DOCUMENTO DE SEGURIDAD

DATOS PERSONALES

BANCO NACIONAL DEL EJERCITO, FUERZA AÉREA Y ARMADA S.N.C

UNIDAD DE TRANSPARENCIA

INDICE

1. INTRODUCCIÓN.

El Banco Nacional del Ejército, Fuerza Aérea y Armada, Sociedad Nacional de Crédito (Banjercito), es una Institución de Banca de Desarrollo que cuenta con patrimonio propio y tiene por objeto el otorgar servicios financieros a todos los integrantes de las Fuerzas Armadas, independientemente de que se encuentren en el servicio activo o en situación de retiro, a través de actividades y operaciones de banca que su normatividad aplicable le permite.

Con fundamento en su Ley Orgánica, Banjercito realiza las operaciones de banca y crédito que se encuentran previstas en la Ley de Instituciones de Crédito con el fin de promover el ahorro nacional, canalizar de forma eficiente los recursos financieros, así como promover y financiar las actividades que corresponden al sector objetivo.

En atención a su naturaleza como banca de desarrollo, Banjercito ofrece diversos productos de crédito, captación y servicios bancarios a un sector estratégico de la sociedad, los integrantes del Ejército, Fuerza Aérea y Armada; sin embargo, proporciona diversos servicios bancarios y ofrece productos de captación también para el público en general, solo los productos de crédito son exclusivos para el personal militar.

Adicionalmente, Banjercito ofrece diversos servicios instruidos por las autoridades aduaneras y migratorias, como la expedición de permisos para la importación e internación temporal de vehículos, embarcaciones y casas rodantes; la inspección física e incorporación al Registro Público Vehicular de los vehículos que son importados de manera definitiva al país; el cobro del Derecho de visitante sin permiso para realizar actividades remuneradas (DNR), entre otros.

Derivado de la publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en el Diario Oficial de la Federación de fecha 26 de enero de 2017, la cual tiene como objetivo entre otros, proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo público y regular su debido tratamiento; Banjercito, en cumplimiento a la Ley, se encuentra obligado a contar con un documento mediante el cual establezca las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal, denominado Documento de Seguridad.

La LGPDPPSO en el artículo 3 fracción XIV, define al Documento de Seguridad como el *"Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee"*

En la actualidad los datos personales se han convertido en un activo clave para el desarrollo, fortalecimiento e intercambio de bienes y servicios en una economía global y digital, por lo que el

reto de cualquier sujeto obligado radica en construir bases normativas que garanticen la transferencia de dichos datos de manera segura sin causar afectaciones.

Por lo anterior, Banjercito como Entidad de la Administración Pública Federal, tiene la obligación de dar cumplimiento a lo establecido en la LGPDPPSO en virtud de los sistemas que utiliza y los datos que recaba con motivo de sus actividades diarias, por lo que de conformidad con el artículo 35 de la LGPDPPSO, ha elaborado el presente documento en el que se encuentran las medidas de seguridad técnicas, físicas y administrativas, para garantizar un cuidado adecuado de los datos personales que se encuentran en su poder en virtud de sus actividades, a través de mecanismos de confidencialidad, integridad y disponibilidad.

Dicho documento cuenta con los requisitos mínimos establecidos en la LGPDPPSO, como son:

- Inventario de datos personales y de los sistemas de tratamiento;
- Funciones y obligaciones de las personas que traten datos personales;
- Análisis de riesgos;
- Análisis de brecha;
- Plan de trabajo;
- Mecanismos de monitoreo y revisión de las medidas de seguridad, y
- Programa general de capacitación.

2. OBJETIVO.

En cumplimiento al marco normativo en materia de protección de datos personales, esta S.N.C. ha establecido las acciones, políticas, mecanismos y programas a seguir a efecto de garantizar a todos los titulares de datos personales el derecho constitucional a la protección de datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El Documento de Seguridad tiene como objetivo dar cuenta de las medidas técnicas, físicas y administrativas, que Banjercito utiliza para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que tiene en su poder.

Para tal efecto, se tomaron en cuenta los avances tecnológicos, la naturaleza de la información almacenada, el contexto en el que ocurren los tratamientos, los riesgos a los que está expuesta la Institución, y el ciclo de vida de los datos recabados, para estar en condiciones de implementar una mejora continua en la protección de datos personales, dando cumplimiento a los principios rectores en la materia: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

3. ALCANCE.

El presente documento es de observancia obligatoria para todos los servidores públicos de Banjercito que intervienen en el tratamiento de datos personales que se encuentren en posesión de esta S.N.C., o bien cualquier otra persona que en virtud de los servicios prestados a Banjercito, tenga acceso a los datos personales, independientemente del sistema en el que se encuentren dichos datos.

Por lo anterior, todo el personal involucrado de Banjercito, está obligado a conocer y aplicar las medidas de seguridad tendientes a garantizar a la protección de datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad. Manteniendo absoluta confidencialidad al respecto, aun después de que finalice su participación como personal involucrado en el tratamiento de datos personales, o bien, por finalizar la relación laboral con Banjercito.

4. INVENTARIO DE DATOS PERSONALES Y DE SISTEMAS DE TRATAMIENTO

A efecto de llevar a cabo sus funciones (operaciones de banca y crédito), Banjercito obtiene datos personales a través de diversos medios como es el reclutamiento de personal, el servicio médico, etc. Cada uno de los datos recabados tienen por objeto cumplir con los requisitos de identificación por el personal, de acuerdo a la normatividad vigente y aplicable.

Se entiende por datos personales toda aquella información concerniente a una persona física, identificada e identificable, es decir, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

Los datos personales se pueden mantener de cualquier modo, sea alfabética, numérica, gráfica, fotográfica o sonora, (por citar algunas), y puede estar contenida en cualquier soporte como en papel, equipo informático, grabado en algún medio óptico etc.

Por lo anterior, con fundamento en el art. 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en relación con lo previsto en el artículo 33, fracción III de la LGPDPPSO, Banjercito cuenta el inventario de datos personales, clasificados por el medio de obtención de dichos datos, los cuales contienen la información básica de cada tratamiento de datos personales, en el que se considera al menos la siguiente información:

I. Medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
II. Finalidades de cada tratamiento de datos personales;
III. Catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
IV. Formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V. Lista de servidores públicos que tienen acceso a los sistemas de tratamiento;
VII. Destinatarios o terceros receptores de las transferencias que se efectúen.

A efecto de dar cumplimiento a la normatividad aplicable en materia de protección de datos, adjunto al presente se agrega el "Inventario de datos personales y de los sistemas de tratamiento" aplicable en esta S.N.C. conforme a lo siguiente:

- **Anexo 1.** Inventario de datos personales de empleados y servicio médico
- **Anexo 2.** Inventario de Datos personales de clientes y usuarios

Los datos personales referidos en el inventario, son resguardados en los sistemas automatizados que maneja Banjercito, de acuerdo a las medidas establecidas por las Direcciones de Tecnologías de la Información y Comunicaciones y la Subdirección de Seguridad de la Información.

Asimismo, los datos que se generan de manera física, son resguardados por la Gerencia DE coordinación de Archivos conforme la normatividad aplicable.

