UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Informe de Seguridad Billeteras Virtuales

Noviembre 2024

Introducción

El objetivo del presente informe consiste en generar un análisis comparativo de aspectos de seguridad en las diferentes aplicaciones utilizadas como billeteras digitales y medios de pago en el mercado argentino, desde la perspectiva del usuario final.

Es importante destacar que el presente documento estará enfocado en los mecanismos de seguridad implementados y cómo los jugadores más relevantes del mercado difieren o coinciden entre sí en funcionalidades de seguridad, mitigación de riesgos, en búsqueda de un balance y compromiso entre la seguridad y la experiencia de usuario.

La seguridad de la información se fundamenta en tres atributos de calidad ampliamente reconocidos en la industria y la academia: confidencialidad, integridad y disponibilidad.

- ✓ Confidencialidad: Es la protección de la información contra accesos no autorizados, garantizando que solo las personas o sistemas con los permisos adecuados puedan acceder a los datos. Este atributo busca preservar la privacidad y el control sobre la información, evitando su divulgación no deseada.
- ✓ Integridad: Consiste en la preservación de la exactitud, consistencia y completitud de la información a lo largo de su ciclo de vida. La integridad asegura que los datos no se modifiquen de forma indebida o accidental y que cualquier alteración sea detectada, de modo que los datos mantengan su confiabilidad.
- ✓ Disponibilidad: Se refiere a la capacidad de garantizar que la información y los recursos estén accesibles y utilizables para los usuarios autorizados cuando se necesiten. Este atributo implica minimizar interrupciones y vulnerabilidades en los sistemas, permitiendo un acceso continuo y oportuno a los datos y servicios.

Aplicaciones Analizadas

Se analizaron las aplicaciones de los bancos y cuentas digitales más populares:

- ✓ BBVA
- ✓ BNA+
- ✓ Cuenta DNI
- ✓ Galicia
- ✓ Macro
- ✓ Mercado Pago
- ✓ Modo
- ✓ NaranjaX
- ✓ Santander
- ✓ Ualá

Funcionalidades Evaluadas

1. **Identificación y autenticación: Protección de acceso a cuenta**
    a. Métodos y calidad de 2FA disponibles
    b. Instancias de validación de identidad en ingreso a cuenta
    c. Proceso para cambio de contraseña o datos de autenticación
    d. Aviso por inicio de sesión en otro dispositivo

2. **Dispositivo y sesión en app: Protección de sesión activa**
    a. Convivencia de validación entre aplicación y teléfono
    b. Gestión de sesiones múltiples (administrar dispositivos vinculados)

3. **Movimientos: Controles para prevenir errores y fraudes**
    a. Trazabilidad de transacciones
    b. Notificaciones por actividad
    c. Validación de identidad en movimientos fuera de parámetros normales

4. **Gestión de incidentes: Reporte de problemas de seguridad**
    a. Canales para denunciar cuenta
    b. Posibilidad de denunciar transferencias o pagos
    c. Pausado tarjeta
    d. Gestión de casos

Metodología

El enfoque metodológico tiene como propósito realizar un análisis mixto, combinando enfoques cuantitativos y cualitativos, sobre la experiencia de seguridad que percibe el usuario final. El objetivo es proporcionar una visión integral de las fortalezas y debilidades en cuanto a la seguridad y experiencia de usuario de estas aplicaciones.

Para comenzar, se definieron objetivos claros que guiarán cada fase del análisis. Se determinaron los aspectos clave de seguridad y experiencia de usuario que se evaluaron en cada aplicación. Esto puede incluir desde parámetros técnicos de seguridad, como autenticación y protección de datos, hasta elementos de usabilidad que impactan en la percepción de seguridad de las personas usuarias.

Se definió un protocolo detallado que permitió una evaluación estructurada y consistente en todas las aplicaciones. Este protocolo incluye un listado de tareas específicas que los evaluadores debieron completar en cada aplicación, garantizando que se sigan los mismos pasos en cada caso para facilitar la comparación de resultados.

La fase de recolección de datos comenzó con la descarga y exploración de las aplicaciones. Durante este proceso inicial, el equipo de investigación se familiarizó con las funciones y configuraciones de cada aplicación para comprender mejor sus características antes de iniciar la evaluación formal.

