Respuestas Definitivas

1.¿Cuáles son los servicios que actualmente le presta a Bancolombia?
Mobbeel presta a Bancolombia el servicio de captura de documentos y validación facial para el registro y onboarding de usuarios. Este servicio se ofrece bajo la modalidad SaaS (Software as a Service)

2.Para la prevención de fuga de información, ¿cuenta con un control DLP (Data Loss Prevention)?
Sí, Mobbeel cuenta con protocolos de protección de la información que incluyen cifrado de datos, controles de acceso y gestión de vulnerabilidades. Estas medidas forman parte de su Sistema de Gestión de Seguridad de la Información (SGSI), certificado bajo la norma ISO 27001. Además, cuenta con políticas de respaldo y copias de seguridad periódicas. Se contempla la integración de soluciones como AWS Macie para la identificación y clasificación de datos sensibles.

3.¿La Organización tiene documentados, justificados y autorizados los cambios en los sistemas de información?
Mobbeel tiene documentados, justificados y autorizados los cambios en los sistemas de información. Se siguen las políticas de revisión de cambios definidas anteriormente, que aseguran que cada modificación sea evaluada y aprobada adecuadamente. Este proceso se documenta en el sistema de gestión de código que utiliza Mobbeel, que es GitLab. Las capturas de pantalla de los "merge requests" de varios proyectos demuestran que se llevan a cabo revisiones de cambios de manera formal y organizada

4.¿La Organización tiene en cuenta las lecciones aprendidas durante la gestión de los incidentes de ciberseguridad y seguridad de la información para tomar medidas correctivas?
Sí, Mobbeel registra y analiza cada incidente de ciberseguridad, identificando áreas de mejora y aplicando medidas correctivas para su mitigación.

5.¿Cuál es la periodicidad con que se revisan los derechos de acceso de los usuarios en los sistemas de información? ¿Cómo se realizan estas revisiones? ¿Quién es responsable de las revisiones?
Las revisiones de los derechos de acceso de los usuarios se realizan semestralmente. El Responsable de Seguridad lleva a cabo estas revisiones, evaluando los permisos de cada usuario según los registros de permisos asignados y documentándolos en el formato Registro de revisión de permisos de usuario.

6.¿Se cuenta con una definición de roles y privilegios de acceso al contendor de información donde se almacena la información de Bancolombia? Si la respuesta es afirmativa, indicar detalladamente cómo se realizó este perfilamiento.
Sí, Mobbeel asigna permisos específicos según las funciones laborales, sensibilidad de datos y políticas de seguridad. La gestión de accesos se realiza a través de un sistema centralizado con mecanismos de acceso seguro.

7.¿Tiene implementado un proceso o procedimiento formal de creación, modificación, revocación y cancelación de usuarios, para la asignación de los derechos de acceso en los sistemas? ¿Qué área de su organización gestiona este procedimiento? ¿Cómo es la solicitud de creación, modificación o revocación de accesos?
Mobbeel tiene un proceso formal gestionado por Recursos Humanos para la creación, modificación y revocación de accesos, definido en su Procedimiento de Gestión de Personal. La asignación y revocación de privilegios siguen protocolos específicos, y las solicitudes se realizan mediante un formulario estandarizado.

8.¿Están documentados los privilegios de acceso?
Sí, los privilegios de acceso están documentados. Mantenemos un registro detallado de los permisos asignados a cada usuario en el formato Registro de revisión de permisos de usuario, el cual se actualiza en cada revisión semestral realizada por el Responsable de Seguridad. Este registro permite garantizar que los accesos se mantengan actualizados y en línea con las políticas de seguridad de la organización.

10.¿El ingreso al contenedor de información está restringido exclusivamente a los usuarios que hayan sido autorizados específicamente, cumpliendo el concepto de mínimos privilegios?
Sí, Mobbeel concede acceso a la información requerida para poder desarrollar las actividades aplicando el principio del mínimo privilegio.

11.¿Cuentan con manuales, políticas, procedimientos, estándares y/o instructivos que definan el ciclo de vida de copias de respaldo (backups)?
Sí, realiza copias diarias automáticas con retención de 10 días, sincronización entre servidores locales y remotos y almacenamiento en AWS con encriptación AES-256. Además, ejecuta pruebas de restauración y tiene un plan de recuperación con RPO y RTO de 5 horas.

