# Lista de verificación para la liberación de servicios soportados por sistemas, aplicaciones y sitios web a producción

## Introducción

La presente lista de verificación tiene como finalidad servir como una guía a los responsables TIC de las entidades o dependencias universitarias, con los elementos que se deben tener en cuenta antes y al momento de poner en producción un sistema, aplicación o sitio web que brinde un servicio a la comunidad universitaria o sociedad en general, con la finalidad de reducir incidentes en su puesta en operación.

Se deja a la consideración del responsable TIC si aplica o no cada uno de los elementos propuestos para la liberación del servicio en la entidad o dependencia.

## Elementos a verificar

### Consideraciones sobre la aplicación

| **Condición** | **Cumple**  **[Sí/No/**  **No aplica]** | **Soporte documental** | **Observaciones** |
| --- | --- | --- | --- |
| El sistema, aplicación y sitio web validan los datos de entrada en formato, tipo y contenido. |  |  |  |
| Se evitó el uso de consultas dinámicas en el desarrollo del sistema o aplicación web. |  |  |  |
| El sistema, aplicación o sitio web envía los datos a través del método POST. |  |  |  |
| Se utilizaron las funciones “prepared statements” propias del lenguaje para el acceso a la base de datos. |  |  |  |
| Para la inclusión de archivos remotos se utiliza file\_get\_contents() en lugar del include(). |  |  |  |
| El sistema, aplicación y sitio web validan los datos de salida en formato, tipo y contenido. |  |  |  |
| Para sistemas, aplicaciones y sitios web que requieran autentificarse se debe validar que se exige una longitud mínima y una serie de caracteres especiales, así como el uso de un *captcha* para evitar robots y ataques de fuerza bruta. |  |  |  |
| Si el sistema o aplicación web maneja sesiones de usuario, estas deben tener un tiempo de vida y terminarse si se cierra el navegador web. |  |  |  |
| No permitir autenticaciones concurrentes con el mismo usuario a nivel del sistema o aplicación web. |  |  |  |
| A nivel sistema o aplicación se utilizan perfiles de usuarios con diferentes privilegios. |  |  |  |
| El sistema, aplicación o sitio web debe de utilizar el mínimo nivel de privilegios cuando accede a la base de datos. |  |  |  |
| Las cadenas de conexión a la base de datos no deben de estar incluidas en el código de la aplicación. Las cadenas de conexión a la base de datos deben de estar en un archivo de configuración separado en un sistema confiable y debería de estar encriptado. |  |  |  |
| El sistema, aplicación o sitio web utiliza librerías de terceros confiables. |  |  |  |
| El sistema, aplicación o sitio web cuenta con un mecanismo de bitácora para el registro de errores o incidentes |  |  |  |
| Si el sistema, aplicación o sitio web maneja información sensible o confidencial, se tiene habilitado un certificado SS/TSL 1.2 o superior |  |  |  |

## Aplicación final

| **Condición** | **Cumple**  **[Sí/No/No aplica]** | **Soporte documental** | **Observaciones** |
| --- | --- | --- | --- |
| Verificar que el código de testeo o cualquier funcionalidad que no sea considerado en producción, previo a realizar la puesta en producción, haya sido eliminado. |  |  |  |
| Se cuenta con los binarios: instaladores de software base, archivos de base de datos, scripts, archivos ejecutables y de configuración. |  |  |  |
| Se cuentan con las licencias del sistema operativo, RDBMS, servidor web/aplicaciones y lenguaje. |  |  |  |
| Se verificó que en caso de que el sistema, aplicación o sitio web conviva con otras aplicaciones en el mismo servidor no tendrá conflicto. |  |  |  |
| Se cuenta con manual de usuario final. |  |  |  |
| Se capacitó a los usuarios en el uso del sistema o aplicación web. |  |  |  |
| Se cuenta con documentación técnica del sistema (manual de instalación, diccionario de datos), aplicación o sitio web que será puesto en producción. |  |  |  |
| Se realizó la prueba del sistema, aplicación o sitio web en un entorno real con intervención del usuario final. |  |  |  |
| Se realizaron pruebas de carga/estrés considerando escenarios para los períodos críticos. |  |  |  |