A continuación, siguiendo el protocolo establecido, los evaluadores documentaron en informes de texto cada interacción, anotando observaciones sobre la navegación, usabilidad y cualquier aspecto relevante de seguridad, además de registrar las percepciones de confianza o desconfianza que surjan durante el uso de cada aplicación. Una vez completados, estos informes se revisaron y organizaron según los criterios del protocolo de evaluación, con el objetivo de identificar patrones comunes o problemas específicos en términos de seguridad. Así, los informes textuales proporcionarán un registro detallado de las interacciones que servirá de base para el análisis posterior.

A través de estos pasos, la investigación busca obtener una visión detallada de la experiencia de seguridad en las aplicaciones móviles seleccionadas, empleando tanto métodos cuantitativos como cualitativos para un análisis fundamentado.

Criterios de Ponderación

1. **Identificación y Autenticación: Protección de acceso a cuenta**
    a. Métodos y calidad de autenticación de dos factores (2FA) disponibles:
        i. Calidad del método: Se analiza la robustez de los métodos de 2FA (como autenticadores, códigos SMS, correos electrónicos, biometría).
        ii. Complejidad de la implementación: Grado de dificultad para configurar 2FA. Se valora que sea intuitivo y sencillo de activar para el usuario.
        iii. Facilidad de uso: Evaluación de cuán práctico resulta el método de 2FA en el uso cotidiano, minimizando fricciones.
        iv. Disponibilidad: Variedad de opciones de 2FA y compatibilidad en distintos dispositivos y contextos.
    b. Instancias de validación de identidad en el ingreso a la cuenta:
        i. Requerimientos de acceso: Evaluación de los pasos necesarios para acceder a la cuenta (nombre de usuario y contraseña, PIN, autenticación biométrica).
        ii. Refuerzos de seguridad: Implementación de refuerzos como preguntas de seguridad, validaciones secundarias al detectar actividad inusual, nuevo dispositivo, entre otros.
    c. Proceso para cambio de contraseña o datos de autenticación:
        i. Seguridad del proceso: Análisis de las medidas de seguridad para el cambio de credenciales, como preguntas de seguridad adicionales, uso de 2FA, y requisitos de complejidad de la contraseña.
        ii. Facilidad y claridad: Evaluación de la claridad y simplicidad en el proceso para que el usuario recupere el acceso rápidamente en caso de pérdida o compromisos de la cuenta.
    d. Aviso por inicio de sesión en otro dispositivo:
        i. Alertas de seguridad: Análisis de la frecuencia y detalle de notificaciones al detectarse un inicio de sesión en un dispositivo o ubicación diferente.
        ii. Opciones de bloqueo de sesión: Capacidad del usuario para bloquear o cerrar sesiones no reconocidas rápidamente.

2. **Dispositivo y sesión en app: Protección de sesión activa**
    a. Convivencia de validación entre aplicación y teléfono:
        i. Verificación de dispositivo adicional: Si se requiere la validación a través de otro dispositivo (como un teléfono) para operaciones críticas, por ejemplo, mediante SMS, WhatsApp o una App de autenticación.
    b. Gestión de sesiones múltiples (administración de dispositivos vinculados):

i. Control de dispositivos: Revisión de si el usuario puede ver y administrar los dispositivos en los que su cuenta está activa.
ii. Cierre remoto de sesiones: Capacidad del usuario para finalizar sesiones activas desde un dispositivo distinto para mayor control de seguridad.
iii. Limitación de sesiones: Si se limita el número de dispositivos conectados simultáneamente o se advierte sobre accesos múltiples.

3. Movimientos: Controles para prevenir errores y fraudes

a. Trazabilidad de transacciones:
   i. Registro de transacciones: Existencia de un historial detallado de transacciones con datos como fecha, hora, ubicación y dispositivo.
   ii. Nivel de detalle: Grado de especificidad en los registros, que permita identificar claramente el origen y destino de cada operación.
   iii. Soporte de verificación: Herramientas para auditar las transacciones, especialmente para investigaciones de fraudes o errores.
b. Notificaciones por actividad:
   i. Alertas en tiempo real: Se valora la rapidez y frecuencia de notificaciones por transacciones (envío y recepción de fondos) para mantener al usuario informado.
   ii. Distintos canales: Si las notificaciones pueden recibirse en múltiples canales (correo, SMS, notificaciones en la app) para asegurar visibilidad.
c. Validación de identidad en movimientos fuera de parámetros normales:
   i. Definición de patrones de normalidad: Análisis de los criterios utilizados para identificar movimientos anómalos (monto, ubicación geográfica, frecuencia).
   ii. Activación de 2FA en operaciones atípicas: Evaluación de los pasos de validación adicionales para movimientos fuera de lo común, como un segundo factor de autenticación.

