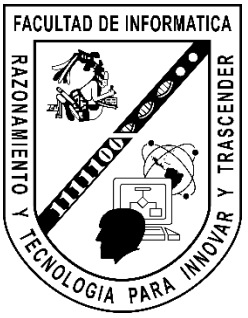


Universidad Autónoma de Querétaro
Facultad de Informática

Arquitectura de las TI

Carrera:

Ingeniería de Software

Integrantes:

Jesus Alejandro Avendaño Peña	256024
Alejandro Monjaraz Gonzalez	301595
Nestor Ivan Rodríguez Zavala	268668
Frida Olivera Martinez	307045
Diego Hernández Sánchez	301579
Jesús García Santiago	301574
Raul Guillermo Valdez Valadez	307028
Daniel Esaú Villagran Cruz	301586
David Emmanuel Cano Cabrera	297140
Ian Ramírez España Cervantes	301566
Alejandro Calixto Montoya	301607

Profesora:

Verónica López Martínez

Fecha:

21 de noviembre de 2024

Escenario de Amenazas de Seguridad en una Red

Contexto: En la era digital actual, los adultos mayores se están incorporando cada vez más al mundo de la tecnología, especialmente en el uso de servicios financieros a través de dispositivos móviles. Nuestro escenario se centra en un usuario adulto mayor que utiliza un asistente de voz para acceder a información financiera y recibir capacitación digital desde su hogar. Esta situación, aunque beneficiosa, presenta desafíos únicos en términos de seguridad digital.

Los adultos mayores, con su limitada experiencia en tecnología, representan un grupo particularmente vulnerable a las amenazas cibernéticas. Su disposición a confiar, combinada con un conocimiento técnico básico, los convierte en objetivos atractivos para diversos tipos de ataques digitales. La red doméstica donde operan estos dispositivos suele carecer de las protecciones robustas que encontraríamos en entornos empresariales.

Posibles amenazas identificadas

1. **Contraseñas débiles**

Escenario: El usuario utiliza una contraseña común como "123456" o "password" para iniciar sesión en la aplicación, facilitando el acceso no autorizado.

Impacto: Un atacante podría acceder a datos sensibles, historial de interacciones y estadísticas almacenadas en el sistema.

2. **Phishing**

Escenario: El usuario recibe un mensaje fraudulento que aparenta ser de soporte técnico del sistema, solicitándole ingresar credenciales en un enlace falso.

Impacto: Las credenciales pueden ser robadas y utilizadas para acceder al sistema.

3. **Malware**

Escenario: El usuario descarga accidentalmente un archivo o aplicación infectada mientras navega por internet en el mismo dispositivo que utiliza para acceder al asistente.

Impacto: El malware podría interceptar datos sensibles o comprometer la funcionalidad del sistema.

4. **Interceptación de Datos (Ataques Man-in-the-Middle)**

Escenario: Un atacante intercepta la comunicación entre el dispositivo del usuario y el servidor, especialmente en redes Wi-Fi públicas.

Impacto: Datos sensibles, como identificadores de usuario o historial de consultas, podrían ser robados.

5. **Explotación de Vulnerabilidades en la Red**

Escenario: La red Wi-Fi doméstica del usuario tiene una configuración predeterminada o utiliza un cifrado obsoleto como WEP.

Impacto: Un atacante puede acceder a la red y monitorear las actividades del usuarios.

Propuestas de solución

- **Contraseñas débiles**

  Acción: Implementar políticas de contraseñas robustas, como requisitos de longitud mínima, uso de caracteres especiales y cambio periódico de contraseñas.

  Adicional: Incluir autenticación de dos factores (2FA) para el acceso al sistema.

- **Prevención contra Phishing**

  Acción: Capacitar a los usuarios, mediante el asistente, sobre cómo identificar correos electrónicos y mensajes fraudulentos.

  Adicional: Bloquear enlaces sospechosos y activar filtros de correo electrónico en el dispositivo.

