ESCENARIOS



FRANCISCO DAVID PARRA MEDINA

MARIA CAMILA PRECIADO ROJAS

ROBINSON FERNANDO RODRIGUEZ APONTE



UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA

FACULTAD DE INGENIERÍA, BOYACÁ

ESCUELA DE SISTEMAS Y COMPUTACIÓN

TUNJA

2017

1. Seguridad: el sistema tendrá un respaldo de la base de datos principal en un equipo remoto ubicado en una locación distinta del servidor principal.
   1. Para registro y consultas de usuarios en la base de datos, el sistema debe proporcionar la respuesta en un tiempo no mayor a 3 segundos.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuario identificado y autorizado con ciertos permisos, elemento (caja) en estado activo. |
| Estímulo | Acceso a opciones de funcionalidad. |
| Artefacto | Servicios |
| Ambiente | Usuario validado con existencia en bases de datos. Condiciones normales, sistema con acceso a internet online. |
| Respuesta | Mostrar las opciones del sistema dependiendo el rol, Muestra de información, datos, permisos, almacenamiento e informar a usuarios. |
| Medida de Respuesta | 90% de éxito |

* 1. El sistema tendrá por motivos de seguridad una base de datos espejo que haga el backup de la base de datos principal.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | El backup será hecho simultáneamente entre la base de datos host y la espejo |
| Estímulo | Acceso a almacenamiento y consulta de datos del sistema intentando “romper” la seguridad |
| Artefacto | Acceso a la base de datos principal |
| Ambiente | Usuario en condiciones normales, sistema con acceso a internet online, sobrecargado. |
| Respuesta | Muestra de información, almacenamiento y creación de una copia base de datos |
| Medida de Respuesta | La confiabilidad va a ser buena porque en caso de que ocurra una catástrofe en la base de datos host se puede tener acceso a la base de datos espejo y continuar normlmente. |

* 1. La seguridad de acceso a la red wifi va a ser por cifrado Wpa2

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuario en modo activo (administrador, coordinador, cajera) |
| Estímulo | Acceso a servicios intentando “romper” la seguridad |
| Artefacto | Acceso a la base de datos principal y servicios |
| Ambiente | Usuario en condiciones activo, con una red local , sobrecargado. |
| Respuesta | Ejecución de elementos actuadores y del sistema |
| Medida de Respuesta | La confiabilidad esta al rededor del 50 % |

* 1. La base de datos tendrá un sistema de encriptación de contraseñas de usuario empleando AES

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuario en condiciones en ingreso al sistema |
| Estímulo | Acceso a servicios y utilidades del sistema intentando “romper” la seguridad |
| Artefacto | Acceso a la base de datos principal, servicios y dispositivos |
| Ambiente | Usuario en condiciones de ingreso, sistema con acceso a internet online |
| Respuesta | Facilidad de acceso al sistema |
| Medida de Respuesta | Tiempo latencia máximo de acceso debe ser de 2 segundos proporcionando fiabilidad y confiabilidad de los datos |

* 1. El sistema debe proporcionar herramientas para la detección de ataques y detener su operación mientras es desbloqueado por un administrador.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Intruso en el sistema, |
| Estímulo | Acceso a servicios, recursos y datos del sistema intentando “romper” la seguridad |
| Artefacto | Acceso a la base de datos principal, servicios y componentes del sistema |
| Ambiente | Sistema en ejecución, con o sin acceso a internet |
| Respuesta | Detención del sistema y bloqueo en la base de datos principal |
| Medida de Respuesta | Cantidad de recursos protegidos |

1.6 El sistema debe proporcionar la recuperación a fallos y pérdida de datos.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Sistema |
| Estímulo | Recursos y datos de usuarios del sistema |
| Artefacto | Almacenamiento, servicios y recursos |
| Ambiente | Usuario o sistema, con presencia de fallos |
| Respuesta | El sistema se recupera ante el fallo y permite continuar con el proceso |
| Medida de Respuesta | Cantidad de servicios recuperados ante el fallo. |

**Tácticas**

Resistir ataques:

* Autenticar usuarios, autorizar usuarios, mantener confidencialidad de datos, mantener integridad, detectar ataques, detección de intrusos, recuperación de un ataque.