4. Gestión de incidentes: Reporte de problemas de seguridad

a. Canales para denunciar cuenta:
   i. Disponibilidad y facilidad de acceso: Evaluación de los canales habilitados (teléfono, chat, correo) para reportar problemas de seguridad de la cuenta.
   ii. Celeridad del proceso: Tiempo estimado de respuesta y resolución al reportar una incidencia.
   iii. Seguridad en el canal de comunicación: Aseguramiento de que los canales de denuncia protegen la privacidad e información del usuario.

b. Posibilidad de denunciar transferencias o pagos:
    i. Procesos de denuncia de movimientos fraudulentos: Evaluación de la facilidad para reportar movimientos no autorizados y el proceso de investigación.
    ii. Seguimiento de la denuncia: Capacidades del usuario para monitorear el estado de su denuncia y obtener actualizaciones.
c. Pausado de tarjeta:
    i. Facilidad y rapidez: Evaluación de la simplicidad y rapidez del proceso para bloquear o pausar una tarjeta en caso de pérdida o sospecha de fraude.
    ii. Seguridad del canal de bloqueo: Confirmación de que el proceso de pausa o bloqueo se realiza por un canal seguro y sin intermediarios.
d. Gestión de casos:
    i. Sopo Soporte y atención al cliente: Evaluación de la asistencia disponible para gestionar problemas de seguridad de la cuenta o tarjeta.
    ii. Seguimiento del caso: Si existe un número de caso o sistema de seguimiento que permite al usuario verificar el progreso de la resolución.

Funcionalidades Ponderadas

Categoría	Ítem	Ponderación	Total Categoría
1. Identificación y autenticación: Protección de acceso a cuenta	a. Métodos y calidad de 2FA disponibles	10	40
	b. Instancias de validación de identidad en ingreso a cuenta	20	
	c. Proceso para cambio de contraseña o datos de autenticación	5	
	d. Aviso por inicio de sesión en otro dispositivo	5	
2. Dispositivo y sesión en app: Protección de sesión activa	a. Convivencia de validación entre aplicación y teléfono	5	15
	b. Gestión de sesiones múltiples (administrar dispositivos vinculados)	10	
3. Movimientos: Controles para prevenir errores y fraudes	a. Trazabilidad de transacciones	10	25
	b. Notificaciones por actividad sospechosa	5	
	c. Validación de identidad en movimientos fuera de parámetros normales	10	
4. Gestión de incidentes: Reporte de problemas de seguridad	a. Canales para denunciar cuenta	4	20
	b. Posibilidad de denunciar transferencias o pagos	5	
	c. Pausado tarjeta	3	
	d. Gestión de casos	8	
		Total	**100**

Resultados Generales

Categoría	BBVA	BNA+	Cuenta DNI	Galicia	Macro	Mercado Pago	Modo	NaranjaX	Santander	Ualá
1. Identificación y autenticación: Protección de acceso a cuenta	16.98	21.99	23.16	14.5	13.5	**27.32**	22.15	25.82	18	24.83
2. Dispositivo y sesión en app: Protección de sesión activa	-	8	8	8	8	**15**	13	8	8	-
3. Movimientos: Controles para prevenir errores y fraudes	**19.96**	4.99	5.98	9.96	7.96	18	6.96	7.96	12.96	12.96
4. Gestión de incidentes: Reporte de problemas de seguridad	6.25	2.25	9.65	11.45	1.45	8.8	**12.7**	11.25	2.25	11.25
Total	**43.19**	**37.23**	**46.79**	**43.91**	**30.91**	**69.12**	**54.81**	**53.03**	**41.21**	**49.04**

Observaciones: Valores obtenidos de las aplicaciones disponibles en las tiendas en noviembre de 2024.