- **Protección contra Malware**

  Acción: Incluir un antivirus actualizado en los dispositivos de los usuarios y advertencias sobre descargar aplicaciones de fuentes no confiables.

  Adicional: Usar navegadores con protección contra sitios web peligrosos.

- **Cifrado de comunicación**

  Acción: Asegurarse de que todas las comunicaciones entre el dispositivo y el servidor utilicen HTTPS y protocolos como TLS.

  Adicional: Implementar tokens de seguridad para cada sesión iniciada.

- **Seguridad en la red Wi-Fi**

  Acción: Promover el uso de configuraciones de seguridad como WPA3 para redes inalámbricas y cambiar las contraseñas predeterminadas del router.

  Adicional: Recomendar el uso de redes privadas virtuales (VPN) para conexiones en redes públicas.

- **Monitorización y registro**

  Acción: Establecer sistemas de monitoreo que detecten patrones inusuales en el uso del sistema, como múltiples intentos de inicio de sesión fallidos.

  Adicional: Proporcionar notificaciones al usuario en caso de actividad sospechosa.

- **Backups y Resiliencia**

  Acción: Realizar copias de seguridad periódicas de los datos almacenados, garantizando que puedan recuperarse en caso de ataque o pérdida.

  Adicional: Diseñar estrategias de recuperación ante desastres que minimicen el tiempo de inactividad.

Educación y Concientización

La primera línea de defensa debe ser un programa de educación adaptado específicamente para adultos mayores. Este no debe limitarse a simples instrucciones de "qué hacer y qué no hacer", sino que debe construirse sobre experiencias relativas a su vida cotidiana. Por ejemplo, así como no abrirían la puerta a un extraño que se presenta como empleado bancario sin identificación, deben aplicar el mismo principio de precaución en el entorno digital.

Sistemas de Seguridad Adaptados

Es fundamental implementar medidas de seguridad que encuentren el balance correcto entre protección y usabilidad. La autenticación biométrica, por ejemplo, puede ser una excelente alternativa a las contraseñas complejas, ofreciendo seguridad sin comprometer la facilidad de uso. Los sistemas de reconocimiento de voz del asistente pueden incorporar verificaciones adicionales para transacciones sensibles, como confirmaciones por múltiples canales.

Monitoreo y Soporte Continuo

El monitoreo proactivo de actividades inusuales debe complementarse con un sistema de soporte accesible y paciente. Cuando un adulto mayor detecta algo sospechoso, debe tener acceso inmediato a asistencia técnica que pueda guiarlo de manera clara y comprensiva. Este soporte debe estar disponible no solo por medios digitales sino también por canales tradicionales como el teléfono.

Implementación Práctica

La implementación de estas medidas de seguridad debe ser gradual y acompañada. Durante el primer mes, el enfoque debe estar en establecer hábitos básicos de seguridad y familiarizar al usuario con las herramientas de protección. Las siguientes semanas deben dedicarse a introducir gradualmente medidas más avanzadas, siempre verificando la comodidad y comprensión del usuario.

Resultados Esperados

Un sistema de seguridad bien implementado debe resultar en una reducción significativa de incidentes y, más importante aún, en un usuario que se siente seguro y capaz en su interacción con la tecnología. El éxito no se mide solo en términos de amenazas bloqueadas, sino en la confianza y autonomía que el usuario desarrolla en su vida digital.

ESCENARIO GENERAL

Un Día en la Vida Digital: La Transformación de Don Roberto con Axolutions

La Situación Inicial

Don Roberto Martínez, un jubilado de 68 años, enfrentaba el desafío de adaptarse al mundo digital bancario. Su hijo Miguel, gerente de tecnología en una empresa local, le recomendó utilizar el nuevo chatbot de Axolutions, una solución integral que prometía simplificar todas sus operaciones financieras. Al principio, Don Roberto se mostró escéptico - después de todo, ya había tenido dificultades con otras aplicaciones bancarias.