12.¿Se han materializado en el último año incidentes, sanciones, requerimientos o investigaciones por temas de ciberseguridad, seguridad de la información?
No, en el último año no se han materializado incidentes, sanciones, requerimientos ni investigaciones por temas de ciberseguridad o seguridad de la información .

13.¿Cuenta con un procedimiento o protocolo para la atención de incidentes de ciberseguridad y seguridad de la información?
Sí, Mobbeel cuenta con un procedimiento formal para la atención de incidentes de ciberseguridad y seguridad de la información. Esta información está detallada en el documento titulado "Gestión de Incidencias", donde se establecen los pasos a seguir para identificar, responder y gestionar incidentes de seguridad de manera efectiva.

14.¿Están definidas las responsabilidades para el procedimiento de atención y gestión de incidentes de ciberseguridad y seguridad de la información?
Sí, el procedimiento de Gestión de Incidencias define claramente los roles de un Equipo de Respuesta a Incidentes, asignando responsabilidades al Responsable de Seguridad de la

Información y a los Administradores de Sistemas para la detección, análisis y mitigación de incidentes.

15.¿Cuenta con lineamientos para clasificar la información que es gestionada dentro de su organización de acuerdo con su criticidad? En caso afirmativo, ¿Cuáles son los niveles en que se clasifica la información? ¿Se ha clasificado la información de la organización?

Mobbeel ha definido un Procedimiento de Clasificación de Información con niveles: Confidencial, Interna y Pública. La clasificación se realiza en base al impacto sobre la organización y se documenta en políticas específicas.

16.¿Cuenta con procedimientos o políticas para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización? Enúncielos.

Sí, Mobbeel cuenta con procedimientos y políticas para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado. Estos procedimientos están documentados en los siguientes documentos: Inventario de activos, Valor propio de activos esenciales y Activos esenciales.

17.¿El aliado cuenta con ambientes de desarrollo seguro, pruebas y producción de los sistemas de información o aplicaciones?

Sí, Mobbeel cuenta con ambientes de desarrollo, pruebas y producción claramente diferenciados para los sistemas de información y aplicaciones. Esta separación garantiza que las actividades de desarrollo y prueba no interfieran con el entorno de producción, lo que contribuye a la seguridad y estabilidad del sistema.

18.¿Los ambientes no productivos se encuentran separados, lógica o físicamente, del ambiente productivo para reducir los riesgos de acceso o cambios no autorizados en producción?

Sí, Mobbeel separa la red de la oficina, utilizada para entornos de desarrollo y prueba, de las redes de producción que se encuentran alojadas en los proveedores de hosting.

19.¿Realiza pruebas de seguridad (Ethical Hacking) sobre los sistemas de información antes de pasar a producción? Describa con qué periodicidad lo realiza.

Mobbeel realiza pruebas de seguridad cada 6 meses, análisis de vulnerabilidades cada 3 meses y hacking ético antes de producción. Estas pruebas incluyen pruebas de intrusión, análisis de redes, bases de datos y aplicaciones, así como auditorías internas y externas. Los hallazgos se documentan y se implementan planes de mitigación.

20.¿Establece requisitos de seguridad de la información en el desarrollo de nuevos sistemas de información o mejoras en los existentes en su organización?

Mobbeel aplica Requisitos de Seguridad en el Desarrollo basados en OWASP y estándares ISO, que se integran en el ciclo de vida del desarrollo (SDLC) para asegurar controles de entrada y validaciones de seguridad en el código.

21.¿Cuenta con políticas y controles de seguridad para los desarrollos de software que contrata con terceros?

Mobbeel tiene políticas y controles de seguridad en vigor para los desarrollos de software que contrata con terceros. En caso de requerir estos servicios, se exige a los proveedores un compromiso de cumplimiento en materia de seguridad de la información equivalente al de Mobbeel, específicamente conforme a la norma ISO 27001.

22.¿Utiliza datos de producción en ambientes de certificación o pruebas?
No, en ningún caso se utilizan datos de producción en los ambientes de certificación o pruebas. Los datos de producción están especialmente protegidos para garantizar la integridad y la confidencialidad de la información sensible.