Escala de Ponderación

Etiqueta	Valor %
Destacado	75 a 100
Adecuado	50 a 74.99
Aceptable	37.5 a 49.99
Regular	25 a 37.49
Inadecuado	0 a 24.99

Resultados por Categoría Ponderados

Categoría	BBVA	BNA+	Cuenta DNI	Galicia	Macro	Mercado Pago	Modo	NaranjaX	Santander	Ualá
1. Identificación y autenticación: Protección de acceso a cuenta	Aceptable	Adecuado	Adecuado	Regular	Regular	Adecuado	Adecuado	Adecuado	Aceptable	Adecuado
2. Dispositivo y sesión en app: Protección de sesión activa	Inadecuado	Adecuado	Adecuado	Adecuado	Adecuado	Destacado	Destacado	Adecuado	Adecuado	Inadecuado
3. Movimientos: Controles para prevenir errores y fraudes	Destacado	Inadecuado	Inadecuado	Aceptable	Regular	Adecuado	Regular	Regular	Adecuado	Adecuado
4. Gestión de incidentes: Reporte de problemas de seguridad	Regular	Inadecuado	Aceptable	Adecuado	Inadecuado	Aceptable	Adecuado	Adecuado	Inadecuado	Adecuado

Observaciones: Valores obtenidos de las aplicaciones disponibles en las tiendas en noviembre de 2024.

Resultados por Ítem

Categoría	Ítem	BBVA	BNA+	Cuenta DNI	Galicia	Macro	Mercado Pago	Modo	NaranjaX	Santander	Ualá
1. Identificación y autenticación: Protección de acceso a cuenta	a. Métodos y calidad de 2FA disponibles	3	-	-	-	-	9	1	-	3	-
	b. Instancias de validación de identidad en ingreso a cuenta	10	19	19	10	9	9	19	19	10	19
	c. Proceso para cambio de contraseña o datos de autenticación	3.98	2.99	4.16	4.5	4.5	4.32	2.15	3.82	5	2.83
	d. Aviso por inicio de sesión en otro dispositivo	-	-	-	-	-	5	-	3	-	3
2. Dispositivo y sesión en app: Protección de sesión activa	a. Convivencia de validación entre aplicación y teléfono	-	-	-	-	-	5	5	-	-	-
	c. Gestión de sesiones múltiples (administrar dispositivos vinculados)	0	8	8	8	8	10	8	8	8	-
3. Movimientos: Controles para prevenir errores y fraudes	a. Trazabilidad de transacciones	4.96	4.99	2.98	4.96	4.96	10	4.96	7.96	4.96	5.96
	b. Notificaciones por actividad sospechosa	5	-	3	5	3	3	2	-	3	2
	c. Validación de identidad en movimientos fuera de parámetros normales	10	-	-	-	-	5	-	-	5	5
4. Gestión de incidentes: Reporte de problemas de seguridad	a. Canales para denunciar cuenta	0.5	0.5	1.2	1.2	0.5	2.5	0.7	2	0.5	2
	b. Posibilidad de denunciar transferencias o pagos	0.75	0.75	1.25	1.25	0.75	3.5	4	4.25	0.75	4.25
	c. Pausado tarjeta	3	1	0.2	2	0.2	2.8	-	3	1	3
	d. Gestión de casos	2	-	7	7	-	-	8	2	-	2
Total		**43.19**	**37.23**	**46.79**	**43.91**	**30.91**	**69.12**	**54.81**	**53.03**	**41.21**	**49.04**

Observaciones: Valores obtenidos de las aplicaciones disponibles en las tiendas en noviembre de 2024.

Puntos Destacados y Oportunidades

BBVA

- ✓ Destacado: Solicita 2FA para el alta de nueva cuenta y transferencia. Envío de Notificaciones en cada operación, por mail y a través de la App.
- ✓ Oportunidad: Permite múltiples sesiones, pero no tiene una gestión centralizada de las mismas.

BNA+

- ✓ Destacado: Si bien permite un solo dispositivo simultáneo, solicita el onboarding completo, con DNI y biometría, al cambiar de dispositivo.
- ✓ Oportunidad: Mejorar trazabilidad de operaciones, envío de notificaciones por movimientos, integrar la gestión de reclamos en la aplicación.

Cuenta DNI

- ✓ Destacado: Si bien permite un solo dispositivo simultáneo, solicita el onboarding completo, con DNI y biometría, al cambiar de dispositivo.
- ✓ Oportunidad: Mejorar trazabilidad de operaciones e integrar la gestión de reclamos en la aplicación.