"Es diferente, papá", le explicó Miguel. "Este asistente virtual entiende el lenguaje natural y puede ayudarte con todo: desde consultar tu saldo hasta pagar servicios, todo con simples comandos de voz o texto."

Los Primeros Pasos y Desafíos

La Configuración Inicial

En una tarde de domingo, Miguel ayudó a su padre a instalar la aplicación de Axolutions. El proceso de registro fue sorprendentemente sencillo: el chatbot guió a Don Roberto paso a paso, usando un lenguaje claro y adaptado para usuarios mayores. Sin embargo, los primeros desafíos no tardaron en aparecer.

El dilema de la Seguridad vs Usabilidad

Las Contraseñas

Don Roberto, siguiendo viejas costumbres, intentó usar "Roberto1955" como contraseña. El chatbot de Axolutions inmediatamente intervino:

"Don Roberto, he notado que esta contraseña podría ser fácil de adivinar. ¿Qué le parece si creamos juntos una contraseña segura pero memorable? Podemos usar frases que sean significativas para usted."

El sistema sugirió un método innovador: crear una contraseña basada en sus recuerdos favoritos. Así nació "TangoAzul$1955!Mate", una contraseña robusta pero significativa para Don Roberto, basada en su color favorito, año de nacimiento y bebida preferida.

El Incidente de Phishing

Una mañana, Don Roberto recibió un mensaje que parecía ser del banco:

"Estimado cliente: Su cuenta requiere verificación urgente. Acceda a través de: www.banco-seguro-verificacion.com"

Aunque el mensaje parecía convincente, el chatbot de Axolutions detectó el intento de acceso a un sitio sospechoso y mostró una alerta inmediata:

"¡Atención, Don Roberto! He detectado que está intentando acceder a un sitio web no seguro. Recuerde que su banco nunca le pedirá verificar sus datos por correo electrónico o enlaces externos."

La Amenaza Silenciosa: Malware

Durante una búsqueda de tutoriales financieros, Don Roberto encontró una página que prometía "mejoras premium" para su asistente financiero. Al intentar descargar el archivo, el sistema de seguridad de Axolutions intervino inmediatamente:

"Don Roberto, he detectado que está intentando descargar software no verificado. Por su seguridad, ha bloqueado la descarga. Recuerde que todas las actualizaciones oficiales se realizan automáticamente a través de nuestra aplicación."

El Punto de Inflexión

La verdadera prueba llegó cuando Don Roberto notó un cargo sospechoso en su cuenta: una compra online de $500 que él no había realizado. Sin embargo, el sistema de Axolutions ya estaba un paso adelante:

1. Detectó la transacción inusual basándose en el patrón de gastos de Don Roberto
2. Congeló temporalmente la transacción
3. Envió una notificación inmediata a través de múltiples canales
4. Activó el protocolo de verificación de identidad

La Implementación de Soluciones Integrales

Fase 1: Protección Fundamental

El equipo de soporte de Axolutions asignó a Don Roberto un asesor virtual personalizado que:

1. Implementó un sistema de autenticación multinivel:
    - Reconocimiento facial para accesos diarios
    - Huella digital para confirmación de transacciones
    - Verificación por voz para operaciones de alto valor
2. Configuró el sistema de alertas inteligentes:
    - Notificaciones por SMS para transacciones inusuales

    - Alertas de voz para intentos de acceso sospechosos
    - Recordatorios amigables para actualizaciones de seguridad
3. Estableció protocolos de verificación adaptados:
    - Preguntas de seguridad personalizadas
    - Confirmación biométrica escalonada
    - Sistema de contactos de confianza para emergencias

Fase 2: Educación Interactiva

Durante el primer mes, Don Roberto participó en un programa de capacitación personalizado:

1. Sesiones Diarias de Práctica:
    - Simulaciones de intentos de phishing
    - Ejercicios de identificación de sitios seguros
    - Práctica de comandos de voz seguros
2. Aprendizaje Contextual:
    - Tutoriales integrados en la aplicación
    - Retroalimentación inmediata sobre acciones seguras
    - Videos explicativos adaptados a su nivel de comprensión
3. Evaluaciones Prácticas:
    - Pruebas simuladas de situaciones de riesgo
    - Ejercicios de respuesta a incidentes
    - Certificaciones básicas de seguridad digital

