CORPORACIÓN GILBERTO ECHEVERRI MEJÍA

ANEXO 3

POLITICAS DE ADMINISTRACIÓN DE LOS AMBIENTES DE LAS PLATAFORMAS EN LA CORPORACIÓN GILBERTO ECHEVERRI MEJÍA

Versión 1

2024

INTRODUCCIÓN

En una organización, la gestión de la seguridad de la información puede resultar compleja y difícil de llevar a cabo. Esto se debe no solo a razones técnicas, sino también a razones organizativas que involucran la coordinación de todos los esfuerzos dirigidos hacia el aseguramiento de un entorno informático institucional. Para lograr esto, es fundamental la administración adecuada de recursos humanos y tecnológicos, donde se requiere un control adecuado que integre los esfuerzos y conocimientos humanos con las técnicas depuradas de mecanismos automatizados, evitando así que el ambiente se vuelva desordenado y confuso. Por lo tanto, es necesario emplear mecanismos reguladores de las funciones y actividades desarrolladas por cada persona vinculada con la Corporación Gilberto Echeverri Mejía.

La política de uso de ambientes tiene como objetivo establecer las medidas técnicas y organizativas necesarias para garantizar la seguridad de todas las plataformas utilizadas en la Corporación Gilberto Echeverri Mejía, así como de las personas que interactúan haciendo uso de los servicios asociados a ellas.

Este documento describe la política de uso de ambientes de trabajo definidas por la Corporación Gilberto Echeverri Mejía. Para su elaboración, se toman como base las leyes y demás regulaciones aplicables. Las políticas incluidas en este manual son parte fundamental del sistema de gestión de seguridad de la información de la Corporación Gilberto Echeverri Mejía, y sirven como base para la implementación de los controles, procedimientos y estándares definidos.

1. Objetivo

La presente política tiene como propósito dar a conocer los requisitos básicos de operación para establecer controles efectivos sobre todas las actividades que se desarrollan en los sistemas la CORPORACIÓN GILBERTO ECHEVERRI MEJIA, con el fin de que todos los involucrados en la operación, manejo y consulta garanticen la confidencialidad, integridad y disponibilidad del sistema.

2. Alcance

La política de uso de ambientes cubre todas las actividades administrativas y de control que deben seguir los empleados y colaboradores que tengan relación o hagan uso de los sistemas de la Corporación

3. Políticas Generales

Como política general se estable que:

1. Los lineamientos funcionales de los ambientes están bajo el control de la oficina TIC, sin importar por cual sea el área que usa la herramienta
2. Las mejoras funcionales o nuevos requerimientos deben ser solicitados por el supervisor o el administrador del sistema, mediante la mesa de ayuda de la oficina TIC
3. El seguimiento de incidencias se realizará a través de la mesa de servicios de TI.
4. Las solicitudes de mejoras funcionales o nuevos requerimientos deben ser registradas en la mesa de servicios.
5. Las funcionalidades complementarias al objeto misional de la aplicación pueden estar bajo el dominio de un supervisor diferente al administrador del sistema.
6. Los usuarios líderes tienen control sobre el acceso a las funcionalidades complementarias de las que son responsables.
7. Los usuarios líderes pueden solicitar cambios y mejoras de la aplicación, pero deben contar con la aprobación del supervisor, administrador o del propietario del sistema.

4. Gestión de Configuración y Control de Cambios

El profesional de sistemas debe realizar la planificación de las actividades que se llevarán a cabo en un ambiente controlado durante el soporte y mantenimiento del sistema. Esta planificación debe permitir el gerenciamiento de la configuración de software para establecer un sistema formal de control de cambios y versiones. Se debe definir un ambiente controlado donde se almacenará, modificará los elementos de la línea base del sistema.

Debe establecer un lugar específico, un "ambiente controlado", donde pueda trabajar con seguridad en los elementos básicos del sistema. Esto garantiza que cualquier cambio se haga de manera segura y ordenada.

En ese mismo ambiente controlado, debe mantener una copia fiel del sistema principal, la "línea base". Cualquier cambio en esta línea base solo se hará después de una aprobación formal, para asegurarse de que todo se mantenga estable y funcione correctamente.