Galicia

- ✓ Destacado: Si bien no permite sesiones múltiples, permite un solo dispositivo simultáneo. Envío de Notificaciones en cada operación, por mail y a través de la App.
- ✓ Oportunidad: Incorporar un 2FA para el alta de nueva cuenta o transferencia.

Macro

- ✓ Destacado: Gestión de sesiones múltiples. Envío de notificaciones por mail por actividad.
- ✓ Oportunidad: Incorporar un 2FA para el alta de nueva cuenta o transferencia. Integrar la gestión de reclamos en la aplicación.

Mercado Pago

- ✓ Destacado: Gestión de sesiones múltiples. Diversidad de 2FA. Simplicidad de Denuncia de Cuenta y Transferencia. Posibilidad de Denuncia por Tercero. Destacada trazabilidad de operaciones. Solicita 2FA en operaciones fuera de parámetros normales.
- ✓ Oportunidad: Integrar la gestión de reclamos en la aplicación.

Modo

- ✓ Destacado: Si bien permite un solo dispositivo simultáneo, solicita el onboarding completo con biometría, al cambiar de dispositivo. Posee integrada la gestión de reclamos.
- ✓ Oportunidad: Incorporar un 2FA para el alta de nueva cuenta o transferencia. Permitir el proceso de cambio de contraseña desde la app con sesión activa.

NaranjaX

- ✓ Destacado: Si bien permite un solo dispositivo simultáneo, solicita el onboarding completo, con DNI y biometría, al cambiar de dispositivo. Destacada trazabilidad de operaciones. Posee integrada la gestión de reclamos.
- ✓ Oportunidad: Incorporar un 2FA para el alta de nueva cuenta o transferencia. Envío de Notificaciones en cada operación, por mail y a través de la App.

Santander

- ✓ Destacado: Si bien no permite sesiones múltiples, permite un solo dispositivo simultáneo. Envío de notificaciones en cada operación por mail. Solicita 2FA para el alta de nueva cuenta y transferencia.
- ✓ Oportunidad: Integrar la gestión de reclamos en la aplicación.

Ualá

- ✓ Destacado: Posee integrada la gestión de reclamos. Solicita el onboarding completo en el nuevo dispositivo.
- ✓ Oportunidad: Permite múltiples sesiones, pero no tiene una gestión centralizada de las mismas. Incorporar un 2FA para el alta de nueva cuenta o transferencia. Permitir el proceso de cambio de contraseña desde la app con sesión activa.

Análisis Detallado

1. Identificación y autenticación: Protección de acceso a cuenta

Para garantizar la seguridad de las cuentas, es crucial implementar un sistema de autenticación robusto. Esto incluye el uso de métodos de autenticación multifactor (2FA) de alta calidad, como autenticadores de aplicaciones o claves físicas en lugar de solo SMS, debido a los riesgos de suplantación. Las instancias de validación de identidad al ingresar deben estar diseñadas para detectar patrones de comportamiento sospechosos. Adicionalmente, el proceso de cambio de contraseña debe estar protegido por validaciones adicionales que impidan el acceso no autorizado, y debe notificar al usuario de cualquier intento de acceso en nuevos dispositivos, permitiéndole responder de inmediato si no reconoce la actividad.

- ✓ **BBVA**
  - Tiene un cumplimiento **aceptable** de las estrategias esperadas en este apartado. Solicita revalidación en nuevo dispositivo. No cuenta con gran desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es correcta, a través de un proceso simple, con una contraseña de robustez media y gestión de históricos. No genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **BNA+**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Solicita revalidación en nuevo dispositivo. No cuenta con desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es mejorable, a través de un proceso de complejidad media, con una contraseña de baja robustez y gestión de históricos. No genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **Cuenta DNI**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Solicita revalidación en nuevo dispositivo. No cuenta con desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es adecuada, a través de un proceso simple, con una contraseña de alta robustez y gestión de históricos. No genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **Galicia**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. No solicita revalidación en nuevo dispositivo. No cuenta con desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es adecuada, a través de un proceso simple, con una contraseña de alta robustez y gestión de históricos. No genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **Macro**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. No solicita revalidación en nuevo dispositivo. No cuenta con desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es adecuada, a través de un proceso simple, con una contraseña de alta robustez y gestión de históricos. No genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **Mercado Pago**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Cuenta con desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es adecuada, a través de un proceso simple, con una contraseña de media robustez y gestión de históricos. Genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **Modo**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Solicita revalidación en nuevo dispositivo. No cuenta con gran desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es mejorable, ya que no permite iniciar el proceso cuando el usuario está con sesión activa. La contraseña de robustez baja y posee gestión de históricos. No genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **NaranjaX**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Solicita revalidación en nuevo dispositivo. No cuenta con gran desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es correcta, a través de un proceso simple, con una contraseña de robustez media y gestión de históricos. Genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **Santander**
  - Tiene un cumplimiento **aceptable** de las estrategias esperadas en este apartado. No solicita revalidación en nuevo dispositivo, pero permite operar en un solo dispositivo, aquel que posee el token. No cuenta con gran desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es adecuada, a través de un proceso simple, con una contraseña de alta robustez y gestión de históricos. No genera notificaciones por inicio de sesión en nuevos dispositivos.

