|  |  |  |
| --- | --- | --- |
| **Id. 14** | |  |
| **Riesgo** | | Ingreso de Software Malicioso que ocasione Pérdida de información o robo de la misma |
| **ESTRATEGIAS** | **Evitar** | |
| 1. Bloquear puertos del servidor que no se utilicen.  VENTAJA: imposibilita la fuga de información  DESVENTAJA: habilitar y deshabilitar de forma recurrente los puertos para su uso | |
| **Aceptar** | |
| 1.Detener la comunicación con el servidor  VENTAJA: Evita la propagación del malware y reduce el daño  DESVENTAJA: Problemas de performance | |
| **Transferir** | |
| 1. Subcontratar una empresa que realice el almacenamiento y la gestión de activos de información  VENTAJAS: desvincular a la organización del control de activos  DESVENTAJAS: se transfiere el riesgo a la gestión de contratos con terceros | |
| **Mitigar - Minimizar Probabilidad** | |
| 1.Analizar frecuentemente estado del servidor  VENTAJA: Permite detectar si el servidor es vulnerable a ataques de Malware  DESVENTAJA: Puede ocasionar inaccesibilidad a tareas de los empleados | |
|  | **Mitigar - Minimizar Impacto** | |
|  | 1.Realizar Backups significativos durante intervalos de tiempos cortos  VENTAJA: Nos da la posibilidad de tener la información más importante actualizada y resguardada.  DESVENTAJA: Límite de tamaño, deberemos de establecer una estrategia de copia diaria que se acomode al ancho de banda y el tiempo disponible para ello. | |
| **CONTROLES** | 1.Seguridad de las Operaciones incorporando Registro de Actividad y Supervisión – Registro y Gestión de  Eventos de Actividad.  Evidencias Objetivas: Regular el estado de nuestro activo controlando el trafico entrante y saliente  2. Seguridad Física y Ambiental teniendo en cuenta Áreas Seguras – Protección contra amenazas externas  Evidencias objetivas: Revisiones periódicas del estado de las instalaciones.  3.Gestion de Activos: Clasificación de la Información – Manejo de los soportes de almacenamiento  4. Seguridad en las Telecomunicaciones: Gestión de servidor en las redes – Intercambio de información con partes externas.Evidencias Objetivas: Control de medios extraíbles y analizar previamente. | |
| **Riesgo Residual** | | |
| Con el bloqueo de puertos se ha disminuido la severidad del riesgo en función de evitar el ingreso de la amenaza y así disminuir su impacto impacto. Por tal motivo La probabilidad de que esta amenaza afecte en su totalidad al servidor es baja.  Con respecto a la aceptación puede darse que la detención de comunicación al activo no sea no se dé rápidamente imposibilitando la de detección.  En el caso de Transferencia:  Se debe realizar el cálculo del riesgo transferido al subcontratar otra empresa.  En caso de mitigación: se reduce la posibilidad ante posibles amenazas analizando el servidor periódicamente, sin embargo, existe el riesgo de que durante el proceso de análisis no sean captadas todas las posibles amenazas por tal motivo se deberá analizar el riesgo residual del mismo.  El impacto en la integridad del activo debería ser llevado a cabo dentro de planes de recuperación logrando definir todo tipo de documentación que quiera ser resguardada, puede ser que se pierda información específica de la empresa al no tener en claro que tipo de información se considera relevante, teniendo en cuenta esto, el impacto sería de menor magnitud. | | |

|  |  |  |
| --- | --- | --- |
| **Id. 20** | |  |
| **Riesgo** | | El ingreso de software malicioso puede generar fallas en la conexión al servicio de internet imposibilitando su uso y de las aplicaciones que lo usen |
| **ESTRATEGIAS** | **Evitar** | |
| 1.Declarar un permiso exclusivo para que el administrador sea el único con manejo de la placa de red.  VENTAJA: Ningún malware podrá inhabilitar la placa red sin autorización del Administrador  DESVENTAJA: Ningún usuario podrá inhabilitar intencionalmente la placa red sin autorización del Administrador | |
| **Aceptar** | |
| 1.Detectar rápidamente el malware y eliminar el mismo  VENTAJA: Evitar daños mayores  DESVENTAJA: Posible no detección del malware. | |
| **Transferir** | |
| 1.Llevar a servicio técnico tercerizado el equipo  VENTAJA: Respuesta de personal específicamente capacitado  DESVENTAJA: Gastos económicos y demoras en la reparación. | |
| **Mitigar - Minimizar Probabilidad** | |
| 1.Capacitacitar al personal que utiliza dichos equipos en materia de seguridad de la información  VENTAJA: Evitar descargas indebidas  DESVENTAJA: Gastos económicos para el sanatorio. | |
|  | **Mitigar - Minimizar Impacto** | |
|  | 1.Reportar al área de sistemas el conflicto.  VENTAJA: Solución rápida.  DESVENTAJA: El área de sistemas no sea capaz de resolver el problema. | |
| **CONTROLES** | 1.Seguridad de las Operaciones incorporando Registro de Actividad y Supervisión – Registro y Gestión de  Eventos de Actividad.  Evidencias Objetivas: Regular el estado de nuestro activo controlando el trafico entrante y saliente  2. Seguridad Física y Ambiental teniendo en cuenta Áreas Seguras – Protección contra amenazas externas  Evidencias objetivas: Revisiones periódicas del estado de las instalaciones.  3. Control de Acceso: Gestión de acceso de usuario – Responsabilidad de usuario – Control de acceso a sistemas  Evidencias objetivas: Administrar permisos de usuarios, y prioridad de acceso. | |
| **Riesgo Residual** | | |
| Con las estrategias presentadas se ha disminuido la severidad del riesgo en función de evitar que el riesgo se propague y tenga mayor impacto impacto.  La probabilidad de que esta amenaza se interfiera en su totalidad a raíz de haber aumentado considerablemente el riesgo de permisos en equipos y de detección es relativamente baja.  La severidad calculada del riesgo residual puede ocupar diferentes estados, pero no justifica la realización de otras estrategias para su reducir el riesgo.  En el caso de Transferencia:  Se debe realizar el cálculo del riesgo transferido a un servicio técnico tercerizado.  En caso de mitigación: se reduce la posibilidad al capacitar al personal ante posibles amenazas, sin embargo, existe el riesgo de que el personal no actué según las acciones requeridas de tal modo se deberá analizar el riesgo residual del mismo. | | |