- **FORMATOS A TRAVÉS DE LOS CUALES SE RECABAN DATOS PERSONALES.**

A efecto de que Banjercito recabe los datos personales que son utilizados dentro de la Institución, con el fin de cumplir con las tareas encomendadas a cada uno de los puestos de la estructura organizacional, utiliza los formatos que a continuación se mencionan:

FORMATOS A TRAVÉS DE LOS CUALES SE RECABAN DATOS PERSONALES.	
UA	**FORMATOS**
Dirección de Crédito.	1. Carta Secore. 2. Carta de Designación de Notaria.
Dirección de Servicios Bancarios Fronterizos.	3. Formato libre de cambio de número de TDC. 4. Declaración de falta de documentos.
Dirección Jurídica Fiduciaria.	5. Formato de solicitud de avalúos de bienes Inmuebles. 6. Formato de solicitud de avalúos de bienes muebles.
Dirección de Factor Humano.	7. Solicitud de préstamo a corto plazo. 8. Solicitud de préstamo para adquisición de bienes de consumo duradero. 9. Certificado médico. 10. Referencia y Contra referencia a Hospitales en Convenio. 11. Constancia de Derechohabiencia. 12. Consentimiento informado para revisión médica deportiva (personal funcionario). 13. Consentimiento informado para revisión médica deportiva (personal operativo). 14. Curva de tensión arterial. 15. Hoja diaria de consulta.

Dirección de Administración de Bienes y Servicios	16. Examen médico (SEP). 17. Informe médico. 18. Historia clínica odontológica. 19. Solicitud de empleo. 20. Curriculum versión pública. 21. Aviso de Privacidad integral para los procedimientos de contratación del Banco Nacional del Ejército. 22. (Anexo III o Anexo IV) Acreditación de existencia legal. 23. (Anexo V) Restricciones del artículo 50 y 60 de la Ley. 24. (Anexo VII) Escrito de declaración de integración del licitante. 25. (Anexo VIII) Nacionalidad Mexicana. 26. (Anexo IX) Margen de Preferencia (internacional). 27. (Anexo IX) Margen de preferencia (nacional). 28. (Anexo XI) Formato de interés en participar en la junta de aclaraciones. 29. Aclaración de Convocatoria. 30. (Anexo XII) Manifiesto de micro, pequeñas y medianas empresas (MIPYMES). 31. (Anexo XIV) Formato de convenio de participación conjunta. 32. Escrito de entrega de opinión positiva de Obligaciones fiscales previo a la firma del contrato. 33. Escrito de entrega de opinión positiva de obligaciones fiscales de seguridad social previo a la firma del contrato. 34. Escrito de entrega de opinión positiva de Obligaciones Patronales (INFONAVIT). 35. (Anexo XVI) Formato para recibir toda clase de notificaciones. 36. Carta de Garantía de Calidad y/o vicios ocultos. 37. Carta de Garantía de Responsabilidad Civil. 38. Carta de Datos Bancarios . 39. Carta de Oferta. 40. Tarjeta de Resguardo Personal de Bienes.
Subdirección de Seguridad Institucional	41. Formato para la elaboración de credenciales institucionales. 42. Formato Solicitud de Fondo de Ahorro y de Trabajo.

Dirección de Fondos de Ahorro y del Trabajo.	43. Formato Cambio de Forma de Pago a Pensionados.
Dirección de Banca Electrónica.	44. Solicitud/Contrato del Servicio de Banca Electrónica.
	45. Solicitud Relativo al Producto Bancario Denominado: Banje – Nómina.
	46. Solicitud Relativo al Producto Bancario Denominado: Banje – Nómina (Beca mayor de edad).
	47. Solicitud Relativo al Producto Bancario Denominado: Banje – Nómina (Beca menor de edad).
	48. Solicitud Relativo al Producto Bancario Denominado: Banje – Nómina (Pensionados).
	49. Solicitud Relativo al Producto Bancario Denominado: Producto Básico de Nómina.
	50. Formato Actualización de Beneficiarios Producto Banje – Nómina y Básico de Nómina.
	51. Actualización de Representante Legal para cuentas "Banje – Nómina Becas Menor de Edad".
	52. Formato de Solicitud de Trámite (Banje – Nómina y Básico de Nómina).
	53. Solicitud de Tarjeta de Débito Adicional.
	54. Solicitud de Trámite (Tarjeta de Crédito)
	55. Solicitud de Tarjeta de Crédito (Titular)
	56. Solicitud de Servicio de Pago Automático a Tarjetas de Crédito con cargo a cuenta de cheques.
	57. Solicitud de Servicio de Pago Automático a Tarjetas de Crédito con cargo a cuenta de cheques para empleados.
	58. Solicitud de Tarjeta de Crédito (Adicional).
	59. Solicitud de Traspaso de saldos de tarjeta de Crédito (otros bancos) a Tarjeta de Crédito Banjercito.
	60. Formato de Autorización de Cargo en caso de Baja en el Servicio.
Dirección de Banca Comercial.	61. Solicitud Relativo al Producto Bancario Denominado: Banje – Nómina.
	62. Consulta al Buró de Crédito.
	63. Solicitud de avalúo de Bienes Inmuebles.
	64. Formato para pago de pasivos.
	65. Carta de Declaración del Origen de los Recursos.

	66. Solicitud de Fondo de Ahorro y del Trabajo.
	67. Compra – Venta Moneda Extranjera.
	68. Orden de Pago por medio de SPEI.
	69. Orden de Pago Internacional.
	70. Formato para Solicitar la Domiciliación.
	71. Formato para Cancelar la Domiciliación.
	72. Formato para Objetar Cargos por Domiciliación.
	73. Formato de Solicitud de Portabilidad.
	74. Solicitud de Tarjeta de Crédito Básica.
	75. Solicitud de Tarjeta de Crédito Trad. Clásica Rosa.
	76. Solicitud de Tarjeta de Crédito Trad. Clásica.
	77. Solicitud de Tarjeta de Crédito Trad. Infinite.
	78. Solicitud de Tarjeta de Crédito Trad Oro.
	79. Solicitud de Tarjeta de Crédito Trad. Platinum.
	80. Solicitud de Productos de Captación/ entrevista para persona física.
	81. Formato para solicitar ante sucursales la transferencia de los recursos correspondientes a Prestaciones Laborales.
	82. Acuse de cancelación de la transferencia de recursos correspondientes a prestaciones laborales.
	83. Datos del Inmueble a adquirir.
	84. Autorización para solicitar reporte de crédito personas físicas.
Subdirección de Prevención de Operaciones Ilícitas.	85. Carta de declaración del origen de los recursos.
	86. Formato origen/destino de los recursos para empleados.
	87. Formato de Visita domiciliaria.
	88. Justificación del servicio de caja de seguridad.
Centro de Atención a Clientes Banjercito.	89. Formato de aclaración que se utiliza para el producto de Tarjeta y Préstamos, generado en nuestro sistema de aclaraciones.
	90. Formato de aclaración para el producto de fallecimiento, generado en nuestro sistema de aclaraciones.
	91. Formato de aclaración manual, utilizado en caso de no ser posible ingresar aclaración a través de nuestro sistema.
Subdirección de Gestión Documental.	92. Formato de Guía Simple.
	93. Formato de Inventario (general).

Unidad de Transparencia	94. Formatos que se emplean de conformidad con los Lineamientos Internos de Organización y Conservación de archivos Banjercito. 95. Formato Solicitud de ejercicio de derechos ARCO.