- ✓ **Ualá**

- Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Solicita revalidación en nuevo dispositivo. No cuenta con desarrollo y diversidad en 2FA como Biometría o QR. La gestión de contraseñas es correcta, a través de un proceso simple, con una contraseña de robustez media y gestión de históricos. Genera notificaciones por inicio de sesión en nuevos dispositivos.

2. Dispositivo y sesión en app: Protección de sesión activa

La protección de la sesión activa en las aplicaciones requiere mecanismos de validación continua para confirmar que el usuario autorizado sigue siendo quien interactúa. Esto puede lograrse mediante la autenticación biométrica o validaciones de PIN en intervalos regulares. La gestión de sesiones múltiples debe permitir a los usuarios monitorear y desvincular dispositivos de forma sencilla y segura, proporcionando control sobre todos los dispositivos conectados a su cuenta. Además, debería existir una integración efectiva entre la aplicación y el teléfono del usuario para responder a posibles accesos sospechosos o no autorizados de manera rápida.

- ✓ **BBVA**
  - Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. Permite sesiones múltiples pero sin gestión de las mismas.

- ✓ **BNA+**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Si bien no tiene soporte a sesiones múltiples, soporta una sola sesión activa, cerrando la sesión en los otros dispositivos.

- ✓ **Cuenta DNI**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Si bien no tiene soporte a sesiones múltiples, soporta una sola sesión activa, cerrando la sesión en los otros dispositivos.

- ✓ **Galicia**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. Si bien no tiene soporte a sesiones múltiples, soporta una sola sesión activa, cerrando la sesión en los otros dispositivos.

- ✓ **Macro**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. Si bien no tiene soporte a sesiones múltiples, soporta una sola sesión activa, cerrando la sesión en los otros dispositivos.

- ✓ **Mercado Pago**
  - Tiene un cumplimiento **destacado** de las estrategias esperadas en este apartado. Utiliza el celular como elemento de seguridad para la validación cruzada entre sesiones. Permite y tiene gestión avanzada de sesiones múltiples.

- ✓ **Modo**
  - Tiene un cumplimiento **destacado** de las estrategias esperadas en este apartado. Si bien no tiene soporte a sesiones múltiples, soporta una sola sesión activa, cerrando la sesión en los otros dispositivos.

- ✓ **NaranjaX**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Si bien no tiene soporte a sesiones múltiples, soporta una sola sesión activa, cerrando la sesión en los otros dispositivos.

- ✓ **Santander**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Si bien no tiene soporte a sesiones múltiples, soporta una sola sesión activa, cerrando la sesión en los otros dispositivos.

- ✓ **Ualá**
  - Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. Permite sesiones múltiples, pero sin gestión de las mismas.

3. Movimientos: Controles para prevenir errores y fraudes

Para prevenir errores y fraudes en las transacciones, la trazabilidad es esencial, por lo que cada transacción debe contar con un registro detallado que permita auditar movimientos sospechosos. Las notificaciones en tiempo real ante cualquier actividad brindan transparencia y permiten al usuario actuar rápidamente si detecta irregularidades. Adicionalmente, para movimientos fuera de los parámetros normales, debería activarse una capa adicional de verificación de identidad, reduciendo así el riesgo de transacciones fraudulentas o accidentales.

- ✓ **BBVA**
  - Tiene un cumplimiento **destacado** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de la trazabilidad de las transacciones. Genera notificaciones por las operaciones realizadas tanto por email, como en la app. Utiliza un 2FA (token) para las operaciones de alta de cuenta y transferencia.

