Estándar de Desarrollo

Subsecretaría de Gestión Pública y Modernización del Estado

Dirección de Desarrollo

Gobierno del Chubut

Autor: Lic. Carmine Fernando

14/06/2016

Versión:2.0

Requisitos para el alojamiento en el Data Center

Alojamiento de los sistemas

Todos los sistemas que no sean de uso interno deberán ser alojados en el Data Center dependiente de la Dirección General de Tecnología (DGT).

Requerimiento de logs:

Los sistemas a implementar en el Data Center de la DGT 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 de 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 DGT. 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 cuándo 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 DGT. Los sistemas no deberán tener ningún archivo de configuración, ni comando alguno o transacción que permita deshabilitar la existencia de estos Logs.

Browsers e Interface con el Usuario

Todas las aplicaciones deberán soportar con la misma funcionalidad y aspecto visual todos los navegadores.
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).

Plataformas de desarrollo

Las plataformas de desarrollo autorizadas son las siguientes:

- Plataforma Java
- Plataforma PHP
- Plataforma Python
- Plataforma Javascript
- Plataforma Móvil

Bases de datos

Las bases de datos autorizadas para los sistemas son:

- Postgres
- Mysql
- MongoDB
- Cassandra

Si se presenta una situación de duda sobre la elección de la plataforma/motor de Base de Datos, se debe solicitar asesoramiento a la Dirección de Desarrollo al momento del Diseño.

Disponibilidad de Datos (API)

Toda aplicación debe contar con una API disponible con la información relevante y con un formato de extracción de datos para exponer y ser publicada, así como también permitiendo la interoperabilidad entre los sistemas.

Requerimientos No Funcionales

Logging

Se debe definir el nivel de logging de los sistemas a implementar dependiendo de la naturaleza de cada uno de ellos.
Plataforma Java: las aplicaciones deben usar log4j
Plataforma PHP: las aplicaciones deben usar syslog

Administración de Errores

La aplicación debe evitar enmascarar los mensajes de error http de forma tal que los balanceadores / proxy puedan entender el estado actual del aplicativo. Ante un error inesperado no debe visualizarse por front características del servidor, ip, path, o cualquier información que permita conocer propiedades de infraestructura Por ejemplo, si ocurre un error en el aplicativo la respuesta http de estado debe ser código 500 y el mismo no debe reemplazarse por ningún otro código.

Disponibilidad

La aplicación debe ser 7x24 sin ventana de mantenimiento, sin interrumpir la prestación de servicios interactivos o Web Services. Se debe tener en cuenta que todos los procesos de backups que sean necesarios deben soportar este requerimiento. En caso de contar con la necesidad de bajar la aplicación por un tiempo determinado, debe contemplar desde la administración del usuario que un administrador pueda realizar una baja controlada del servicio que permita visualizar a los usuarios un aviso de la situación.

Modularidad

Los distintos servicios, Application servers, base de datos, etc. deben estar desacoplados, permitiendo separarlos y configurarlos en distintas vlans según la funcionalidad de los mismos, como se encuentra especificado en el Documento de Arquitectura.

Estética

Tanto los sitios web como los sistemas Gubernamentales deben tener una concordancia estética homogénea que se corresponde con el plan gráfico integral del Gobierno del Chubut. Por este motivo, los diseños web ya sean de aplicaciones accedidas desde la intranet o desde internet deben tener la conformidad de la Dirección de Desarrollo.

Validación de los Datos de Entrada

Todas las pantallas de ingreso de datos deben validar los datos provistos por el usuario en tipo de dato, longitud y rango válido. No se debe confiar en las validaciones del cliente. Las validaciones deben estar implementadas tanto en la capa de presentación de la aplicación como en el servidor. Los datos ingresados deben presumirse incorrectos hasta que se demuestre lo contrario.