Asimismo, aclara que existen 7 formatos repetidos, reportados en su momento por las Direcciones de Banca Comercial, Crédito y Administración de Bienes y Servicios y la Subdirección de Seguridad Institucional.

Dirección de Crédito y Dirección de Banca Comercial	1. Solicitud/Entrevista Banje-Auto Banjercito. 2. Solicitud Crédito Hipotecario/ Entrevista. 3. Solicitud Crédito de Adquisición de Bienes de Consumo Duradero / Entrevista. 4. Solicitud Crédito de Liquidez / Entrevista. 5. Solicitud Préstamos Quirografarios / Entrevista. 6. Solicitud Aval /Entrevista.
Dirección de Administración de Bienes y Servicios y Subdirección de Seguridad Institucional	7. Resguardo de Objetos

Cabe señalar, que por lo que respecta a los formatos enlistados reportados por la Dirección de Administración de Bienes y Servicios, se precisa que se tratan de "escritos en formato libre", donde obra nombre completo y firma del represente legal del proveedor licitante o de la persona física y/o persona física con actividad empresarial licitante, por lo que el mismo, se enuncia a efecto de que sea considerado como un documento donde se asientan datos personales de carácter confidencial, sin que ello deba considerarse como un Formato propio del Banco y el cual puede variar según la contratación de que se trate:

- Escrito de entrega de opinión positiva de Obligaciones fiscales previo a la firma del contrato: Los licitantes deberán presentar dentro de su proposición, un escrito en formato libre, preferentemente en papel membretado y firmado por su representante legal en el que manifiesten que al momento de suscribir su proposición cuentan con la opinión positiva vigente expedida por el SAT que acredite que está al corriente de sus obligaciones fiscales y que en caso de resultar adjudicado la presentará previo a la formalización del contrato.

- Escrito de entrega de opinión positiva de obligaciones fiscales de seguridad social previo a la firma del Contrato.

Los licitantes deberán presentar dentro de su proposición, un escrito en formato libre, preferentemente en papel membretado y firmado por su representante legal en el que manifiesten que al momento de suscribir su proposición cuentan con la opinión positiva vigente expedida por el IMSS que acredite que está al corriente de sus obligaciones en materia de seguridad social y que en caso de resultar adjudicado la presentará previo a la formalización del contrato.

- Escrito de entrega de opinión positiva de Obligaciones Patronales (INFONAVIT)
  Los licitantes deberán presentar dentro de su proposición, un escrito en formato libre, preferentemente en papel membretado y firmado por su representante legal en el que manifiesten que al momento de suscribir su proposición cuentan con la opinión positiva vigente expedida por el INFONAVIT que acredite que está al corriente de sus obligaciones en materia de aportaciones patronales y entero de descuentos y que en caso de resultar adjudicado la presentará previo a la formalización del contrato.

5. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

De conformidad con lo establecido en el art. 83 de la LGPDPPSO, el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, supervisando el debido cumplimiento a las medidas implementadas por la Institución para el cumplimiento de la normatividad aplicable.

En el tratamiento de datos personales se observan tres figuras importantes, donde cada uno de ellos toma un rol correspondiente, dichas figuras son: el Titular, el Responsable y el Encargado.

a) El titular. Es la persona física a quien pertenecen los datos personales, es el dueño de los mismos, aunque éstos se encuentren en posesión de un tercero para su tratamiento.

b) El responsable. Es Banjercito, es el Sujeto Obligado que establece las finalidades del tratamiento, así como el uso que se le dará a los datos personales, el tipo de datos que se requieren por parte del Titular, la forma en que se obtienen, se almacenan y se suprimen, así como los casos en los que se divulgaran, entre otros factores.

c) El encargado. Es la persona física o moral ajena a Banjercito que trata los datos personales a nombre y por cuenta del responsable. Se considera encargados aquellas empresas a las que Banjercito contrata para proporcionar algún servicio en específico. Si el encargado tratara los datos personales para finalidades distintas a las especificadas por el responsable, estaría sujeto a las sanciones previstas por la ley, en caso de incumplimiento.

Todo servidor público de Banjercito, que en el ejercicio de sus funciones obtenga, use, registre, organice, conserve, elabore, utilice, comunique, difunda, almacene, posea, maneje, aproveche, divulgue, transfiera o disponga de datos personales, debe observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales y está obligado a cumplir con las siguientes disposiciones:

Al momento de recabar los datos personales:

- Dar un uso responsable, desde el momento de su obtención. No utilizar medios engañosos o fraudulentos para la obtención de los datos personales, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.
- Poner a disposición el Aviso de Privacidad que corresponda, de tal manera que el titular de los datos personales pueda conocer las características principales del tratamiento al que serán sometidos y cómo podrá ejercer sus derechos ARCO.
- Obtener el consentimiento del titular para el tratamiento de sus datos personales, salvo las excepciones previstas en los artículos 22 y 70 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Cuando se recaben datos personales sensibles, patrimoniales y financieros, el consentimiento del titular deberá ser expreso y por escrito. Fuera de los casos antes mencionados, como regla es válido el consentimiento tácito siempre y cuando se ponga a disposición de los titulares el Aviso de Privacidad que corresponda.
- Evitar la creación de bases de datos de carácter sensible, salvo que se justifique plenamente la necesidad del tratamiento para la consecución de finalidades legítimas y concretas relacionadas con las actividades de Banjercito.
- Recabar sólo aquellos datos personales que sean estrictamente necesarios para las finalidades para las que se obtienen.
-

Durante el manejo o utilización de los datos personales:

- Respetar la expectativa razonable de privacidad del titular de los datos personales.
- Limitar el tratamiento de los datos personales conforme a lo expuesto por el Aviso de Privacidad que corresponda y en los términos establecidos en la normatividad aplicable.
- Mantener los datos personales actualizados y correctos.
- Limitar el periodo de conservación de los datos personales al mínimo necesario.
- Implementar medidas de carácter administrativo, físico y técnico que garanticen la confidencialidad e integridad de los datos personales.
- Informar al titular de los datos personales, en caso de presentarse un incidente de seguridad de la información en el que exista una vulneración ocurrida en cualquier fase

del tratamiento que afecte de forma significativa derechos patrimoniales o morales de éste, en cuanto se confirme la vulneración sucedida por el Comité de Transparencia.
- Rendir cuentas al titular en caso de algún incumplimiento con relación a la protección de sus datos personales.

Una vez agotadas las finalidades que justificaron el tratamiento de los datos personales:
- Llevar a cabo la cancelación (Eliminación o supresión definitiva) de los datos personales cuando hayan concluido las finalidades que justificaron el tratamiento de los datos personales, previo bloqueo.

Asimismo, las funciones específicas de acuerdo al nivel jerárquico de cada una de las personas involucradas (niveles de mando y operativos), se encuentran inmersas en cada uno de los manuales internos que maneja la Institución, los cuales permiten a todo servidor público de la Institución la identificación de las tareas encomendadas a cada uno de los puestos de la estructura y de esa manera apoyar en el desempeño de sus funciones.

En caso de alguna vulneración a los Datos Personales que maneja esta Institución, los puestos de mando del área donde surja la vulneración, deberán notificar sobre dicho suceso al Oficial de Protección de Datos Personales, adscrito a la Unidad de Transparencia de conformidad con el Procedimiento de atención a incidentes de seguridad de la información que impliquen una vulneración a la seguridad de datos personales.