- ✓ **BNA+**
  - Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle bajo de la trazabilidad de las transacciones. No genera notificaciones por las operaciones realizadas tanto por email, como en la app. No utiliza un 2FA para las operaciones de alta de cuenta y transferencia.

- ✓ **Cuenta DNI**
  - Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle bajo de la trazabilidad de las transacciones. No genera notificaciones por las operaciones realizadas tanto por email, como en la app. No utiliza un 2FA para las operaciones de alta de cuenta y transferencia.

- ✓ **Galicia**
  - Tiene un cumplimiento **aceptable** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de trazabilidad de las transacciones. Genera notificaciones por las operaciones realizadas tanto por email, como en la app. No utiliza un 2FA para las operaciones de alta de cuenta y transferencia.

- ✓ **Macro**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de trazabilidad de las transacciones. Genera notificaciones por las operaciones realizadas por email. No utiliza un 2FA para las operaciones de alta de cuenta y transferencia.

- ✓ **Mercado Pago**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de trazabilidad de las transacciones. Genera notificaciones por las operaciones realizadas por email. No utiliza un 2FA para las operaciones de alta de cuenta y transferencia.

- ✓ **Modo**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de la trazabilidad de las transacciones. No genera notificaciones por las operaciones realizadas tanto por email, como en la app. No utiliza un 2FA para las operaciones de alta de cuenta y transferencia.

- ✓ **NaranjaX**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de la trazabilidad

de las transacciones. Permite Exportación y Reportes. No genera notificaciones por las operaciones realizadas tanto por email, como en la app. No utiliza un 2FA para las operaciones de alta de cuenta y transferencia.

- ✓ **Santander**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de la trazabilidad de las transacciones. Genera notificaciones por email de las operaciones realizadas. Utiliza un 2FA (token) para las operaciones de alta de cuenta y transferencia.

- ✓ **Ualá**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Cuenta con un nivel de detalle adecuado de la trazabilidad de las transacciones. Permite la generación de Reportes. Genera notificaciones en la app de las operaciones realizadas. Utiliza un 2FA para las operaciones de transferencia.

4. Gestión de incidentes: Reporte de problemas de seguridad

Contar con canales de reporte accesibles es fundamental para que los usuarios puedan informar problemas de seguridad rápidamente. El sistema debería permitir denunciar no solo la cuenta en caso de compromiso, sino también transferencias o pagos sospechosos, proporcionando la posibilidad de pausar tarjetas y activos en tiempo real. La gestión de casos debe ser ágil, asegurando que cada incidente sea tratado con prioridad y resolución rápida, minimizando el impacto en el usuario y restaurando su seguridad.

- ✓ **BBVA**
  - Tiene un cumplimiento **regular** de las estrategias esperadas en este apartado. No permite denunciar la cuenta y transferencias a través de la app. Permite el pausado y bloqueo de las tarjetas a través de la app de forma simple. No permite generar y gestionar casos a través de la app.

- ✓ **BNA+**
  - Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. No permite denunciar la cuenta y transferencias a través de la app, solamente a través de teléfono fijo. No permite el pausado de las tarjetas a través de la app de forma simple. No permite generar y gestionar casos a través de la app.

- ✓ **Cuenta DNI**
  - Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. No permite denunciar la cuenta y transferencias a través de la app, solamente a través de teléfono fijo. No permite el pausado de las tarjetas a través de la app de forma simple. No permite generar y gestionar casos a través de la app.

- ✓ **Galicia**
  - Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. No permite denunciar la cuenta y transferencias a través de la app, solamente a través de teléfono fijo o whatsapp. Permite el pausado de las tarjetas a través de la app de forma simple. Permite generar casos y su seguimiento a través de la app.

- ✓ **Macro**
  - Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. No permite denunciar la cuenta y transferencias a través de la app, solamente a través de teléfono fijo. No permite el pausado de las tarjetas a través de la app de forma simple. No permite generar y gestionar casos a través de la app.

- ✓ **Mercado Pago**

- Tiene un cumplimiento **aceptable** de las estrategias esperadas en este apartado. Permite denunciar la cuenta y transferencias a través de la app. Además, incorpora la figura de persona de confianza, que permite denunciar la cuenta por un tercero. Permite el pausado de las tarjetas a través de la app de forma simple. No permite generar y gestionar casos a través de la app.

