplicaciones será definido por la ASI. El servidor físico o virtual en el que correrá podrá ser un espacio compartido con otras aplicaciones.

Todas las aplicaciones correrán en la modalidad 7x24, sin ventana de mantenimiento. En todos los casos los procesos serán ejecutados sin interrumpir la prestación de servicios interactivos o servicios Web.

5. Servicios

El Data Center de la ASI dispondrá de un conjunto de Servicios que los Desarrolladores podrán utilizar para implementar sus aplicaciones.

Los servicios disponibles en el Data Center de la ASI son los siguientes (ver Anexo 2):

- → **Motor Bases de Datos**
- → Sistema Operativo
- → **Gestión Documental**
- → **Correo Electrónico**
- → **Protocolo de Sincronización de Relojes**
- → **Documentos en Formato Portable y Firma Digital**
- → **Mensajería Instantánea**
- → **Servidores de Dominio por Entorno**

  Servidores Web / Servidores de aplicacion Java / Servidores de aplicacion .net

NOTA: Ver en Anexo 2 "Versiones Homologadas" las versiones soportadas actualmente de cada uno de estas herramientas descriptas.

6. Logs

Los sistemas a implementar en el Data Center de la ASI deben prever la creación simultánea de tres tipos de logs:

Logs de Debugging

Los Logs de Debugging serán utilizados por los Desarrolladores como ayuda en el diagnóstico del funcionamiento de un programa.

El formato de los mismos es libre, sin restricciones específicas, y su contenido será normalmente información acerca del estado del programa, de las variables, etc.

Cualquier Log generado por una aplicación que no corresponda a Log des Actividad o Log de Auditoría –los cuales se describen más abajo- serán considerados Logs de Debugging.

Los Logs se almacenarán en el mismo servidor que los produce y no estarán incluidos en ningún proceso de backup.

La generación y grabación de los Logs deberá estar controlada por un archivo externo al programa (por ejemplo un XML), de tal forma que la generación y grabación de los Logs de Debugging pueda activarse o desactivarse en caliente sin cambiar los programas, y sin tener que reiniciar la aplicación.

Logs de Actividad

Los Logs de Actividad serán utilizados por las herramientas de monitoreo del Data Center para determinar la actividad de los sistemas y predecir comportamientos anómalos que puedan estar indicando fallas en las aplicaciones y/o en la infraestructura tecnológica.

Se deberá generar un registro de Log de Actividad por cada transacción ejecutada, sea ésta de consulta o actualización.

Deberá logearse el 100% de las transacciones con este tipo de Logs. La generación del Log se efectuará cuando la transacción comienza, no cuando termina.

Estos Logs serán generados y serán almacenados remotamente en el repositorio de Logs de Actividad, contenido en un servidor dedicado exclusivamente a dicha función y administrado por la ASI.

Los sistemas no deberán tener ningún archivo de configuración, ni comando alguno o transacción que permita deshabilitar la existencia de estos Logs.

Logs de Auditoría

Los Logs de Auditoría serán utilizados por Auditoria para reconstruir el contenido de las Bases de Datos en función de las modificaciones que los registros de la base han sufrido a lo largo del tiempo, con el objeto de determinar cuando fue modificada una determinada información de la Base de Datos y quién efectuó la modificación.

Estos Logs serán generados y serán almacenados remotamente en el repositorio de Logs de Auditoría, contenido en un servidor dedicado exclusivamente a dicha función y administrado por la ASI.

Los sistemas no deberán tener ningún archivo de configuración, ni comando alguno o transacción que permita deshabilitar la existencia de estos Logs.

7. Componentes de Aplicaciones y Servidores

Versiones de Componentes

Cualquier paquete de software que se instale en los servidores de producción asociado a una aplicación y en adición al software de base provisto por la ASI, será considerado parte de la aplicación, siendo el Desarrollador responsable de su buen funcionamiento y compatibilidad con el software de base definido como estándar por la ASI para sus servidores.

El desarrollador es también responsable de garantizar la compatibilidad de su software con otros aplicativos que pudieran correr simultáneamente en los mismos servidores de producción, sean estos físicos o virtuales.

Los paquetes de software a ser instalados como requerimiento para la ejecución de las aplicaciones, deberán ser siempre versiones estables y que correspondan a la distribución del sistema operativo estándar que se encontrará en los Servidores de Producción. Bajo ningún concepto se aceptarán versiones "beta" de ningún paquete de software.

En el caso que sea necesario instalar paquetes compilados, se deberá declarar y documentar qué paquetes se instalarán, manteniendo el Desarrollador la responsabilidad de actualizar dichos paquetes.

En estos casos, los paquetes compilados serán considerados parte de la aplicación debiendo suministrarse pre-compilados e integrados en ella. Al momento de solicitar el pase del sistema al Entorno de Producción, se deberá informar qué librerías externas utiliza la aplicación, de tal forma que puedan integrarlas a una Base de Datos con el nombre de la librería, la versión, el sistema que depende de la librería, y los servidores donde se encuentra instalada.