23.¿Realiza análisis de vulnerabilidades sobre la infraestructura tecnológica? Describa con qué
periodicidad lo realiza.
Mobbeel realiza análisis de vulnerabilidades cada 3 meses con Prowler e implementa un sistema automático en los flujos de lanzamiento. Además, utiliza OWASP Dependency Check y Trivy para analizar vulnerabilidades en los merge requests, fortaleciendo la seguridad en su infraestructura.

24.¿Tiene implementado controles para la protección sobre el acceso a la documentación física sensible (papel, ej. Contratos, cartas, formatos de vinculación, cheques)? Mencione los procedimientos y controles y si están documentados.
Sí, los controles están documentados en la Declaración de Aplicabilidad y en la Normativa de Seguridad de la Información, específicamente en el apartado "6.9 Cuidado y protección de la información impresa".

25.¿Cuenta con un procedimiento o método para custodiar la información física? (bóveda de seguridad, locker con llave, cajonera con llave,etc)
La organización cuenta con un procedimiento para custodiar la información física confidencial, la cual se almacena en lockers con llave. Estos lockers son custodiados por el responsable de seguridad.

26.Si la información necesita ser extraída, ¿Se cuenta con una bitácora de registro de personas y acciones sobre la información? ¿Esta bitácora es física o digital? ¿Quién custodia esta bitácora?
Sí, dispone de un registro de acceso y actuaciones, tanto físico como digital, custodiado por el personal de seguridad designado.

27.¿Cuenta con lineamientos o procedimientos definidos para evitar la fuga de información a través de medios removibles (discos magnéticos, USB y/o dispositivos de almacenamiento extraíbles) y con que periodicidad verifica el cumplimiento de dichos lineamientos o procedimientos?
Sí, la organización tiene lineamientos y procedimientos definidos para prevenir la fuga de información mediante medios removibles como discos magnéticos y USB. Estos están documentados en la declaración de aplicabilidad y en la "Normativa de Seguridad de la Información" (punto 6.4). Además, se establece una periodicidad para verificar su cumplimiento.

28.¿El proveedor realiza pruebas de seguridad sobre su sitio web? ¿Se reportan los hallazgos de seguridad del sitio al banco? Favor indique la dirección (URL) de su sitio web.

Se llevan a cabo de forma periódica auditorías de seguridad en la web corporativa de Mobbeel, ubicada en www.mobbeel.com .

29.¿El contrato establecido con el Grupo Bancolombia cuenta con anexo de seguridad (ciberseguridad y seguridad de la información) y el acuerdo de confidencialidad?

Sí, el contrato entre Mobbeel y B. Agrícola cuenta con cláusulas de Seguridad de la información (incluida en la última adenda al contrato en 2023 para adecuarlo a las regulaciones técnicas NRP-23 y NRP24). En cuanto al Acuerdo de confidencialidad, en el acuerdo de servicio hay varias cláusulas que hacen referencia a la confidencialidad.

30.¿Tiene establecidos acuerdos de confidencialidad y requisitos de seguridad de la información con los terceros o proveedores que puedan tener acceso, procesen, almacenen, comuniquen o suministren información de la organización o de sus clientes? ¿Cuales?

Mobbeel cuenta con acuerdos de confidencialidad y requisitos de seguridad de la información establecidos con todos los proveedores que puedan acceder, procesar, almacenar, comunicar o suministrar información de la organización o de sus clientes. Estos acuerdos son parte de la política de gestión de proveedores, que asegura que todos los colaboradores cumplen con las normativas de seguridad adecuadas.

31.¿Realiza seguimiento, revisa y audita con regularidad la prestación de servicios de sus proveedores? ¿Con áreas internas o entidades externas? ¿Qué tipo de revisiones realiza?

Mobbeel realiza seguimiento y auditoría regular de sus proveedores mediante su procedimiento de gestión, liderado por el Responsable de Seguridad y equipo técnico. Evalúa niveles de servicio, informes del proveedor, incidentes de seguridad, registros de eventos y problemas identificados. Estas revisiones se realizan al menos una vez al año, con documentación en formatos específicos.