1. Funcionalidad: El sistema debe ser capaz de procesar información de las claves solicitadas por las cajeras, esto no debe superar los límites de tiempo de procesamiento que estén dentro de un rango de tolerancia muy pequeño.
   1. Para solicitud de servicio de clave el sistema debe hacer uso de un rango de tiempo de 0 a 3 segundos para reflejar dicha solicitud en el actuador de la coordinadora. Y así mismo hará respuesta a una solicitud de servicio de clave el sistema no debe demorar más de 5 segundos en desbloquear la caja.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuario identificado y autorizado con ciertos permisos. Acceso limitado a ciertos recursos |
| Estímulo | Acceso a opciones de funcionalidad o datos del sistema |
| Artefacto | Servicios, opciones del sistema acceder a la base de datos |
| Ambiente | Usuario validado con existencia en bases de datos. Condiciones normales, sistema sin acceso a internet offline, sobrecargado. |
| Respuesta | Muestra de información, almacenamiento e informar a usuarios. |
| Medida de Respuesta | La calidad en la comunicación de estos dos módulos debe ser alta- moderada |

**Tácticas:**

3. Disponibilidad: el sistema debe garantizar el acceso a todas las funcionalidades dependiendo la operación a realizar teniendo en cuenta cada rol.

3.1 El sistema debe disponer los recursos en un 90% de las veces que se quiere acceder.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuario del sistema |
| Estímulo | Acceso a servicios, recursos y datos del sistema |
| Artefacto | Acceso a la base de datos principal, servicios y componentes del sistema |
| Ambiente | Sistema en ejecución, con o sin acceso a internet, sobrecargado |
| Respuesta | Datos, recursos y servicios solicitados |
| Medida de Respuesta | Calificación del sistema |

3.2 El sistema debe proporcionar herramientas de recuperación que no involucren un tiempo mayor a 60 segundos.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Sistema con errores o caído |
| Estímulo | Acceso a servicios, recursos y datos del sistema |
| Artefacto | Acceso a la base de datos principal, servicios y componentes del sistema |
| Ambiente | Sistema con dificultades en el acceso, sin acceso a internet, sobrecargado |
| Respuesta | Triggers para reanudar el sistema |
| Medida de Respuesta | El tiempo de recuperación debe entre 2- 3 minutos |

3.3 El tiempo máximo de operación para cada transacción que se realice por un usuario debe ser menor a 3 segundos

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuarios del sistema |
| Estímulo | Acceso a servicios, recursos y datos del sistema |
| Artefacto | Acceso a la base de datos principal, servicios y componentes del sistema |
| Ambiente | , sin acceso a internet, sobrecargado |
| Respuesta | Triggers para reanudar el sistema |
| Medida de Respuesta | El tiempo de recuperación debe entre 2- 3 minutos |

**Táctica**

4. Usabilidad: El tiempo para el aprendizaje del manejo del sistema para el rol del almacén debe ser menor a 1 hora

4.1 El sistema debe contar con manuales de usuario estructurados adecuadamente para que los usuarios finales puedan entender correctamente dicho sistema.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuarios del sistema y documentación |
| Estímulo | Acceso a recursos externos |
| Artefacto | Manuales y documentación |
| Ambiente | Usuario en modo de aprendizaje |
| Respuesta | El usuario con conocimientos previos en el manejo y ejecución del sistema. |
| Medida de Respuesta | El aprendizaje no debe tardar más de 1 hora. |

**Tácticas**

* Separar interfaz del resto del sistema, seguir “reglas de oro de la usabilidad”, diálogos simples y naturales, hablar el lenguaje del usuario, ser consistente, Proveer feedback, dar buenos mensajes de error, ayuda y documentación

5. Escalabilidad: El sistema debe permitir la ejecución e implementación de cambio a futuro

5.1 Contara con la actualización de nuevos módulos

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuarios y sistema |
| Estímulo | Facilidad para implementación de nuevos módulos |
| Artefacto | Módulos y herramientas |
| Ambiente | Ambiente adaptado a nuevos módulos y funcionalidades del sistema. |
| Respuesta | Usuarios con capacidades de operación de nuevas funcionalidades. |
| Medida de Respuesta | Cantidad de usuarios con capacidades de uso de dichos elementos. |

5.2 Permitirá la incorporación de otro tipo de hardware distinto a la manilla de comunicación.

|  |  |
| --- | --- |
| Escenario | Posibles valores |
| Fuente | Usuarios y sistema |
| Estímulo | Incorporar nuevo hardware compatible con el sistema android, en reemplazo de la manilla, como los Smartphone. |
| Artefacto | Componente de hardware (Smartphone). |
| Ambiente | Modo normal, con las implicaciones del software ya desarrollado. |
| Respuesta | Usuarios con capacidad de consulta según su rol, empleando el Smartphone. |
| Medida de Respuesta | Cantidad de usuarios con capacidades de uso de dichos elementos empleando nuevo hardware. |