Universidad Mariano Gálvez de Guatemala

Facultad de Ingeniería en Sistemas de Información y Ciencias de la Computación

Dirección de Posgrados

SEGURIDAD Y AUDITORIA DE SISTEMAS

|  |  |
| --- | --- |
| Alumno: Wilder Esau García Barrera | Carné: 2990 13 2941 |
| Alumno: Oscar David Tizol | Carne:2990 14 1638 |

Para el caso presentado realice un análisis de riesgos

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Id Riesgo. | Amenaza | Impacto | Probabilidad | C | I | D |
| 1 | Exposición de información de reportes de venta | 4 | 4 | x | x |  |
| 2 | Mal diseño de infraestructura de red | 4 | 3 |  | x | x |
| 3 | Degradación en el servicio del sistema  (cuando el sistema se satura) | 5 | 4 |  | x | x |
| 4 | No tener servidores de respaldo | 5 | 3 |  |  | x |
| 5 | Falta de seguridad de servidores | 4 | 2 |  | x | x |
| 6 | Errores de facturación | 3 | 3 |  |  | x |
| 7 | Contraseña con estructura no definida | 2 | 3 | x | x |  |
| 8 | Falta de renovación de telefonía | 3 | 3 |  |  | x |
| 9 | Falta de trazabilidad de transacciones de los usuarios | 5 | 4 | x | x |  |
| 10 | Personal insuficiente en ventas | 3 | 4 |  |  | x |
| 11 | Roles y permisos no definidos | 4 | 4 | x | x |  |
| 12 | Grupo de dominio no definido | 5 | 5 | x | x |  |
| 13 | Robo de información de proveedores | 4 | 4 | x | x |  |
| 14 | Diseño del sistema mal estructurado | 3 | 5 | x | x | x |
| 15 | Falta de recepción de información de correos | 5 | 4 |  |  | x |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. Identifique las opciones de tratamiento de riesgo para cada riesgo identificado en inciso anterior Iso 27002:

|  |  |  |
| --- | --- | --- |
| Id Riesgo. | Opción de tratamiento de riesgo | Control (es) |
| 1 | Reducción de Riesgo | Definición de Roles (Rol Gerencia será el único que podrá tener acceso a Información Financiera |
| 2 | Transferencia Riesgo | Contratación de Empresa o Entidad (Adquisición Servicio Diseño e Implementación de Infraestructura de Red) |
| 2 | Reducción de Riesgo | Contratación Empresa o Entidad Semestralmente (Adquisición Servicio para Personal Técnico/TI) |
| 3 | Transferencia Riesgo | Contratación de Empresa o Entidad (Adquisición Servicio de evaluación, corrección y Mejoras en el sistema) |
|  |  |  |
| Id Riesgo. | Opción de tratamiento de riesgo | Control (es) |
| 4 | Reducción de Riesgo | Adquisición de Almacenamiento Físico o Nube para Respaldo de Información |
| 5 | Transferencia Riesgo | Contratación de Empresa o Entidad (Adquisición Servicio asesoría en Seguridad e Infraestructura) |
| 5 | Reducción de Riesgo | Adquisición de Dispositivos de Seguridad (T-5) |
| 5 | Reducción de Riesgo | Delegación de Administración de Servidor únicamente a una persona de la empresa. |
| 6 | Reducción de Riesgo | Capacitación mensual al personal de facturación sobre el impacto y consecuencias de facturación errónea, uso de software de facturación |
| 7 | Transferencia Riesgo | Contratación Empresa o Entidad (Modificación de parámetros en la creación de usuarios y definición e implementación de patrón seguro contraseñas en sistema) |
| 8 | Aceptación de Riesgo | Gerencia esta al tanto de la deficiencia de disponibilidad y asume el riesgo. |
| 9 | Transferencia de Riesgo | Contratación de Empresa o Entidad (Implementación de Bitácora para monitoreo de usuarios) |
| 10 | Aceptación de Riesgo | Gerencia está al tanto de la deficiencia de disponibilidad y asume el riesgo. |
| 11 | Reducción de Riesgo | Definición, reevaluación e implementación de Roles y Permisos en la empresa y en sistema. |
| 12 | Reducción de Riesgo | Definición e implementación de Dominios en red de Sistema y limitación por usuario |
| 13 | Transferencia de Riesgo | Contratación Empresa o Entidad (Adquisición de servicio de Verificación y corrección de vulnerabilidad en el sistema de empresa) |
| 13 | Reducción de Riesgo | T-9, T-11 |
| 14 | Transferencia de Riesgo | T-3 |
| 15 | Reducción de Riesgo | Eliminación de correos con antigüedad de 2 a;os en adelante |
| 15 | Reducción de Riesgo | Apertura de Cuentas de Correo Electrónico para cada departamento. |

Realice el mapa de calor colocando los riesgos identificados en el cuadrante que se encuentran