32.¿Cuenta con procedimientos documentados para el control de acceso a los sistemas por parte de los proveedores que tiene subcontratados para el servicio del Banco? ¿Cuáles?

No, Mobbeel no tiene proveedores subcontratados para el servicio del banco. AWS es el único proveedor de infraestructura en la nube, operando bajo protocolos de seguridad propios y cumpliendo estándares como ISO 27001 y SOC 2.

33.¿Se realiza verificación de los antecedentes de otros terceros que contrata en su organización de acuerdo con las leyes, reglamentaciones y ética pertinentes, requisitos de negocio, clasificación de la información a la que se va a tener acceso y/o riesgos identificados? Describa cuáles de los anteriores criterios cumple.

La información sobre si se realiza verificación de los antecedentes de otros terceros que contrata en su organización de acuerdo con las leyes, reglamentaciones y ética pertinentes,

requisitos de negocio, clasificación de la información a la que se va a tener acceso y/o riesgos identificados no está explícitamente detallada en las fuentes proporcionadas .

34.¿Los acuerdos contractuales con empleados y contratistas establecen claramente las responsabilidades de éstos en cuanto a la seguridad de la información? ¿Sus empleados firman acuerdos de confidencialidad o de no divulgación de información privilegiada?
Sí, los empleados y contratistas firman acuerdos de confidencialidad y reciben formación en seguridad desde su incorporación. Mobbeel cuenta con mecanismos para exigir cumplimiento, sanciones internas y cláusulas contractuales. Además, ha establecido normativas y políticas para garantizar la protección de la información.

35.¿Cuenta con mecanismos para exigir a los empleados y contratistas la aplicación de la seguridad de la información, de acuerdo con las políticas y procedimientos establecidos por la organización? Describa cuáles.
Sí, Mobbeel establece en los acuerdos contractuales las responsabilidades de empleados y contratistas en materia de seguridad de la información. Además, exige la firma de acuerdos de confidencialidad o de no divulgación. Para garantizar el cumplimiento, aplica mecanismos alineados con sus políticas y procedimientos de seguridad.

36.¿El aliado cuenta con apoyo de auditorias externas para verificar que cumpla con sus obligaciones en materia de seguridad de la información manera planificada y periódica?
¿Con qué frecuencia? ¿Qué compañías tiene contratadas actualmente para este fin?
Mobbeel ha implementado un Sistema de Gestión de la Seguridad de la Información (SGSI) certificado según la norma ISO 27001. Este sistema incluye auditorías anuales, tanto internas como externas, para evaluar y verificar de forma continua y rigurosa los controles de seguridad implementados. La auditoría externa es llevada a cabo por una entidad certificadora independiente.

37.¿Cuenta con una política de protección de datos personales, que se encuentre visible para consultas publica (ejemplo: página web)?
Sí, la política de privacidad está expuesta en la web: https://www.mobbeel.com/politica-privacidad/ .

38.¿Cuenta con un Oficial de Privacidad o área encargada de protección de datos personales?
Mobbeel ha designado la figura de Responsable de Seguridad, quien supervisa las cuestiones relacionadas con la seguridad de la información y la protección de datos personales. Además, cuenta con el apoyo legal del despacho de abogados Écija para abordar aspectos legales vinculados a la seguridad de la información.

39.¿Cuenta con un protocolo para la atención de incidentes de seguridad en materia de protección de datos personales?
Sí, Mobbeel tiene un protocolo para la atención de incidentes de seguridad relacionados con la protección de datos personales. Este protocolo establece procedimientos para identificar y notificar brechas de seguridad, evaluar el impacto y aplicar medidas correctivas, garantizando así el cumplimiento de las normativas de protección de datos.

40.¿Cuenta con protocolos para la atención de requerimientos, consultas y reclamaciones en materia de protección de datos personales?

Sí, Mobbeel tiene protocolos para atender requerimientos, consultas y reclamaciones sobre protección de datos personales. Los usuarios pueden ejercer sus derechos, como acceder, rectificar o suprimir sus datos, enviando solicitudes a las direcciones especificadas en su Política de Privacidad.

41.¿Ha tenido sanciones, requerimientos o investigaciones por parte de la Superintendencia de Industria y Comercio (SIC) u otras autoridades por temas de protección de datos?

No.

