**Política de Seguridad en procesos de desarrollo y soporte**

Se debe asegurar la revisión de todo cambio al sistema para comprobar que no debilite su seguridad

1. **Procedimientos de control de cambios.**
   1. Se debe implementar procesos formales de cambio que debe considerar lo siguiente:
      * Los cambios de realizaran solo por usuarios autorizados.
      * Mantener un registro de los niveles de autorización
      * Mantener un control de versiones de toda actualización software.
      * Mantener un seguimiento de auditoria de toda petición de cambio.
2. **Revisión técnica de los cambios en el sistema operativo**
   1. Se debe garantizar que las modificaciones en el sistema operativo por lanzamiento de parches o actualizaciones del proveedor no comprometan el sistema.
   2. Monitorear las vulnerabilidades de las actualizaciones en el sistema operativo.
3. **Restricciones en los cambios de paquetes de software**
   1. Las modificaciones en los paquetes de software suministrados por proveedores deberán ser controladas y en lo posible evitadas.
   2. Se debe guardar el software original y los cambios realizados, así como documentar los cambios realizados.
4. **Fuga de información**
   1. Se debe monitorear regularmente las actividades del personal y el uso de los recursos en sistema de cómputo.
5. **Desarrollo externo del software**
   1. Se debe considerar los requisitos contractuales sobre calidad y funcionalidad segura del código.
   2. Establecer acuerdos bajo licencia, propiedad del código y derechos de propiedad intelectual.
   3. Probar el software antes de la implementación para detectar el código troyano o backdoors.