✓ **Modo**

- Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Permite denunciar las transferencias a través de la app y whatsapp. Además, incorpora la figura de persona de confianza, que permite denunciar la cuenta por un tercero. No permite el pausado o bloqueo de las tarjetas a través de la app, algo que se puede comprender por la naturaleza de la app. Permite generar, gestionar casos y ver el histórico a través de la app.

✓ **NaranjaX**

- Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Permite denunciar la cuenta y transferencias a través de la app y teléfono fijo. Permite el pausado y bloqueo de las tarjetas a través de la app de forma simple. Permite generar casos, pero no su gestión, seguimiento e histórico.

✓ **Santander**

- Tiene un cumplimiento **inadecuado** de las estrategias esperadas en este apartado. No permite denunciar la cuenta y transferencias a través de la app, solamente a través de teléfono fijo. No permite el pausado de las tarjetas a través de la app de forma simple. No permite generar y gestionar casos a través de la app.

✓ **Ualá**

- Tiene un cumplimiento **adecuado** de las estrategias esperadas en este apartado. Permite denunciar la cuenta y transferencias a través de la app y teléfono fijo. Permite el pausado y bloqueo de las tarjetas a través de la app de forma simple. Permite generar casos, pero no su gestión, seguimiento e histórico.

Conclusión

La evolución constante de las aplicaciones no solo abarca mejoras funcionales sino también optimizaciones en aspectos no funcionales, donde la seguridad se ha convertido en un pilar esencial de la calidad. En este contexto,la seguridad se encuentra presente en múltiples facetas del desarrollo, algunas de ellas más evidentes para el usuario que otras. Luego de un análisis detallado y comparativo entre aplicaciones, se destacan las siguientes conclusiones clave:

- ✓ **La robustez y versatilidad del factor de autenticación (2FA)**: La implementación de un 2FA eficaz es fundamental para garantizar la seguridad de la aplicación. La calidad y diversidad de métodos de autenticación de doble factor incrementan significativamente la protección contra accesos y acciones no autorizadas.

- ✓ **Adopción obligatoria de biometría facial**: Para los procesos críticos y transacciones principales, se recomienda la adopción mandatoria de autenticación biométrica facial, dada su capacidad para brindar un nivel adicional de seguridad y confiabilidad en la verificación de identidad.

- ✓ **Dinamismo en el requisito de 2FA**: Es crucial que el sistema de autenticación sea capaz de evaluar el contexto en tiempo real y adaptarse de acuerdo con factores como el dispositivo, el tipo de cuenta, el monto de la transacción, entre otros. Este enfoque contextualizado permite una gestión de seguridad más inteligente y menos invasiva para el usuario.

- ✓ **Importancia de las notificaciones proactivas**: Las notificaciones juegan un papel esencial en la experiencia de usuario, permitiéndole mantenerse informado sobre todas las operaciones y actividades relevantes en su cuenta, lo que refuerza la confianza y la transparencia en el uso de la aplicación.

- ✓ **Gestión accesible y trazable de incidentes**: La gestión de incidentes de seguridad debe estar fácilmente disponible para el usuario y contar con trazabilidad completa. Este aspecto es fundamental para permitir un control efectivo y responder oportunamente ante posibles amenazas o vulnerabilidades.

Estas conclusiones destacan la importancia de un enfoque proactivo en la gestión de la seguridad, garantizando que la protección del usuario esté integrada en cada punto de interacción y proceso dentro de la aplicación. Así, se asegura una experiencia segura, confiable y alineada con los estándares actuales de calidad de la industria.

Descargo de Responsabilidad

Este informe ha sido preparado por UTN BA con el propósito exclusivo de proporcionar información y no constituye asesoramiento de seguridad ni una recomendación de acción.

La elaboración del informe se basa utilizando datos de las aplicaciones móviles disponibles públicamente en sus versiones actuales al momento de la prueba. El análisis abarca únicamente funciones de seguridad no técnicas, vistas desde la perspectiva del usuario final, y sigue un protocolo de pruebas definido para asegurar la consistencia en todas las aplicaciones evaluadas.

Este estudio se realizó entre el 01 de octubre de 2024 y el 20 de noviembre de 2024 y UTN BA renuncia a cualquier responsabilidad en la medida máxima permitida por la ley.