La ASI cruzará las vulnerabilidades publicadas periódicamente con la matriz de dependencias y alertar qué servidores deben ser actualizados.

Los desarrollos que hayan sido realizados integrando componentes, módulos o sistemas de cualquier tipo sujetos a licenciamiento, deberán ser entregados por el Desarrollador conjuntamente con la documentación que acredite la legítima propiedad o derecho de uso de dichas licencias.

8. Actualizaciones de Aplicaciones

Todos los involucrados en un proyecto de desarrollo deberán subir las nuevas versiones de sus aplicaciones al GIT dedicado a tal efecto.

Para obtener acceso a dicho servicio, se deberá consultar el *ES0901 - Estándar de Desarrollo ASI*.

9. Solicitud de Servicios

La Solicitud de Servicios debe ser hecha a través de una CCOO (Comunicación Oficial), adjuntando un Formulario Único de Requerimiento (FUR) dirigida al Director Ejecutivo de la ASI.

En la solicitud no se podrán especificar condiciones especiales, sino elegir entre las imágenes disponibles para estos servidores, las cuales coinciden con las imágenes de producción. Se podrán bajar copias de esas imágenes virtuales desde la misma dirección para ser utilizadas en el desarrollo o para

enviar a los Desarrolladores de manera tal que estos puedan desarrollar sus aplicaciones sobre sistemas idénticos a los de la ASI.

En caso que el Desarrollador haya decidido implementar sus productos sobre una imagen provista por la ASI, podrá optar por enviar la imagen completa a la ASI, quien procederá a efectuar la implementación en el Entorno de Homologación.

10. BackUps

La ASI efectuará un backup de los servidores de aplicaciones cada vez que se modifique un programa (aplicación), el software de base (sistema operativo, etc.) o un archivo de configuración (ver Resolución *177-ASINF/13*). Solo se realizarán backups de los servidores de aplicaciones si se verifica alguna de estas condiciones.

En función de esta condición, se deberá tener en cuenta que no se debe almacenar ninguna información relevante en los servidores de aplicaciones. Solo podrán almacenarse en el servidor de aplicación los *logs de debug* y *archivos temporarios* que pierdan su valor al terminar la transacción que los genera.

Las Bases de Datos y repositorios de documentos se persistirán a través de procesos de backup totales y/o incrementales ejecutados con la periodicidad que la aplicación requiera, y que la disponibilidad de la infraestructura tecnológica existente permita. Estos se efectuarán en caliente, sin ventana de mantenimiento. Esto significa que ningún sistema podrá incluir un programa o procedimiento, sea batch o interactivo, que requiera el uso exclusivo de la Base de Datos o la suspensión de la interacción del sistema con Usuarios físicos (transacciones interactivas) o lógicos (Web Services o accesos directos a la Base de Datos)

En otras palabras, todos los sistemas tienen que ser capaces de operar con todas sus funcionalidades las 24 horas del día, los 7 días de la semana, sin ventana de mantenimiento.

11. Browsers e Interface con el Usuario

Todas las aplicaciones deberán soportar con la misma funcionalidad y aspecto visual todos los navegadores y sistemas operativos detallados en el Anexo de Versiones Homologadas.

No se podrán usar componentes que deban residir en la PC del Usuario y que requieran licenciamiento o la ejecución sobre un sistema operativo propietario.

Los Desarrolladores serán responsables de incluir en los programas interactivos los controles necesarios para neutralizar los ataques listados por el Top Ten 2013 de Open Web Application Security Project (OWASP).

12. Configuraciones Standard

Para los Servidores Instalados en la ASI, la configuración estándar es la siguiente:

- RedHat
- Apache
- Jboss
- Tomcat
- PHP
- JDK/JRE
- Hibernate
- Drupal

Servicios Instalados en VLAN de Storage de Producción

- Adobe LiveCycle (versión última vigente):
  - Adobe Reader Extensions
  - Adobe PDF Generator
  - Adobe Digital Signatures
- Active MQ (versión última vigente).

Anexos

Anexo 1: Esquema Lógico del Data Center – Política General del Flujo de Tráfico

Las políticas generales de flujos de tráfico pretenden dar las pautas de dirección de los flujos de datos entre dominios. Los controles generales de dirección de flujos de datos que fija la ASI son los que se exponen a continuación:

El dominio de redes públicas sólo podrá realizar peticiones a equipos que se encuentren en el domino de extranet. En ningún caso deben realizar conexiones a equipos que se encuentren en dominios confiables distintos de la extranet.