Fase 3: Optimización del Entorno Digital

El sistema de Axolutions implementó mejoras progresivas:

1. Seguridad de Red:
    - Configuración automática de VPN para transacciones
    - Detección de redes no seguras
    - Aislamiento de operaciones financieras
2. Monitoreo Inteligente:
    - Análisis continuo de patrones de uso
    - Detección temprana de amenazas

    - Sistema predictivo de riesgos
3. Respaldo y Recuperación:
    - Copias de seguridad automáticas de configuraciones
    - Sistema de recuperación de acceso simplificado
    - Registro encriptado de transacciones

Resultados Transformadores

Primer Trimestre

Don Roberto pasó de ser un usuario temeroso a uno confiado:

- Realizaba transacciones diarias sin asistencia
- Identificaba y reportaba intentos de fraude
- Compartía consejos de seguridad con otros usuarios

Segundo Trimestre

Su progreso se aceleró:

- Comenzó a usar funciones avanzadas del chatbot
- Participaba en sesiones de retroalimentación
- Ayudaba a otros adultos mayores a adoptar la tecnología

Tercer Trimestre

Se convirtió en un embajador digital:

- Organizaba talleres en su centro comunitario
- Compartía historias de éxito en el blog de Axolutions
- Participaba en pruebas beta de nuevas funciones