42.¿Cuenta con controles y procesos internos documentados e implementados que tiendan a proteger los datos personales?

Sí, cuenta con controles y procesos alineados con el RGPD, asegurando el cumplimiento de las políticas de gestión de datos personales y la protección de la privacidad de los usuarios.

43.¿Tiene registrada sus bases de datos en calidad de responsable y /o encargado ante el registro nacional de bases de datos?

No aplica.

44.¿Cuenta con un programa de capacitación para los empleados y contratistas de la organización en materia de protección de datos personales y lo ejecuta de manera periódica?

Sí, Mobbeel cuenta con un programa de capacitación en materia de protección de datos personales para empleados y contratistas, el cual se ejecuta de manera periódica. Este programa busca asegurar que todos los involucrados comprendan sus responsabilidades en relación con la protección de datos y la seguridad de la información, así como las políticas y procedimientos establecidos por la organización.

45.¿El proveedor o su personal prestará servicio dentro de sedes, sucursales u oficinas de Bancolombia?

No.

46.¿El proveedor cuenta con una metodología y/o sistema para la administración de sus riesgos operacionales y el riesgo cibernético (identificación, medición, control y monitoreo) a los que está expuesta su empresa? Especifique el nivel de madurez y/o tiempo que lleva con dicho sistema. - ¿Explique de manera general cuáles son los controles, políticas y actividades que ejecuta para mitigar los riesgos operacionales y cibernéticos identificados en su organización?

Si Mobbeel cuenta con una metodología de gestión de riesgos operacionales y cibernéticos, implementada a través del procedimiento Magerit y la herramienta PILAR. Este sistema se encuentra en un nivel de madurez evaluado mediante el modelo CMMI, realizando análisis de riesgos anuales que incluyen la identificación de activos críticos, evaluación de vulnerabilidades y amenazas. Se aplican medidas de seguridad adaptadas a los niveles de madurez, con revisiones periódicas y propuestas de acciones correctivas. Los resultados y

decisiones sobre riesgos son presentados al Comité de Seguridad de la Información para su aprobación y seguimiento.

47.¿Los empleados del proveedor tienen relación directa con los clientes del banco?
No, los empleados de Mobbeel no tienen relación directa con los clientes del banco. El servicio que Mobbeel presta a Bancolombia es el de captura de documentos y validación facial para el registro y onboarding de usuarios, ofrecido bajo la modalidad SaaS. El personal que presta este servicio está bajo relación laboral directa con Mobbeel.

48.¿El personal que presta el servicio se encuentra bajo relación laboral directa con el proveedor? En caso de ser directa, ¿tiene un proceso propio de selección de colaboradores?
Sí, Mobbeel contrata directamente a su personal y gestiona internamente el proceso de selección, verificando la adecuación de los candidatos y solicitando títulos.

49.¿Capta, almacena o transmite información sensible de tarjetas de crédito y débito como números completos de tarjetas, fechas de vencimiento o códigos de seguridad?
No.

50.¿Para qué proceso o servicio prestado, necesita esta información?
N/C.

51.¿Tiene certificado un ambiente en la norma PCI DSS?
No aplica .

52.¿Requiere que el número de la tarjeta de crédito o debito esté visible (16 dígitos)?
No aplica .

53.¿Podría realizar el proceso con los últimos 4 dígitos visibles?
No aplica.

54.¿Cuenta con estrategias de continuidad de negocio y recuperación ante desastres, para responder y dar continuidad a la prestación de sus servicios en caso de interrupción o materialización de dichos eventos? Detalle cuáles son las estrategias.
Sí, Mobbeel cuenta con estrategias de continuidad de negocio y recuperación ante desastres. Utiliza AWS para gestionar copias de seguridad de datos críticos, protegidas con cifrado AES-256 y almacenadas en ubicaciones redundantes. Además, AWS implementa controles avanzados de seguridad, acceso restringido y protección contra ataques, incluyendo ransomware, para garantizar la integridad y disponibilidad de la información.

55.¿Ejecuta pruebas en el año sobre sus estrategias de continuidad de los diferentes frentes?
Sí, realiza al menos dos pruebas de continuidad al año, registradas en el Registro de Pruebas de Continuidad.
AWS, como proveedor, ejecuta pruebas anuales en empleados, procesos, infraestructura y tecnología, incluyendo simulaciones y recuperación de desastres.