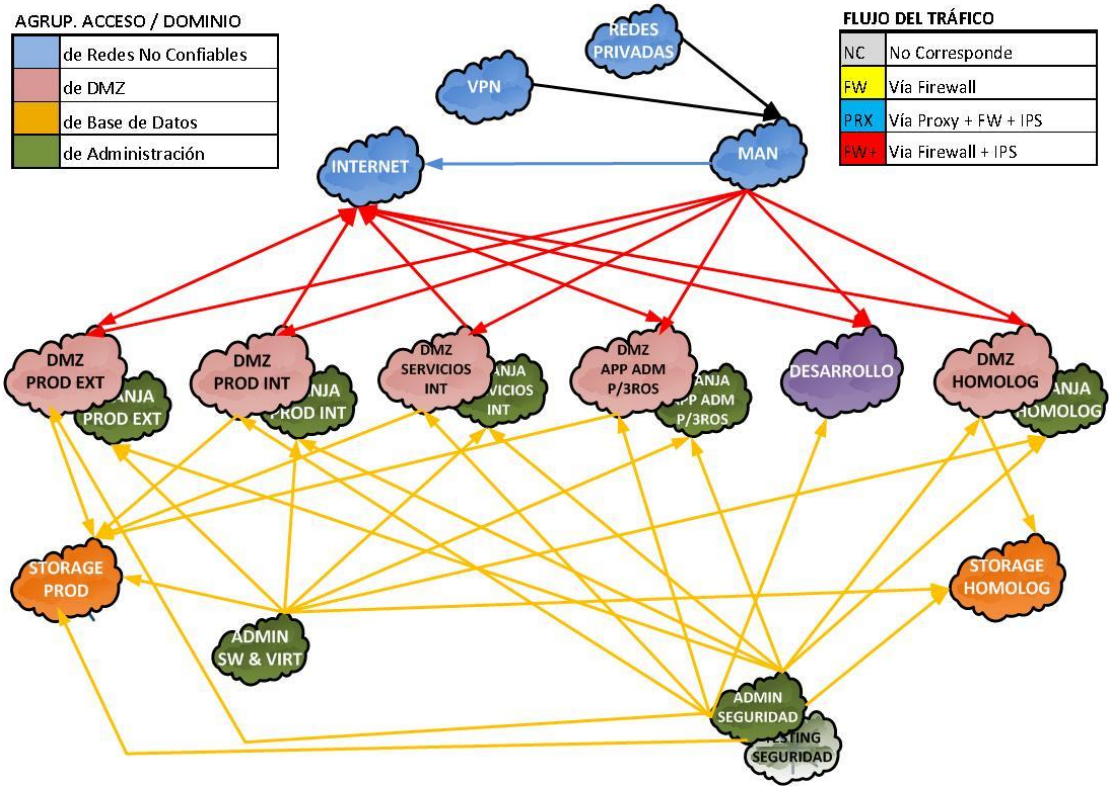
Los servidores del dominio de extranet podrán realizar peticiones exclusivamente hacia los servidores del dominio de servidores que tengan sus bases de datos.

Los servidores de pasarela (gateway) de la extranet tendrán privilegios especiales de acceso, pudiendo acceder a Internet (proxy de salida) y a la Intranet (dispositivos de VPN).

El dominio de Intranet no podrá realizar conexiones hacia los dominios públicos. Para poder acceder a ellos deberán hacerlo a través de las pasarelas de acceso a Internet (proxy de salida).

Los servidores del dominio de Servidores en ningún caso podrán realizar conexiones salientes hacia otros dominios. Podrán recibir conexiones del resto de dominios a través de la interfaz que corresponda

En la siguiente figura se representa gráficamente los diferentes flujos de datos permitidos entre los distintos dominios de la Red del GCABA:


AGRUP. ACCESO / DOMINIO
de Redes No Confiables
de DMZ
de Base de Datos
de Administración
FLUJO DEL TRÁFICO
NC No Corresponde
FW Vía Firewall
PRX Vía Proxy + FW + IPS
FW+ Via Firewall + IPS
REDES PRIVADAS
VPN
INTERNET
MAN
DMZ PROD EXT
DMZ PROD INT
DMZ SERVICIOS INT
DMZ APP ADM P/3ROS
DESARROLLO
DMZ HOMOLOG
STORAGE PROD
STORAGE HOMOLOG
ADMIN SW & VIRT
ADMIN SEGURIDAD

Anexo 2: Versiones Homologadas

Tipo de Aplicativo	Programa	Versión
Bases de Datos	Oracle DB2 MySQL Server Version POSTGRES	11 G V 10.5.0.3 5.5 9.1.9
Sistema Operativo	RedHat Enterprise Server Suse	6.5 11 SP3
Navegadores	Microsoft Internet Explorer Firefox	11 32
Firma digital	Adobe LiveCycle con Adobe Reader Extensions, Adobe PDF Generator y Adobe Digital Signatures	10.0.2
Lenguajes de programación	PHP Drupal Java	5.3.3 7.26 JDK 1.7.0_55
Gestor Documental	WebDav	Apache 2.2.15
Servidores de Aplicación	Tomcat Apache JBoss	6 2.2.15 (Unix) 7.1.1
Mensajería	JDK/JRE Hipernate Active MQ	1.6.0 IBM 3.2 5.3.0
Virtualizador	VMWare ZVM	5.5 6.3

Nota: las versiones serán consensuadas al momento de establecer el modelo de arquitectura de la aplicación.