6. ANÁLISIS DE RIESGOS.

A efecto de realizar el análisis de riesgo correspondiente, se realizó la clasificación de los datos de acuerdo a su riesgo inherente conforme lo siguiente:

- **Riesgo inherente bajo**: Datos de identificación y contacto o información académica o laboral.

- **Riesgo inherente medio**: Datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más.

  También aquéllos que permitan inferir el patrimonio de una persona, datos de autenticación y cualquier otro que permita autenticar a una persona, datos jurídicos.

- **Riesgo inherente alto**: Datos personales sensibles, y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

- **Riesgo inherente reforzado**: Los datos de mayor riesgo son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante.

- **IDENTIFICACIÓN DE RIESGOS.**

Se identificaron los siguientes riesgos:

- Riesgo por tipo de dato.
- Riesgo por accesibilidad.
- Riesgo por nivel de anonimidad.

[redacted]

Para tal efecto se toma en cuenta el nivel de riesgo inherente por cada tipo de dato que se trate y el volumen de titulares de cada dato tratado, agrupados de la siguiente manera:

Agrupador	Rango de Datos
<500	Datos de hasta 500 personas
<5k	Datos entre 501 hasta 5,000 personas
<50k	Datos entre 5,001 hasta 50,000 personas
<500k	Datos entre 50,001 hasta 500,000 personas
>500k	Datos de más de 500,000 personas

De acuerdo a lo anterior, se establecen cinco niveles de riesgo:

- Nivel 1-**Bajo:**
  - El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas.
  - El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas.
  - El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas.

- Nivel 2-**Bajo medio**:
  - El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas.
  - El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas.

- Nivel 3-**Medio**:
  - El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante.
  - El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante.

- Nivel 4-**Medio alto**:
  - El nivel de riesgo inherente de los datos personales sea reforzado y se tengan hasta cinco mil (5000) personas.

- Nivel 5-**Alto**:
  - El nivel de riesgo inherente de los datos personales sea reforzado y se tengan más de cinco mil (5,000) personas.

[redacted]

De manera general, de acuerdo al puntaje identificado en cada riesgo, se clasificarán de la siguiente manera:

Puntos	Riesgo
1	Bajo
2	Bajo medio
3	Medio
4	Medio alto
5	Alto

El **riesgo por accesibilidad** se establece determinando la cantidad de personas que tienen la posibilidad de accesar a los datos personales que protege la Institución, en un periodo determinado. Entre mayor sea la accesibilidad, mayor es el riesgo para la información.

Agrupador Cantidad de accesos a los datos	Puntos por nivel de riesgo
≤ 20	1
>20 ≤ 200	2
> 200 ≤ 2,000	3
> 2,000	4

[redacted]

Una vez que se obtiene el Riesgo por accesibilidad, se debe de identificar que tan anónimos son los accesos a esta información, lo que se denomina **riesgo por tipo de entorno.** Esto representa la facilidad con la que podría ser identificado un atacante y los efectos negativos que tendrá, en caso de acceder o hacer un uso no autorizado de los datos tratados por Banjercito.

De acuerdo al entorno, se tienen los siguientes niveles de anonimidad, donde 1 implica baja anonimidad y 5 mayor anonimidad del atacante, es decir entre mayor anonimidad, mayor confianza tendrá el atacante para intentar vulnerar la seguridad.

Entorno	Nivel de Anonimidad
Físico	1
Red interna	2
Red inalámbrica	3
Red de terceros	4
Internet	5

[redacted]

7. SOLUCIONES PARA GARANTIZAR LA PROTECCIÓN DE DATOS.

Una vez establecido el nivel para cada uno de los riesgos establecidos, se identificaron las medidas de seguridad aplicables a Banjercito.

[redacted]

[redacted]

8. IMPLEMENTACIÓN.

Las medidas recomendadas contribuyen a la disminución del riesgo que pudiera presentarse en esta Institución.

[redacted]

Medidas aplicables para la información de los empleados de Banjercito.

[redacted]			
Control	**Parámetro**	**Carácter**	**Resultado**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de **controles por patrón** como política de seguridad	Necesario	[redacted]
Revisión de la Política de seguridad de la información:	Revisión anual o cuando exista una modificació	Necesario	

La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad	n a las medidas o procesos de seguridad, o las condiciones de riesgo		[redacted]

			[redacted]
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual	Necesario	
Atender las necesidades de seguridad cuando se trata con clientes: Todos los requisitos identificados	Se deben identificar todas las interacciones entre la organización y el cliente en los	Necesario	

de seguridad deben atenderse antes de dar acceso a los clientes, a los activos o información de la organización.	cuales se involucren datos personales. Deberán tratarse como ejercicio de Derechos ARCO con una autenticación previa		[redacted]
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido	Considerar dentro del inventario cualquier activo físico o lógico que almacene, procese, transmita u otorgue acceso datos personales o sensibles	Necesario	
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Estos contratos deben ser	Necesario	

y documentados en concordancia con la política de seguridad de la información de la organización	firmados por los empleados, contratistas y usuarios de terceros.		[redacted]
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y	Ninguno	Necesario	

procedimientos organizacionales, conforme a la importancia de su función en el trabajo.			[redacted]
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo con lo establecido en la LGPDPPSO	Necesario	

Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	Necesario
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno	Opcional

[redacted]

			[redacted]
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad	Opcional	

Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado	Opcional	[redacted]
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	Opcional	
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	Opcional	

terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.			[redacted]
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de Banjercito	Ninguno	Opcional	
Seguimiento y revisión de los servicios de terceros: Los servicios,	Revisiones anuales	Opcional	

reportes y registros provistos por una tercera parte deberán ser monitoreados y revisados regularmente. Se deberán ejecutar auditorías de estos elementos de manera periódica.		
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Realizar revisiones aleatorias de las bitácoras de acceso para identificar accesos no autorizados. Considerar una frecuencia semestral.	Opcional
Política de escritorios y pantallas limpias: Se deberá implementar una política de	Ninguno	Opcional

escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.			[redacted]
Análisis y especificación de los requerimientos de seguridad: Los requerimientos de nuevos sistemas o de mantenimientos de sistemas existentes deben especificar los controles de seguridad requeridos.	Debe existir una documentación de los requerimientos de seguridad para instalaciones, desarrollos y mantenimientos	Opcional	
Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de	Considerar la aprobación del cambio por parte del responsable de seguridad.	Opcional	

testa medidas de seguridad que requieren ser reforzadas, análisis de riego, análisis de brecha y plan de implementación de medidas de seguridad (plan de trabajo), con fundamento en los artículos 44, fracción II, 101 párrafo penúltimo, 103 de la LGTAIP; 65 fracción II, 99 párrafo penúltimo, 102 10 fracción IV y VII de la LFTAIP; y Trigésimo cuarto, párrafo primero, de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

procedimientos formales de control de cambios.	El procedimiento debe considerar la capacidad de realizar roll-back del cambio		[redacted]
Revisión técnica de aplicaciones después de cambios del sistema operativo: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio debe ser revisado y probado para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	La revisión de las condiciones de seguridad de la información debe ser realizada por personal de seguridad	Opcional	
Procedimientos y responsabilidades de respuesta a incidentes de seguridad de la información:	Incluir los criterios de tipificación de un incidente.	Opcional	

Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad			[redacted]
Colección de evidencias: Cuando a raíz de un incidente de seguridad de la información se requieran acciones legales y acciones de seguimiento contra una persona o empresa, se deben recolectar, retener y	Ninguno	Opcional	[redacted]

presentar evidencias de acuerdo a las reglas de la jurisdicción.			[redacted]
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista	Opcional	

[redacted]

Control	Parámetro	Carácter	Resultado
Controles contra código malicioso: Se	Ninguno	Necesario	[redacted]

deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.		
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Eliminar contraseñas de fábrica Evitar protocolos de comunicación en texto claro	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios,	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha	Necesario

las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	de acceso, usuario y cambios a realizar Asegurar que se registren las actividades de administración del sistema		[redacted]
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	Poner especial atención en los usuarios de altos privilegios.	Necesario	
Uso de contraseñas: Se deberá exigir a	Contraseña de mínimo 10 caracteres	Necesario	

los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas		
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear	Necesario
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único(ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario	Ninguno	Necesario
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las	Ninguno	Necesario

[redacted]

vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados			[redacted]
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación	Ninguno	Opcional	
Gestión del cambio: Los cambios en las instalaciones de procesamiento y	Considerar la autorización del responsable de seguridad	Opcional	

sistemas de información deben ser controlados	previo a cualquier cambio. Alinear las prácticas de gestión del cambio a las propuestas de ITIL	
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	Opcional
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	Opcional

			[redacted]
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes	Utilizar protocolo NTP	Opcional	
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo. En particular en los equipos que intervienen en el tratamiento de datos personales	Opcional	

[redacted]

[redacted]			
Control	Parámetro	Carácter	Resultado
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Ninguno	Necesario	[redacted]
Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados, llaves y tarjetas de	Necesario	

recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	acceso en archiveros y habitaciones que resguarden datos personales.		[redacted]
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	Necesario	
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos	Necesario	

cuando no se les necesite más, usando procedimientos formales	que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos		[redacted]
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	Necesario	
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, nombre completo de la persona que accede y cambios a realizar	Necesario	

utilizados en futuras investigaciones y monitoreo de control de accesos.		
Implementar un sistema de cámaras de seguridad	Ninguno	Necesario
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso	Considerar sitios donde se le de tratamiento a información física y electrónica. Considerar tarjetas de proximidad, teclados de combinación.	Opcional
Áreas de acceso público, carga y entrega: Los puntos de acceso tales como los de entrega, áreas de carga y otros puntos donde personas no autorizadas pueden entrar a las instalaciones, debe estar controladas y, si es posible, aisladas de las instalaciones	Ninguno	Opcional

[redacted]

donde se procesa información para evitar accesos no autorizados.			[redacted]
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado	Ninguno	Opcional	
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos, utilizar candados para equipos	Opcional	
Separación de la información en diferentes bases de datos e infraestructura.	Ninguno	Opcional	

9. ANÁLISIS DE BRECHA.

[redacted]

Medias aplicables para la información de los empleados de Banjercito.

[redacted]

No.		Totales		
		SI	NO	N/A
Medidas de seguridad basadas en la cultura personal				
1	A.1.1 · ¿Tienes una política de escritorio limpio?	[redacted]		
2	A.1.2 · ¿Tienes hábitos de cierre y resguardo de datos personales?			
3	A.1.3 · ¿Mantienes las impresoras, los escáneres, copiadoras y buzones libres de documentos cuando no están en uso?			
4	A.1.4 · ¿Realizas gestión de bitácoras, usuarios y accesos?			
5	A.2.1 · ¿Realizas destrucción segura de documentos físicos?			

6	A.2.2 · ¿Realizas eliminación segura de información en equipo de cómputo, celulares, tabletas y medios de almacenamiento electrónico?	[redacted]
7	A.2.3 · ¿Fijas periodos para la retención y destrucción de información?	
8	A.2.4 · ¿Tomas precauciones cuando reutilizas o reciclas documentos, equipos de cómputo, celulares, tabletas y medios de almacenamiento?	
9	A.3.1 · ¿Informas al personal sobre sus deberes mínimos de seguridad y protección de datos?	
10	A.3.2 · ¿Fomentas la cultura de la seguridad de la información al interior de la organización?	
11	A.3.3 · ¿Difundes noticias sobre temas de seguridad entre el personal de la organización?	
12	A.3.4 · ¿Previenes al personal sobre la ingeniería social?	

13	A.3.5 · ¿Cuentas con procedimientos para realizar subcontrataciones relacionadas con el tratamiento de datos personales?	[redacted]
14	A.4.1 · ¿Cuentas con procedimientos para la atención y notificación de vulneraciones de seguridad?	
15	A.4.2 · ¿Realizas revisiones y auditorías a los sistemas de tratamiento de datos personales?	[redacted]
16	A.5.1 · ¿Realizas respaldos periódicos de los datos personales?	

[redacted]

No.		Totales		
		SI	NO	N/A
Medidas de seguridad en el entorno de trabajo físico				
1	B.1.1 · ¿Cuentas con alertas en el entorno de trabajo?	[redacted]		
2	B.1.2 · ¿Mantienes registros del personal con acceso al entorno de trabajo?			

