|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Asunto:** | | **Comité De Cambios –** Instalación Anti-Malware Servidores COAC 29 de Octubre | | | | | | | | | | |
| **Lugar:** | Sala de reuniones Riesgos | | **Fecha:** | | | 23/07/2019 | **Hora Inicio**: | 16h40 | | **Hora Fin:** | | 17h20 |
| 1. **Objetivo(s):** | | | | | | | | | | | | |
| * Analizar y aprobar el control de cambios levantado por el área de Seguridad de la Información, para ejecutar la instalación del software Anti-Malware, en todos los servidores de la Cooperativa. | | | | | | | | | | | | |
| 1. **Desarrollo:** | | | | | | | | | | | | |
| * + Xavier Albán da comienzo al comité de cambios, indicando que esta es una segunda revisión al control, ya que en un inicio se había levantado observaciones a la documentación presentada por Santiago Hernández, se indica que se tiene un cronograma actualizado, en el cual se tiene el detalle del Responsable de la instalación, la criticidad, y el ambiente al cual pertenece cada servidor.   + También se expone que en este cronograma de instalación se está iniciando con los servidores de desarrollo, el cual es una buena estrategia, ya que de presentarse una indisponibilidad el riesgo se minimiza y se podría manejar de mejor manera.   + Se indica que en el cronograma de instalación se está tomando la última semana de julio para la instalación en servidores de producción, y que también se está tomando en cuenta el viernes 9 de agosto, mismo que está considerado como feriado nacional, y que por proceso de control de cambios estas fechas deben ser aplazadas, ya que no se permite realizar cambios en las mismas.   + Se analiza cada uno de los servidores, tanto de Desarrollo, como de Producción, y se identifica que los servidores de desarrollo solo se tienen Linux, por lo que se debe considerar un servidor que tenga SO. Windows, de producción, mismo que no debe ser crítico, para considerarlo como piloto y poder monitorear el comportamiento de los mismos luego de la instalación del software.   + Omar Redroban pregunta telefónicamente a Cesar Fonseca, quien será la persona por parte del área de Gestión Técnica que dará soporte a la desinstalación del antivirus que se encuentra actualmente instalado en los servidores, por lo que Cesar menciona que la persona encargada será Omar Gaibor.   + Se define que para la instalación del Anti-Malware en los servidores del ambiente de desarrollo se lo realizará durante el día, y para los ambientes de producción, en servidores no críticos de lunes a viernes desde las 15:00, con un total de 5 servidores por día, y para los servidores de producción críticos, los días sábados desde las 17:00.   + Omar Redroban expone que una posible maquina con la cual se puede iniciar, y que se encuentra dentro del ambiente de Producción es la EQP\_DBA, mismo que pertenece a una máquina que se utiliza para conexiones a las Bases de Datos.   + Patricia Chicaiza indica que no se tendría problema, siempre y cuando se notifique para dar aviso al proveedor que se puede tener intermitencia o desconexión a la misma, y tener otra estrategia de trabajo.   + Omar Redroban también expone que un servidor de producción que no es crítico, ya que actualmente es ocupado solamente por el área de Control de Cambios es el servidor de iTop, por lo que se sugiere tomar ese para el piloto.   + Se llega a la conclusión que se tomará un servidor de desarrollo (Linux) y un servidor de Producción (Windows) como piloto de la instalación, se debe monitorear el comportamiento de cada uno de los servidores durante la siguiente semana, mientras se realiza la instalación en el resto de servidores de desarrollo, el mismo debe ser realizado mediante las herramientas VMWare, mismos que permiten revisar si se tiene problemas con algún componente de cada servidor   + Patricia Chicaiza alerta al comité que en la lista del cronograma de instalación existen IP’s duplicadas, y que se deben revisar, ya que no se pueden tener servidores con la misma IP.   + Se indica al comité, que para los servidores de desarrollo se notificará al área de Gestión de Aplicaciones la posible indisponibilidad durante de la desinstalación del antivirus e instalación del antimalware   + Se solicita a Santiago Hernández que se debe depurar el archivo, ya que en el mismo se encuentran servidores que ya tienen instalado el software, también se debe revisar nuevamente el archivo para revisar las IP’s duplicadas, y se solicita que luego de esta depuración se añada una columna en la que Patricia Chicaiza indique si el servidor tiene base de datos o no, ya que de necesitar el reinicio del servidor, primero de debe desconectar de la Base.   + Se llega a la conclusión que el día 24/07/2019 se instalará el Anti-Malware en el servidor iTop (132.147.10.126) de producción, y en el servidor CERTIFICACION29 (132.147.10.177) de desarrollo, como un piloto y poder monitorear el comportamiento de cada uno de estos. | | | | | | | | | | | | |
| 1. **Acuerdo(s):** | | | | | | | | | | | | |
| Actividad | | | | | Responsable | | | Fecha Inicio | | | Fecha Fin. | |
| Depurar el archivo de cronograma para eliminar servidores con el antimalware ya instalado, y duplicidades en las IP de los servidores | | | | | Santiago Hernández  Omar Redroban | | | 24/07/2019 | | | 31/07/2019 | |
| Añadir la columna que indique si el servidor posee Base de Datos o no | | | | | Santiago Hernández  Omar Redroban  Patricia Chicaiza | | | 24/07/2019 | | | 31/07/2019 | |
| Desinstalación del antivirus actual, según el cronograma | | | | | Omar Gaibor | | | 24/07/2019 | | | 14/08/2019 | |
| Acceso al proveedor, a los servidores para la instalación del software | | | | | Omar Gaibor | | | 24/07/2019 | | | 14/08/2019 | |
| Inicio de instalación en servidor iTop y Desarrollo y realizar el monitoreo | | | | | Omar Gaibor  Xavier Albán  Proveedor | | | 24/07/2019 | | | 02/08/2019 | |
| 1. **Participantes:** | | | | | | | | | | | | |
| Nombre | | | | Cargo | | | | | Firma | | | |
| Omar Redroban | | | | Analista Gestión Técnica | | | | |  | | | |
| Santiago Hernández | | | | Analista Seguridad de la Información | | | | |  | | | |
| Patricia Chicaiza | | | | DBA | | | | |  | | | |
| Hugo Chanatasig | | | | Analista Riesgo Operativo | | | | |  | | | |
| Xavier Albán | | | | Analista Control de Versiones y Calidad | | | | |  | | | |