TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLALNEPANTLA

INSTITUTO TECNOLÓGICO DE TLALNEPANTLA.

TECNOLOGÍAS DE SEGURIDAD EN SOFTWARE.

DOCENTE: DÍAZ RINCÓN HILDA.

ALUMNO Y N^{o} CONTROL:

ALDAMA MÁRQUEZ JOEL JAIR - 15251870.

GRUPO: T91.

ACTIVIDAD: 3.1 CONTROLES EN APLICACIONES EN PRODUCCIÓN

ANALISIS DEL DOCUMENTO ST-PT-01_V3_copia_controlada.pdf

La finalidad es establecer los lineamientos y definir los artefactos para la entrega en producción de todos los nuevos servicios de tecnología o sus actualizaciones, que faciliten su gestión, administración y mantenimiento.

Establecer y describir los lineamientos que se deben cumplir de las nuevas soluciones de tecnología (infraestructura, sistemas de información y/o servicios tecnológicos) del Ministerio de Educación Nacional.

El protocolo describe los lineamientos a cumplir para nuevas soluciones y actualizaciones y aplica desde el inicio de su implementación hasta la salida en productivo y entrega a la operación de la misma.

Se describen los roles que interactúan en el proceso, y las responsabilidades asociadas a cada uno:

- El Coordinador de Aplicaciones y/o Coordinador de Infraestructura es el encargado de asegurar la aprobación de paso a producción de las soluciones tecnológicas adquiridas.
- El líder técnico se encarga de coordinar con el proveedor de la solución la entrega acorde a los requisitos de este documento, se encarga de gestionar con el coordinador que corresponda, la aprobación para el paso a producción y se encarga de gestionar y coordinar con el proveedor o área funcional
- El Change Manager es el responsable de verificar la solicitud de paso a producción, de garantizar el flujo y ejecución del RFC
- El líder Funcional es el responsable de validar y dar conformidad al cumplimiento de los requerimientos funcionales.
- El operador se divide en 3 perfiles

- El especialista de Aplicaciones es el responsable de validar y dar conformidad a la aplicación y el encargado de hacer el despliegue de la aplicación en el ambiente de producción
- El especialista de Base de Datos es el responsable de validar y dar conformidad a la base de datos y se encargado de hacer el despliegue de base de datos en el ambiente de producción.
- El especialista de Seguridad es el responsable de verificar que la aplicación cumpla con las políticas de seguridad.

I. El proveedor es el responsable de la entrega de la solución actualizada o nueva.
II. El coordinador es el responsable de aprobar el pase a producción y es el administrador de verificar el cumplimiento del protocolo.
III. El líder técnico es el responsable de verificar el cumplimiento de protocolo
IV. El change manager y el operador son los informados que se verifico el cumplimiento del protocolo.
V. El usuario final es el que consulta la verificación del cumplimiento del protocolo.

Requisitos para la entrega de nuevas aplicaciones en productivo.

Se indican los requisitos que se deben cumplir para entregar en productivo las nuevas aplicaciones.

- ✓ Las pruebas funcionales y técnicas son de ambiente de certificación y producción.
- ✓ El inventario de aplicaciones son de ambiente de certificación y producción.
- ✓ Las fuentes o medios de instalación de la aplicación son de ambiente de certificación y producción.
- ✓ El manual técnico es de ambiente de producción.

- ✓ El manual de instalación tiene los 3 ambientes, que son de pruebas, certificación y producción.
- ✓ La Arquitectura de la aplicación es de ambiente de producción.
- ✓ El manual de usuario es de ambiente de producción.
- ✓ El diagrama entidad-relación es de ambiente de producción.
- ✓ El sizing es de ambiente de pruebas, certificación y producción.
- ✓ Las pruebas de carga y stress es de ambiente de certificación y producción.
- ✓ Las pruebas de seguridad es de ambiente de certificación y producción.
- ✓ Los backups es de ambiente de pruebas, certificación y producción.
- ✓ Los servicios monitoreados es de ambiente de certificación y producción.
- ✓ La categorización de la aplicación es de ambiente de producción.
- ✓ El licenciamiento es de ambiente de producción.
- ✓ Las cuentas y contraseñas de usuarios son de ambiente de certificación y producción.
- ✓ La gestión de vulnerabilidades es de ambiente de certificación y producción.
- ✓ La gestión de blacklog es de ambiente de certificación y producción.
- ✓ El plan de recuperación tecnológica es de ambiente de certificación y producción.
- ✓ IPV6 es de ambiente de pruebas, certificación y producción.
- ✓ Los tiempos de logueo para aplicaciones nuevas son de ambiente de certificación y producción.
- ✓ Los Diagramas DSI son de ambiente de pruebas, certificación y producción.
- ✓ El ingreso al almacen es de ambiente de pruebas, certificación y producción.
- ✓ La actualización de lina base APP es de ambiente de certificación y producción.
- ✓ La actualización de archivos en la intranet es de ambiente de certificación y producción.