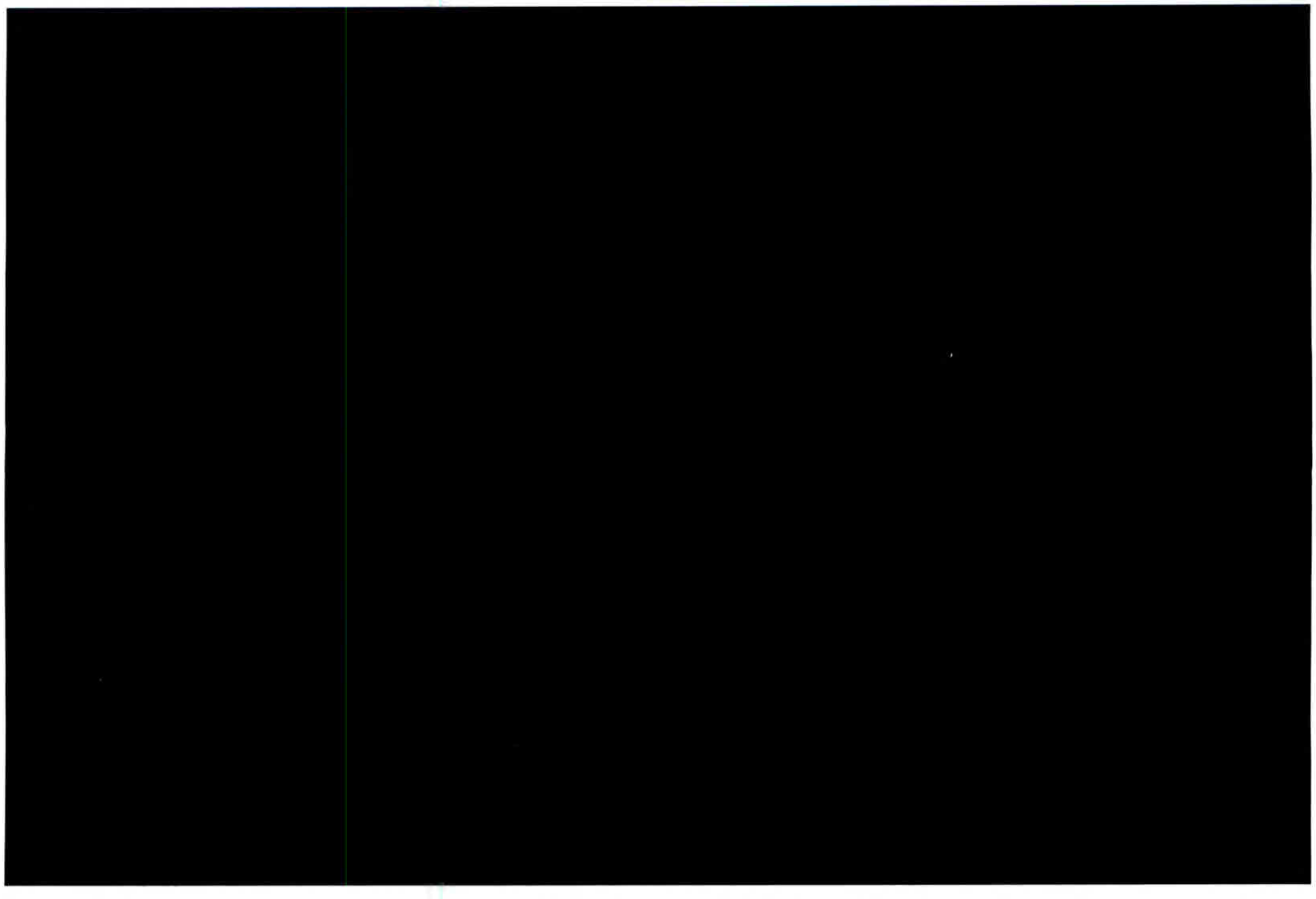
3	B.2.1 · ¿Utilizas cerraduras y candados para resguardar los datos personales?	[redacted]
4	B.2.2 · ¿Cuentas con elementos disuasorios en el entorno de trabajo?	
5	B.2.3 · ¿Tomas acciones para minimizar el riesgo oportunista?	
6	B.3.1 · ¿Cuentas con procedimientos para la aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico?	
7	B.3.2 · ¿Mantienes en movimiento copias controladas de la información, no la fuente original o principal?	
8	B.3.3 · ¿Usas servicios de mensajería o correo certificado ?	

Se testa medidas de seguridad que requieren ser reforzadas, análisis de riego, análisis de brecha y plan de implementación de medidas de seguridad (plan de trabajo), con fundamento en los artículos 44, fracción II, 101 párrafo penúltimo, 103 de la LGTAIP; 65 fracción II, 99 párrafo penúltimo, 102 y 110 fracción IV y VII de la LFTAIP; y Trigésimo cuarto, párrafo primero, de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

[redacted]

No.	Totales		
	SI	**NO**	**N/A**
Medidas de seguridad en el entorno de trabajo digital			
C.1.1 · ¿Realizas actualizaciones de sof tware al equipo de cómputo, celulares y tabletas?	[redacted]		
C.2.1 · ¿Revisas periódicamente el software y las aplicaciones instaladas en el equipo de cómputo?			
C.3.1 · ¿Utilizas contraseñas y/o cifrado para proteger los datos personales?			

4	C.3.2 · ¿Utilizas contraseñas sólidas y seguras?					
5	C.3.3 · ¿Realizas bloqueo y cierre de sesiones?					
6	C.3.4 · ¿Administras el acceso a los sistemas de tratamiento, por parte de los usuarios?					
7	C.4.1 · ¿Revisas la configuración de seguridad de los equipos de cómputo, celulares y tabletas?					
8	C.5.1 · ¿Cuentas con herramientas antimalware y de filtrado de tráfico de red?					
9	C.5.2 · ¿Tienes establecidas reglas para la navegación segura en Internet?					
10	C.5.3 · ¿Cuentas con reglas para divulgar información?					
11	C.5.4 · ¿Utilizas conexiones seguras?					
12	C.6.1 · ¿Validas el destinatario de una comunicación, antes de realizarla?					
13	C.6.2 · ¿Cuentas con procedimientos para proteger la información que envías y recibes?					



- **MEDIDAS NECESARIAS FALTANTES DE IMPLEMENTACIÓN.**

Medidas de seguridad basadas en la cultura personal:

Medidas que se implementan:

Medidas que requieren ser reforzadas:

[redacted]

Medidas de seguridad en el entorno de trabajo físico:

Medidas que se implementan:

[redacted]

Medidas que requieren ser reforzadas:

[redacted]

Medidas de seguridad en el entorno de trabajo digital:

Medidas que se implementan:

[redacted]

Medidas que requieren ser reforzadas

[redacted]

10. PLAN DE IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Medias de seguridad aplicables a la información de los empleados de Banjercito.

PLAN DE IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD		
Área responsable: Dirección de Factor Humano		
Medidas de seguridad faltantes o que requieren ser reforzadas	Acción de mejora	Fecha de atención
Medidas de seguridad basadas en la cultura personal		
A.1.4 · ¿Realizas gestión de bitácoras, usuarios y accesos?	[redacted]	

A.2.1 · ¿Realizas destrucción segura de documentos físicos?	[redacted]
A.2.2 · ¿Realizas eliminación segura de información en equipo de cómputo, celulares, tabletas y medios de almacenamiento electrónico	

	[redacted]
A.2.3 · ¿Fijas periodos para la retención y destrucción de información?	
A.2.4 · ¿Tomas precauciones cuando reutilizas o reciclas documentos, equipos de cómputo, celulares, tabletas y medios de almacenamiento?	
A.3.1 · ¿Informas al personal sobre sus deberes mínimos de seguridad y protección de datos?	[redacted]

A.3.4 · ¿Previenes al personal sobre la ingeniería social?	[redacted]
A.3.5 · ¿Cuentas con procedimientos para realizar subcontrataciones relacionadas con el tratamiento de datos personales?	

A.4.1 · ¿Cuentas con procedimientos para la atención y notificación de vulneraciones de seguridad?	[redacted]

	[redacted]
A.4.2 · ¿Realizas revisiones y auditorías a los sistemas de tratamiento de datos personales?	[redacted]
A.5.1 · ¿Realizas respaldos periódicos de los datos personales?	[redacted]

	[redacted]

Medidas de seguridad en el entorno de trabajo físico

B.1.2 · ¿Mantienes registros del personal con acceso al entorno de trabajo?	[redacted]
B.2.1 · ¿Utilizas cerraduras y candados para resguardar los datos personales?	

B.2.2 · ¿Cuentas con elementos disuasorios en el entorno de trabajo?	[redacted]
B.2.3 · ¿Tomas acciones para minimizar el riesgo oportunista?	

Medidas de seguridad en el entorno de trabajo digital

C.2.1 · ¿Revisas periódicamente el software y las aplicaciones instaladas en el equipo de cómputo?	[redacted]
C.3.1 · ¿Utilizas contraseñas y/o cifrado para proteger los datos personales?	
C.3.4 · ¿Administras el acceso a los sistemas de tratamiento, por parte de los usuarios?	