Su trabajo también implica seguir de cerca cada cambio que se haga en el sistema. Desde que se solicita un cambio hasta que se aprueba e implementa, es su responsabilidad asegurarse de que todo el proceso se lleve a cabo correctamente. Esto garantiza que el sistema siga funcionando sin problemas.

La naturaleza de los cambios se define:

Funcionales: cuando se modifica un requerimiento de la línea base del sistema o se genera un nuevo requerimiento.

Tecnológicos: cuando se cambia o actualiza la versión de algún componente como, Sistema operativo, web server o aplication server, motor de base de datos, framework o lenguaje de programación.

Infraestructura: cuando se realiza una modificación o cambio de, servidores físicos, servidores virtuales, enrutamiento, dns, etc.

Se debe garantizar el registro de solicitudes de cambio.

El profesional de sistemas liderara el comité de cambios donde se analizarán los cambios y se dejara evidencia de la evaluación.

El profesional de sistemas deberá evidenciar la aprobación o rechazos de cambios posterior a la evaluación del comité de cambios.

Los cambios aprobados deberán contar con un plan de implementación, el cual debe considerar tiempos de implementación y baja del servicio si aplica, comunicación a los interesados y proceso de recuperación del estado anterior o rollback.

5. Control de accesos

En cada uno de los ambientes de la corporación se definen los tipos de perfiles de acceso a las plataformas

Los usuarios externos están conformados por beneficiarios o aspirantes a ser beneficiarios, el acceso es otorgado por el proceso funcional de la aplicación de forma automática y solo es autorizado a autogestionar su información.

Los usuarios internos están conformados por empleados o contratistas de la Corporación.

La autorización de los usuarios internos se define en cada aplicación según la política de seguridad de la información.

La solicitud de acceso y autorización debe ser realizada por el responsable directo del empleado en el momento del alta, cambio de funciones o promoción.

La solicitud de acceso y autorización debe ser realizada por el supervisor directo del contratista al inicio de la ejecución del objeto contractual

Las solicitudes de acceso y autorización, para empleados y contratistas deben ser realizadas a través de la herramienta de gestión de servicios de TI.

Cada solicitud de acceso y autorización debe ser aprobada por el administrados del sistema.

La baja de un empleado o terminación de un contrato debe ser notificada por el responsable directo del empleado o el supervisor de contrato a través de la herramienta de gestión de servicios de TI, antes de la culminación de las labores del usuario indicando la fecha de terminación, este usuario quedara inactivo en el sistema al finalizar la jornada laboral.

Se debe tener un formato para describir los accesos de los usuarios en cada una de las plataformas de la Corporación

6. Aplicación

Este documento, donde se suscriben las políticas de separación de ambientes, control de cambios y paso a producción, aplica a todo el personal de la Corporación y activos de información.

7. Roles y responsabilidades

Profesional de sistemas:

1. Responsable de implementar y actualizar las políticas de manejo de ambientes y control de versiones.
2. Encargado de realizar los requerimientos a las empresas encargadas del soporte de las aplicaciones.
3. Se encarga de interpretar y realizar casos funcionales de las solicitudes realizadas por los usuarios.
4. Solicita los manuales y documentar las versiones.

5. Ejecuta Planes de Pruebas y asegura la calidad.
6. Realiza ajustes necesarios durante las pruebas.

Tecnólogo en infraestructura:

1. Revisar y planificar la configuración de ambientes según la arquitectura empresarial definida por el área de sistemas.
2. Crea, ejecuta, instala y mantiene los ambientes.
3. Garantiza la disponibilidad, integridad y confiabilidad de las plataformas.

Contratistas de desarrollo, soporte y mantenimiento:

1. Una vez analizados los requerimientos, elaborar el diseño del sistema con los estándares establecidos.
2. Desarrollan los requerimientos entregados por el cliente, interno o externo.
3. Redactar manuales y documentar las versiones.
4. Instalar los sistemas en el ambiente de desarrollo correspondiente.
5. Ejecutar Planes de Pruebas y aseguran la calidad.
6. Realizar ajustes posteriores a las pruebas según sea necesario.