A continuación, se indican los requisitos que se deben cumplir para entrega a productivo de nueva infraestructura tecnológica.

1. Inventario: Entregar el inventario o relación de la infraestructura con mínimo los siguientes ítems:
   a) Marca
   b) Modelo
   c) Cantidad
   d) Descripción
   e) Modelo
   f) Estado
   g) Fabricante
   h) Ubicación física
   i) # de placa, etc.
   j) Relación de VPNs existentes indicando usuario rol y permisos de acceso.
   k) CMDB actualizada a la fecha de entrega en la herramienta CA.
2. Manuales Técnicos: Garantizar que en este documento estén contemplados como mínimo los aspectos técnicos de la infraestructura como:
   a) Tipos de garantía
   b) Niveles de escalamiento
   c) Instructivo del soporte técnico (forma de operar), si lo tiene, los servicios ofrecidos y en general la forma de administrar cada elemento.
3. Manuales Administración: El documento debe contener instructivos para la administración del elemento según su rol.
4. Ingeniería: En este documento debe contener la arquitectura detallada así:
   a) Arquitectura de la solución (esquema de red (físico y lógico, vlans, etc.), equipos de seguridad, balanceo.
   b) Descripción de capa media entre otros) de la solución a nivel donde se puede identificar cada componente.

c) Direccionamiento IP,
d) Tablas de rutas
e) NAT público
f) Mapeo de servicios
g) Plan de capacidad proyectado a 3 años

5. Aseguramiento de infraestructura: Entregar inventario de los dispositivos de seguridad y la evidencia de las pruebas de seguridad realizadas por el área de seguridad, para garantizar que NO se tiene vulnerabilidad, en caso de que existiera, garantizar que estas se encuentren documentadas y argumentadas.
6. Backups de configuración: Entregar los Backups en medio magnético, los archivos de configuración de cada uno de los elementos que componen la solución.
7. Backups: Entregar la política de Backups y sus tiempos de retención, manuales de administración de la herramienta de Backups (librería y aplicación), en la que se indica:
   a) Cuál es la frecuencia
   b) Tipos de Backups
   c) Tiempos de retención
   d) Rutas de almacenamiento
   e) Inventario de medios de almacenamiento.
   f) Lineamientos de custodia.
8. Servicios Monitoreados: Definir cuáles son los elementos que deben ser monitoreados:
   a. Puertos de monitoreo
   b. Dispositivos y URLs. Por cada componente de la solución
9. Cuentas y contraseñas de Usuarios: Entregar los usuarios y contraseñas en sobre sellado de: ROOT, Administrador, y consulta.
10. Capacity Planing; Análisis y estadísticas de uso de los recursos que componen la solución
11. Licenciamiento: Entregar los acuerdos de licenciamiento suscritos con los proveedores de Hardware y software que compone la solución.
12. Garantía: Contratos de soporte y garantía de cada elemento de la solución.

13. Gestión de Vulnerabilidades: Entregar informe de los últimos tres (3) meses del escaneo de vulnerabilidades y mitigación pertinente de la plataforma a entregar.
14. Gestión de Backlog: Gestionar y dar cierre al backlog para los procesos de: gestión de cambios, gestión de incidentes, gestión de problemas y gestión de solicitudes asociadas a la infraestructura a entregar.
15. Plan de Recuperación Tecnológica: Entregar documentación con el plan de recuperación ante una indisponibilidad en donde se evidencie el procedimiento de cómo se debe realizar su recuperación.
    a) Introducción
    b) Objetivos
    c) Alcance
    d) Fecha de realización
    e) Metodología utilizada
    f) Resumen ejecutivo
    g) Procedimiento de recuperación
    h) Tiempos de recuperación
16. IPV6: Configuración dentro de la infraestructura del protocolo IPV6.
17. Arquitectura: Entrega de la arquitectura en donde se asegure un esquema de alta disponibilidad y full tolerancia.
18. Ingreso a Almacén: Entregar el certificado de ingreso a almacén del Ministerio.

Se indican los requisitos que se deben cumplir para entregar el nuevo servicio a la mesa de ayuda.

- Capacitación
- Matriz de escalamiento
- Árbol de tipificación de la herramienta de gestión
- Catálogo de Servicios
- Tiempo de respuesta.
- Base de Datos del conocimiento.