	[redacted]
C.4.1 · ¿Revisas la configuración de seguridad de los equipos de cómputo, celulares y tabletas?	
C.5.1 · ¿Cuentas con herramientas antimalware y de filtrado de tráfico de red?	
C.5.2 · ¿Tienes establecidas reglas para la navegación segura en Internet?	

C.5.3 · ¿Cuentas con reglas para divulgar información?

[redacted]

C.5.4 · ¿Utilizas conexiones seguras?

Capacitación al personal de Servicio Médico	[redacted]

11. MECANISMOS DE MONITOREO Y REVISIÓN DE MEDIDAS DE SEGURIDAD.

El mecanismo que se prevé por parte de este sujeto obligado, son las auditorias que lleva a cabo el Oficial de Protección de Datos Personales, de conformidad con el programa aprobado por el H. Comité de Transparencia, y el cual consiste en lo siguiente:

AUDITORÍA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

Objetivo
El presente procedimiento tiene como objetivos:

- Contribuir a la mejora en el tratamiento de los datos personales en posesión de la Institución.
- Evaluar las medidas y mecanismo implementados para el cumplimiento de las disposiciones previstas en la LGPDPPSO y en los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Validar el proceso de tratamiento de datos personales que realizan las Unidades Administrativas de esta Sociedad Nacional de Crédito.
- Evaluar el cumplimiento de los principios de licitud, finalidad, proporcionalidad, lealtad, consentimiento, calidad, información, responsabilidad, así como a los deberes de seguridad y confidencialidad y obligaciones de la LGPDPPPSO, dentro los procedimientos que tratan datos personales.

Alcance
El presente procedimiento está dirigido al personal adscrito a todas las Unidades Administrativas de esta Sociedad Nacional de Crédito que serán sometidas a las auditorías en materia de protección de datos personales.

Políticas Particulares

Las fases de la auditoría son las siguientes:

- Notificación de inicio de auditoría.
- Revisión documental.
- Visita a la Unidad Administrativa.
- Identificación de hallazgos.
- Informe
- Seguimiento a los hallazgos.

Las auditorías en cuestión se realizarán al total de las Unidades Administrativas de la institución, conforme al calendario aprobado por el Comité de Transparencia, teniendo como sede la oficina donde se establezca el área auditada.

El informe final y la cédula de observaciones se deberá elaborar en un plazo no mayor a 20 días hábiles contados a partir de la conclusión de la visita de inspección y recopilación de información. Una vez formalizados dichos documentos, se tendrán que remitir a la Unidad Administrativa auditada en un plazo no mayor a 5 días hábiles.

En caso de que los hallazgos no sean aceptados por la Unidad Administrativa auditada, la Unidad de Transparencia girará cédula de aceptación de riesgos, en caso de no conformidad, se dará vista al Órgano Interno de Control y a la Dirección General.

Los Titulares de las Unidades Administrativas tendrán un plazo máximo de 45 días hábiles para atender las observaciones y/o informar los avances que se susciten.

El Oficial de Protección de Datos Personales dará el debido seguimiento a la atención de los hallazgos y a las actividades que se requieran para el cumplimento de la LGPDPPSO.

Narrativa

No.	Responsable	Actividad
1	Oficial de Protección de Datos Personales.	Somete en la 11ª. sesión ordinaria del Comité de Transparencia la aprobación del calendario de auditorías a ejecutar en el año subsecuente, considerando las circunstancias y posibilidades que la Institución tenga para atender la misma.

2	Comité de Transparencia.	Aprueba el calendario de auditorías propuesto.
3	Oficial de Protección de Datos Personales.	Notifica vía oficio a las Unidades Administrativas que serán auditadas una semana antes de iniciar los trabajos, a fin de recibir su confirmación y asignación del personal destinado para atenderla. Nota: Adjunta formato denominado "ciclo de vida", mismo que se deberá entregar al iniciar la auditoría.
4		Realiza el levantamiento del acta de inicio, posteriormente hace entrega del primer oficio de solicitud de información.
5		Remite los oficios complementarios con la finalidad de solicitar la información que considere pertinente.
6		Notifica vía correo electrónico al personal de la Unidad Administrativa auditada, la fecha y hora en la que acudirá a realizar las entrevistas y visitas de inspección.
7		Requisita la cédula de trabajo por cada visita realizada.
8		Genera informe final y cédula de observaciones una vez concluida la visita de inspección y recopilación de información de conformidad con el calendario aprobado.
9		Reúne a los funcionarios públicos designados para la aceptación de hallazgos.
10		Remite el informe final y la cédula de observaciones a la Unidad Administrativa correspondiente.
11	Titular de la Unidad Administrativa	Asegura que el personal a su cargo atienda la totalidad de las observaciones y/o informe los avances obtenidos.

		Fin del procedimiento.

12. PROGRAMA GENERAL DE CAPACITACIÓN.

La Unidad de Transparencia, forma parte del programa de inducción que la Dirección de Factor Humano desarrolla al interior de esta Sociedad Nacional de Crédito, en el cual se imparten a los empleados de nuevo ingreso los siguientes temas:

- Portal de Transparencia
- Acceso a la Información
  - Procedimiento de Acceso a la Información
  - Atención a Solicitudes de Acceso a la Información
  - Clasificación de la Información
  - Recurso de Revisión
  - Causas de Sanciones
- Índice de Expedientes Clasificados como Reservados
- Obligaciones de Transparencia
- Protección de Datos Personales
  - Obligaciones de Banjercito en materia de Datos Personales
  - Aviso de Privacidad
  - Derechos Arco
  - Solicitudes Arco
  - Vulneración de Datos Personales

Asimismo, en seguimiento al **"Programa de Capacitación en materia de Transparencia, Acceso a la Información, Protección de Datos Personales y temas relacionados 2021"**, y con la finalidad de refrendar nuestro compromiso para incentivar de manera permanente la construcción de una cultura de transparencia, acceso a la información y protección de datos personales al interior de esta Sociedad Nacional de Crédito, se invita al personal a tomar los cursos impartidos en línea a través del Centro Virtual de Capacitación (CEVINAI) como son:

1) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
2) Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública.
3) Introducción a la Ley General de Transparencia y Acceso a la Información Pública.
4) Introducción a la Ley General de Archivo.
5) Tratamiento de datos biométricos y manejo de incidentes de seguridad de datos personales.

Finalmente, se cuenta con la Programación de una serie de talleres, mismo que fue aprobado en la 12ª Sesión Ordinaria del Comité de Transparencia, celebrada el 30 de diciembre de 2019, mismo que debido a la Pandemia por COVID – 19 fue cancelado, sin embargo, será retomado para este 2021, incluyendo al menos los siguientes temas:

Aprobación del calendario de talleres en materia de transparencia acceso a la información pública y protección de datos personales, 2020, para la Alta Dirección de Banjercito, S.N.C., se establece lo siguiente:

Mes	Nombre del taller
Enero	Taller de clasificación de la información y búsqueda exhaustiva de la información.
Febrero	Taller de Criterios emitidos por el INAI.
Marzo	Taller de elaboración de Pruebas de Daño.
Abril	Taller de atención a solicitudes de acceso a la información.
Mayo	Taller de atención a solicitudes de derechos ARCO.
Junio	Taller de actualización del Índice de Expedientes Clasificados como Reservados (IECR).
Julio	Taller de actualización del Sistema de Portales de Obligaciones de Transparencia (SIPOT).
Agosto	Taller de elaboración de versiones públicas.
Septiembre	Talleres de elaboración de Avisos de Privacidad.
Octubre	Taller de atención a vulneraciones a seguridad de datos personales.
Noviembre	Taller de implementación de medidas de seguridad administrativas, físicas y técnicas para la protección de datos personales.
Diciembre	Taller de borrado seguro de datos personales.