Usuarios:

1. Ejecutar Planes de Pruebas en el ambiente de Control de Calidad (QA).
2. Dejar constancia de la aceptación de los cambios solicitados

8. Separación de diferentes Ambientes (Desarrollo, Pruebas y Producción)

Ambientes existentes en la Corporación:

Ambiente de Producción: Es la plataforma tecnológica destinada a alojar los Sistemas de Información que la corporación utiliza para respaldar sus procesos misionales o de soporte operativo. Aquí se ejecutan las aplicaciones en uso real por los usuarios finales.

Ambiente de Pruebas: Estos ambientes alojan los sistemas de información recién desarrollados o personalizados para que sean evaluados por los usuarios finales en términos de funcionalidad, y por el equipo de infraestructura para realizar pruebas de rendimiento y seguridad. Las pruebas en este ambiente son la última etapa antes de pasar a la implementación y puesta en producción de los sistemas.

Ambientes de Desarrollo: Estos ambientes proporcionan entornos para el desarrollo de nuevas implementaciones, mejoras o modificaciones de código, ya sea para corregir errores o para optimizar el funcionamiento de las aplicaciones. También se utilizan para instalar software propietario que debe ser personalizado para su uso posterior en la corporación.

Para garantizar la seguridad y eficiencia en los diferentes ambientes de sistemas, se deben implementar las siguientes medidas:

Separación de red: Cada ambiente debe tener segmentos de red separados, con grupos de direcciones IP distintos. Esto ayuda a prevenir la interferencia entre los ambientes y limita el acceso no autorizado.

Separación de bases de datos: Se debe mantener una separación de las bases de datos según el ambiente. Cada ambiente debería tener su propia instancia de base de datos, lo que facilita la gestión y evita posibles conflictos o pérdidas de datos.

Separación de roles y seguridad:

Se deben asignar roles de seguridad específicos para cada ambiente y gestionar las transiciones entre ellos de manera controlada.

Ambiente de Desarrollo: Los roles de seguridad están a cargo de la empresa contratista que desarrolla o personaliza las aplicaciones. El acceso está restringido al personal autorizado de la empresa contratista.

Ambiente de Pruebas: Los roles de seguridad son gestionados por el área de sistemas y los usuarios encargados de realizar pruebas. El acceso se limita al personal autorizado para pruebas.

Ambiente de Producción: Los roles de seguridad son responsabilidad de los usuarios finales y clientes. El acceso se restringe a los usuarios finales autorizados y se implementan medidas de seguridad adicionales para proteger los datos y el funcionamiento del sistema en producción.

Planificar detalladamente las etapas de paso a producción es fundamental para garantizar una implementación exitosa de cambios en el ambiente de producción. Aquí hay un desglose de las actividades que deben considerarse en este proceso:

Respaldos: Realizar copias de seguridad completas y verificadas de todos los datos y configuraciones relevantes antes de realizar cualquier cambio en el ambiente de producción. Estos respaldos son críticos en caso de que sea necesario revertir el cambio (rollback) por cualquier motivo.

Recursos: Asegurar de que se disponga de los recursos necesarios, como hardware, software, personal capacitado y tiempo suficiente, para llevar a cabo la implementación de manera efectiva y sin contratiempos.

Conjunto de pruebas pre-instalación: Realizar pruebas exhaustivas en un ambiente de pruebas que simule el ambiente de producción para verificar la funcionalidad y estabilidad del cambio propuesto. Esto incluye pruebas de integración, pruebas de rendimiento, pruebas de seguridad y cualquier otro tipo de prueba relevante.

Criterio de aceptación del cambio: Establecer criterios claros y objetivos que determinen cuándo el cambio propuesto está listo para ser implementado en el ambiente de producción. Esto puede incluir la validación de pruebas exitosas, revisión por parte de partes interesadas clave y cumplimiento de estándares de calidad.

Plan de rollback: Desarrollar un plan detallado y documentado que describa cómo revertir el cambio en caso de que surjan problemas durante la implementación o después de ella. Esto puede incluir instrucciones paso a paso, roles y responsabilidades del personal involucrado, y los criterios que indican cuándo activar el plan de rollback.

Conjunto de pruebas post-instalación: Realizar pruebas adicionales después de la implementación en el ambiente de producción para confirmar que el cambio se ha realizado correctamente y que no ha causado efectos secundarios no deseados. Esto puede incluir pruebas de funcionalidad, pruebas de regresión y monitoreo de la estabilidad del sistema.