Subida de Archivos

Si la aplicación permite la subida (upload) de archivos se debe verificar no solo la extensión sino también su tipo MIME. En el caso de ser imágenes se recomienda realizar algún tipo de transformación del lado del servidor para prevenir ataques conocidos (Ej.: GIFAR) No se debe permitir la subida de ningún archivo que pueda ser procesado por el servidor. Por ejemplo, están prohibidas las subidas de archivos con extensiones php, asp, htm, exe entre otras. Adicionalmente, si estos archivos se almacenan en un sistema de archivos, la carpeta correspondiente no debe permitir ejecución. Toda subida de archivos debe validar el tamaño máximo permitido de los archivos. Este valor debe ser configurable a través de un administrador.

Entrega de Actualizaciones

Toda entrega de archivos entre un proveedor externo y la Dirección de Desarrollo se hace a través de un servicio Versionador con autenticación y encriptación provista por SSH. Se busca evitar el uso de VPNs manteniendo una comunicación segura entre las partes y ofreciendo la integridad de los datos.

Versionamiento

Es obligatorio que todo producto a instalar debe contar una etiqueta de versión visible fácilmente siguiendo las reglas siguientes:

- La versión beta es una versión completa desde un punto de vista funcional. El equipo de proyecto debe ser capaz de justificar que se han alcanzado los requisitos y expectativas.
- La versión estable se denota como 1.0.0, luego se tienen las siguientes reglas:
    - 1.0.Z: Resolución de incidencias sobre la versión 1.0.0
    - 1.Y.0: Si aumenta la Y, la Z se pone a cero e implica que se han incorporado mejoras y probablemente resolución de incidencias

- Z.0.0: Conlleva lo anterior pero además implica cambios importantes a múltiples niveles (diseño, funcionalidades, UI, etc.)

Transferencia de Conocimientos

El proveedor debe realizar la transferencia de conocimientos del proyecto a un grupo de funcionarios de la Dirección de Desarrollo y al organismo responsable del sistema con la menor cantidad de inconvenientes posible. Dicho traspaso debe incluir la entrega de las últimas versiones de la documentación funcional y de diseño relacionada con el proyecto más una capacitación de los funcionarios técnicos sobre la estructura del código fuente, las particularidades de compilación y funcionamiento del sistema, configuración, parametrización y todo lo necesario para poder realizar la implementación del desarrollo y su posterior mantenimiento. Esta capacitación debe realizarse antes de finalizar la ejecución del proyecto de manera de poder detectar en forma temprana los problemas que se encuentren en el sistema y entender los arreglos que se vayan realizando. Esta transferencia tiene como segundo objetivo permitir la evaluación de cuestiones no funcionales que sólo son visibles si se comprende el funcionamiento interno de los componentes.

Entregables

Se detallan a continuación los entregables mínimos requeridos para un proyecto de desarrollo de software y el contenido esperado en cada uno de ellos:

Entregable	Contenido
Documento de Proyecto	Objetivo y alcance del proyecto
Documento de Requerimiento	• Documento de requerimientos (funcionales y no funcionales) que incluya los objetivos funcionales del proyecto, alcance y origen de los requerimientos. • Requerimientos funcionales acordados y priorizados.
Documento de Arquitectura	• Modelo lógico y físico de datos. • Ambientes requeridos • Herramientas de desarrollo • Arquitectura tecnológica (sistema operativo, software de base, motor de base de datos, etc.)
Paquetes de software	Para cada entrega acordada con el proveedor se debe presentar: • Código fuente generado en su totalidad instalado en los ambientes de Desarrollo de la DGT. • Instalación de todos los componentes de software adicionales necesarios para el correcto funcionamiento de lo entregado. • Documento de requerimientos / funcionalidades incluidas en el paquete entregado. • Documento de control de cambios. • Transferencia de conocimiento. • Manual de operaciones e instalación.
Documento Manual de Usuario	Documentación completa del software que incluya todas las funcionalidades para todos los roles y la administración de roles, permisos y seguridad.
Material de Capacitación	• Propuesta con el plan de capacitación. • Documentación que incluya la completitud de la funcionalidad a capacitar.

Control del documento

Versiones

Fecha	Autor	Versión	Descripción
27/05/2016	Carmine Fernando	1.0	Documento versión inicial