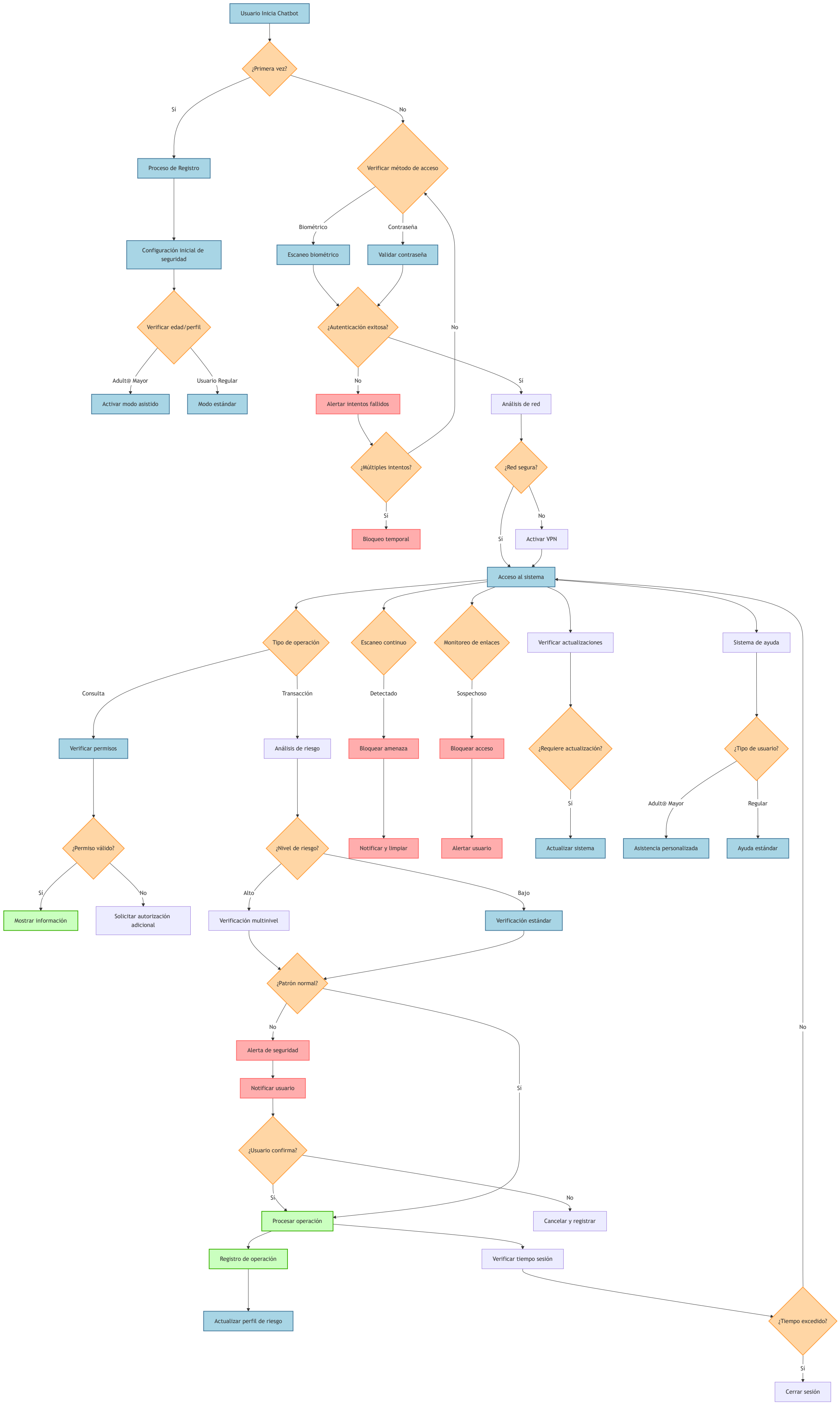
Impacto Sostenible

La transformación de Don Roberto ilustra el poder de un sistema bien diseñado:

1. Seguridad Adaptativa:
    - Protección que evoluciona con el usuario
    - Alertas contextuales y relevantes
    - Respuestas automatizadas a amenazas
2. Educación Continua:
    - Aprendizaje basado en experiencias reales
    - Retroalimentación constante y positiva
    - Comunidad de apoyo activa
3. Empoderamiento Digital:
    - Independencia en operaciones financieras
    - Confianza en la tecnología
    - Capacidad de ayudar a otros

Conclusión

La historia de Don Roberto con el chatbot de Axolutions demuestra cómo la tecnología adecuada, combinada con un enfoque centrado en el usuario y sistemas de seguridad robustos, puede transformar la vida digital de cualquier persona, independientemente de su edad o experiencia previa. Su viaje de usuario vulnerable a embajador digital inspire a otros y valida el enfoque integral de Axolutions hacia la seguridad y usabilidad.


Usuario Inicia Chatbot
¿Primera vez?
Sí
No
Proceso de Registro
Verificar método de acceso
Biométrico
Contraseña
Configuración inicial de seguridad
Escaneo biométrico
Validar contraseña
Verificar edad/perfil
¿Autenticación exitosa?
No
Adult@ Mayor
Usuario Regular
No
Sí
Activar modo asistido
Modo estándar
Alertar intentos fallidos
Análisis de red
¿Múltiples intentos?
¿Red segura?
Sí
No
Bloqueo temporal
Sí
Activar VPN
Acceso al sistema
Tipo de operación
Escaneo continuo
Monitoreo de enlaces
Verificar actualizaciones
Sistema de ayuda
Consulta
Transacción
Detectado
Sospechoso
Verificar permisos
Análisis de riesgo
Bloquear amenaza
Bloquear acceso
¿Requiere actualización?
¿Tipo de usuario?
Sí
Adult@ Mayor
Regular
¿Permiso válido?
¿Nivel de riesgo?
Notificar y limpiar
Alertar usuario
Actualizar sistema
Asistencia personalizada
Ayuda estándar
Sí
No
Alto
Bajo
Mostrar información
Solicitar autorización adicional
Verificación multinivel
Verificación estándar
¿Patrón normal?
No
No
Alerta de seguridad
Notificar usuario
Sí
¿Usuario confirma?
Sí
No
Procesar operación
Cancelar y registrar
Registro de operación
Verificar tiempo sesión
Actualizar perfil de riesgo
¿Tiempo excedido?
Sí
Cerrar sesión