## Infraestructura

| **Condición** | **Cumple**  **[Sí/No/No aplica]** | **Soporte documental** | **Observaciones** |
| --- | --- | --- | --- |
| La infraestructura de cómputo que soportará el servicio proporcionado por el sistema, aplicación o sitio web tiene la capacidad para soportarlo tanto en la operación normal como en los períodos críticos. |  |  |  |
| La infraestructura de cómputo tiene la capacidad para absorber actualizaciones que involucren nuevas funcionalidades, el volumen de información y el aumento de usuarios concurrentes. |  |  |  |
| El ancho de banda de la red puede soportar la transferencia de información en períodos críticos. |  |  |  |
| La infraestructura de cómputo, red y potencia eléctrica cuenta con elementos redundantes que ayuden a mantener la disponibilidad en el servicio. |  |  |  |
| Verificar que en el ambiente de producción donde residirá el sistema, aplicación o sitio web no tiene aplicaciones ajenas a su operación o aplicativos con los que requiera convivir. |  |  |  |
| La infraestructura de cómputo cuenta con las últimas actualizaciones a nivel sistema operativo, servidor web/aplicación y RDBMS. |  |  |  |

## Seguridad

| **Condición** | **Cumple**  **[Sí/No/No aplica]** | **Soporte documental** | **Observaciones** |
| --- | --- | --- | --- |
| Se revisaron que no existan puertos TCP y UDP abiertos y que no sean requeridos por el sistema, aplicación o sitio web. |  |  |  |
| No se tiene la configuración por defecto en el servidor web. |  |  |  |
| No se tiene la configuración por defecto en el RDBMS. |  |  |  |
| Las cuentas administrativas en el RDBMS han sido cambiadas por contraseñas fuertes. |  |  |  |
| No se tienen los ejemplos instalados en el RDBMS. |  |  |  |
| Deshabilite todas las funcionalidades innecesarias de la base de datos (por ejemplo: procedimientos almacenados innecesarios, servicios no utilizados, paquetes de utilidades, instale solo el conjunto mínimo de funcionalidades y opciones requeridas (reduce el área de ataque). |  |  |  |
| Se tiene deshabilitado la indexación por directorios. |  |  |  |
| El servidor web no muestra información sobre sí mismo. |  |  |  |
| Se deshabilitó register\_globals (PHP). |  |  |  |
| Se tiene deshabilitado el despliegue de errores del servidor web o del RDBMS en pantalla. |  |  |  |
| Se tienen habilitadas las bitácoras de error del sistema operativo, servidor web y RDBMS. |  |  |  |
| Se restringen las conexiones remotas al RDBMS. |  |  |  |
| Se tienen desactivados los algoritmos de cifrado débiles. |  |  |  |
| Se cuenta con seguridad física en el(los) servidor(es) que contiene el sistema, aplicación o sitio web. |  |  |  |
| Se cuenta con seguridad lógica en el(los) servidor(es) que contiene el sistema, aplicación o sitio web. |  |  |  |
| Se tiene restringido el acceso a las bitácoras (logs). |  |  |  |

## Gestión del servicio

| **Condición** | **Cumple**  **[Sí/No/No aplica]** | **Soporte documental** | **Observaciones** |
| --- | --- | --- | --- |
| Se tiene definido al dueño o responsable del servicio cuando esté en producción. |  |  |  |
| Se tienen definido el nivel requerido para el servicio y validado por el dueño del servicio. |  |  |  |
| Se tiene definido el impacto de una interrupción en el servicio. |  |  |  |
| Se tiene definido el tiempo máximo para la recuperación del servicio. |  |  |  |
| Se tiene definido el punto de recuperación para la información (cuánta información se puede perder). |  |  |  |
| Se tiene definida la información que será respaldada en el servicio. |  |  |  |
| Se tiene definido el periodo y tipos de respaldos a realizar. |  |  |  |
| Se tiene definido un procedimiento para el control de cambios en producción. |  |  |  |
| Se tiene considerado un plan de actualizaciones para el sistema operativo, servidor web/aplicación y RDBMS. |  |  |  |
| Se tiene registrado el nuevo servicio en un catálogo de la entidad o dependencia. |  |  |  |
| Se tienen identificados los períodos críticos en la operación del servicio (de mayor carga/demanda, impacto). |  |  |  |