56.¿Tiene su organización un esquema de gestión de crisis para la recuperación del servicio que presta al banco?
Sí, está definido en su SGSI y Plan de Continuidad. Además, AWS refuerza la recuperación con infraestructura redundante, replicación de datos y monitoreo continuo.

57.¿Cuenta con un análisis de impacto al negocio (BIA) documentado, que permita administrar e identificar los procesos críticos relacionados con el servicio ofrecido a Bancolombia y/o sus filiales?
Sí, utiliza Magerit y PILAR para evaluar riesgos, identifica activos críticos y realiza pruebas de continuidad bianuales. AWS refuerza con pruebas de recuperación y continuidad de negocio.

58.¿Suministra información para el procesamiento y preparación de los estados financieros del Grupo Bancolombia?
No aplica

59.¿Realiza mantenimientos a bases de datos o registros del Grupo Bancolombia que tengan implicación o afectación
en el reporte financiero?
Mobbeel realiza mantenimientos a bases de datos o registros con impacto en el reporte financiero, pero la respuesta no está en las fuentes.
Los cuestionarios de seguridad a proveedores abordan temas como información del proveedor, ciberseguridad, acceso, seguridad de la información, datos personales, negocio, certificación PCI, continuidad y SOX.

60.¿Autoriza transacciones del Grupo Bancolombia dentro del proceso o servicio a contratar?
No, Mobbeel no autoriza transacciones dentro del proceso o servicio.

61.¿Prepara estados financieros para el Grupo Bancolombia?
Mobbeel no prepara estados financieros para el Grupo Bancolombia

62.¿Realiza estimaciones contables y/o revelaciones que sirven de base o fuente para la elaboración de los estados financieros del Grupo Bancolombia?
Mobbeel no realiza estimaciones contables ni revelaciones que sirvan de base o fuente para la elaboración de los estados financieros del Grupo Bancolombia

63.¿Administra, parametriza y/o realiza mantenimientos a la infraestructura o plataformas de tecnología propias del proveedor o del Grupo Bancolombia relacionada con el proceso o servicio a contratar con afectación al reporte financiero?
No, Mobbeel no gestiona ni realiza mantenimientos en la infraestructura o plataformas del banco que afecten el reporte financiero.

64.¿El proveedor Digitaliza, captura y/o custodia documentos de valor que puedan afectar los estados financieros del Grupo Bancolombia (pagarés, Garantías, títulos u Otros)?

No, Mobbeel no maneja documentos de valor como pagarés, garantías o títulos que puedan impactar los estados financieros del banco.

65.¿El proveedor tiene acceso a la información confidencial del banco o aplicativos internos que puedan afectar el reporte financiero?
Mobbeel no tiene acceso a información confidencial del banco o aplicativos internos que puedan afectar el reporte financiero.

66.¿El contrato u orden de servicio está relacionado con el Desarrollo, certificación y/o producción de componentes como Bases de datos, aplicaciones, updates u otros con afectación en el reporte financiero?
No, el contrato no implica el desarrollo, certificación o producción de bases de datos, aplicaciones o actualizaciones con impacto en el reporte financiero.

67.¿El contrato u orden de servicio está relacionado con servicios en la nube con afectación en el reporte financiero?
No, el contrato no está vinculado a servicios en la nube ni componentes que impactan el reporte financiero de Bancolombia.

68.¿Desarrolla metodologías que soporten la valoración de los activos del Grupo Bancolombia. (p.e. inversiones, cartera, depreciaciones, avalúos, provisiones, entre otros)?
No aplica

69.¿Una falla o error ocasionado en el proceso prestado por el proveedor puede ocasionar un error o fraude en la información financiera?
No, Mobbeel no tiene acceso ni realiza procesos que puedan causar errores o fraudes en la información financiera de Bancolombia.

70.¿La Organización de Servicios realiza registro, modificación o eliminación de datos o información y para estás se requiere que exista una solicitud, autorización y/o parametrización por parte del Grupo Bancolombia ?
No, Mobbeel no registra, modifica ni elimina datos que requieran autorización del banco y no afecta la información financiera.