Implementación: Ejecutar el cambio en el ambiente de producción siguiendo el plan detallado y siguiendo los procedimientos establecidos. Esto debe hacerse con precaución y siguiendo las mejores prácticas de seguridad y control de cambios.

Al planificar detalladamente cada una de estas etapas, se puede minimizar el riesgo de interrupciones y problemas durante el paso a producción, garantizando una implementación exitosa del cambio propuesto.

Para garantizar una gestión efectiva de los entornos de sistemas, es importante tener en cuenta varios aspectos para diferenciar cada entorno:

- Separación de equipos y sistemas operativos
- Niveles de pruebas y datos asignados
- Controles de acceso diferenciados
- Configuración de perfiles de usuario y ambiente

9. Otras consideraciones

- Mantener la confidencialidad de las contraseñas con privilegios superiores en los sistemas en producción, tanto por la oficina TIC como por el personal contratista.
- Custodiar las credenciales de acceso de todos los Activos de Información de la Corporación, tarea asignada al Encargado de Seguridad de la Información.
- Probar los cambios a los sistemas y aplicaciones en un entorno de pruebas antes de aplicarlos a los sistemas en producción, a menos que existan circunstancias excepcionales aprobadas por el profesional de sistemas.
- Restringir el acceso a compiladores, editores y otras herramientas de desarrollo desde los sistemas de producción.
- Utilizar distintos perfiles de usuario para acceder a los sistemas en producción y en entornos de pruebas.
- Identificar claramente los ambientes de pruebas y desarrollo en todas sus pantallas e interfaces.
- Evitar copiar datos sensibles en los entornos de pruebas o desarrollo a menos que se implementen controles de seguridad equivalentes para cada ambiente.

Prohibiciones:

- Prohibir escribir o modificar código auto copiante o cualquier otro tipo de código malicioso.
- Evitar incluir funciones u operaciones no documentadas o no autorizadas en el desarrollo.
- No modificar programas sin dejar registro en un documento de cambio.

Obligaciones

- Registrar la generación de código fuente en el repositorio correspondiente para garantizar la trazabilidad de las modificaciones.
- Proteger el acceso al código fuente de los distintos sistemas mediante contraseñas seguras, según la política de seguridad de la información.
- Dar acceso a los desarrolladores externos solo durante el período que dure el contrato y/o proyecto.
- Establecer un repositorio de código fuente único y controlado para los sistemas propios de la Corporación.
- En caso de ser aplicable, entregar las credenciales al gestor de contenido.
- Información sobre herramientas de desarrollo:
- Proporcionar información sobre las herramientas utilizadas en el desarrollo y manipulación del código.
- Incluir pruebas de integración (instalación, almacenamiento, configuración, seguridad, recuperación ante errores), pruebas funcionales y de rendimiento. Documentar estos registros.
- Mantener un control de acceso igual de estricto que en el ambiente de producción, según la política de seguridad de la información.
- Suministrar información sobre la arquitectura utilizada para el desarrollo de la plataforma.
- Como control final, tener en cuenta la aplicabilidad de la política de seguridad de la información en todos los ambientes mencionados y en los casos que sea necesario implementarla.

10. Auditoria para los sistemas en la Corporación

Para garantizar una correcta auditoria de las diferentes plataformas con las que se cuenta en la Corporación, mínimamente se deben tener en cuenta los siguientes criterios

Objetivo: En el cual se debe describir para que se realiza el proceso de auditoria

Alcance: se debe definir los temas que se desean abarcar en el proceso de auditoria

Roles: Se describen los tipos de usuarios que se tienen en la aplicación

Descripción y alcance de roles: se identifica las funciones y tipos de permisos de cada uno de los roles

Usuarios: se deben describir cada uno de los usuarios que se tienen creados en la plataforma y su estado

Módulos: se describen los módulos que existen dentro de las plataformas

Información: se describe toda la información correspondiente al objetivo de la auditoria

Conclusión: se debe informar cuales fueron los hallazgos que fueron encontrados y las posibles soluciones que se presentan desde el área TIC

Juan Camilo Díaz Valderrama
Profesional universitario oficina TIC