13. ACTUALIACIÓN DEL DOCUMENTO DE SEGURIDAD.

Con fundamento en el artículo 36 de la LGPDPPSO, Banjercito actualizará el documento de seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y

IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

14. GLOSARIO

Banjercito	Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C.
Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
Bloqueo	La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Datos personales	Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
Datos personales Sensibles	Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual
Documento de Seguridad	Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
Encargado	La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Medidas de seguridad	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales
Medidas de seguridad administrativas	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales

Medidas de seguridad físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.
Responsable	Es el Sujeto Obligado, en este caso BANJERCITO.

Responsable del Sistema	Siempre será el Titular de la Unidad Administrativa donde se administre el Sistema de que se trate, quien deberá: - Dar aviso a la Unidad de Transparencia de Banjercito, de los sistemas que involucren tratamiento de datos personales, a cargo de su Unidad. - Designar al Administrador del Sistema. - Validar la información entregada por lo titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado.
Sistema de Gestión	Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.
Titular	La persona física a quien corresponden los datos personales.
Transferencia	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.
Tratamiento de datos personales	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

15. MARCO JURÍDICO.

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- Artículo 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

- Ley Orgánica de la Administración Pública Federal, cuya última reforma fue publicada en el Diario Oficial de la Federación el 11 de enero de 2021.

- Lineamientos generales de protección de datos personales para el sector público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018.

- Lineamientos que establecen los parámetros, modalidades y procedimiento para la portabilidad de datos personales, publicados en el Diario Oficial de la Federación el 12 de febrero de 2018.

Normatividad Interna:

- Ley Orgánica del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. y su Reglamento.

- Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C.

INVENTARIO DE DATOS PERSONALES DE LA DIRECCIÓN DE RECURSOS HUMANOS.
SISTEMA INTEGRAL DE RECURSOS HUMANOS (SIRH), QUE A SU VEZ CONTIENE LOS MÓDULOS: A) SISTEMA MÉDICO DE BANJERCITO (SISMED), B) SERVICIO ODONTOLÓGICO.

Datos personales	DE IDENTIFICACIÓN Y CONTACTO							
	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destruccón	Ubicación
Nombre completo	✓	Formularios físicos y electrónicos		Para la integración del expediente personal, elaboración de nombramiento, trámites administrativos (invitaciones a cursos, evaluaciones de desempeño, asignación de metas, invitaciones a cumpleañeros, etc.), consultas e identificación del empleado.		Autoridades y entidades regulatorias internas y externas. Secretaría de la Función Pública, Secretaría de Hacienda y Crédito Público y Secretaría de Economía.		Servicios informáticos, administrados por la Dirección Informática de Banjercito, ubicado en Av. Industrial Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo.
Estado civil	✓							
Registro federal de contribuyentes (RFC)	✓		✓					
Clave única de Registro de Población (CURP)	✓		✓					
Lugar de nacimiento	✓							
Fecha de nacimiento	✓							
Nacionalidad	✓							
Domicilio particular	✓		✓					
Teléfono particular	✓							
Telefono celuar	✓		✓					
Número de cuenta de Afore	✓		✓					
Número de cartilla militar	✓							
Correo electrónico	✓							
Firma autógrafa	✓		✓					
Firma electrónica	✓		✓					
Sexo	✓							
Matrícula	✓							
Edad	✓							
Fotografía	✓		✓					
Referencias personales	✓		✓					
Datos personales	**SOBRE CARACTERISTICAS FÍSICAS**							
	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destruccón	Ubicación
Color de piel	✓	Formulario físico y electrónico		El objetivo primordial se basa en satisfacer el cumplimiento de la NOM/024 del expediente clínico electrónico, para ser una herramienta que permita llevar el control de las atenciones que se realizan en el Servicio Médico de Banjercito		Autoridades y entidades regulatorias internas y externas. Secretaría de la Función Pública, Secretaría de Hacienda y Crédito Público y Secretaría de Economía.		Servicios informáticos administrados por la Dirección Informática de Bnajercito, ubicado en A.v. Industria Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo
Color de cabello	✓							
Señas particulares	✓							
Estatura	✓							

Peso	✓							
Cicatrices	✓							
Tipo de Sangre	✓		✓					
Datos personales	**BIOMÉTRICOS**							
	¿Da tratamiento a estos datos?	**Medios de obtención**	**Datos sensibles**	**Finalidad del tratamiento**	**Terceros receptores (Remisiones)**	**Terceros receptores (Transferencias)**	**Bloqueo, Cancelación, Supresión o Destruccón**	**Ubicación**
Imagen del iris	✓	Formulario electrónico	✓	Registro de asistencia de todo el personal de Banjercito				Servicios informáticos administrados por la Dirección Informática de Bnajercito, ubicado en A.v. Industria Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo
Huella dactilar	✓		✓					
palma de la mano								
Datos personales	**LABORALES**							
	¿Da tratamiento a estos datos?	**Medios de obtención**	**Datos sensibles**	**Finalidad del tratamiento**	**Terceros receptores (Remisiones)**	**Terceros receptores (Transferencias)**	**Bloqueo, Cancelación, Supresión o Destruccón**	**Ubicación**
Puesto o cargo que desempeña	✓	Formularios físicos y electrónicos		Para conocer su experiencia laboral, integración de expediente y fines estadisticos.Información generada durante los procedimientos de reclatamiento, selección y contratación.		Autoridades y entidades regulatorias internas y externas. Secretaría de la Función Pública, Secretaría de Hacienda y Crédito Público y Secretaría de Economía.		Servicios informáticos administrados por la Dirección Informática de Bnajercito, ubicado en A.v. Industria Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo
Tipo de plaza que ocupa	✓							
Fecha de ocupación del puesto	✓							
Motivo de renuncia								
Domicilio de trabajo								
Correo electronico institucional	✓							
Telefono institucional	✓							
Referencias laborales	✓							
Experiencia/Capacitación	✓							
Datos personales	**ACADÉMICOS**							
	¿Da tratamiento a estos datos?	**Medios de obtención**	**Datos sensibles**	**Finalidad del tratamiento**	**Terceros receptores (Remisiones)**	**Terceros receptores (Transferencias)**	**Bloqueo, Cancelación, Supresión o Destruccón**	**Ubicación**
Nivel de estudios	✓	Formularios físicos y electrónicos		Para conocer y verificar su escolaridad y perfil profesional. Otorgamiento de becas y capacitación.		Autoridades y entidades regulatorias internas y externas. Secretaría de la Función Pública, Secretaría de Hacienda y Crédito Público y Secretaría de Economía.		Servicios informáticos administrados por la Dirección Informática de Bnajercito, ubicado en A.v. Industria Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo
Nombre de los estudios	✓							
Grado de avance	✓							
Títulos	✓							
Cédula profesional	✓		✓					
Certificados	✓							
Reconocimientos	✓							
Idiomas que maneja	✓							

Datos personales	MIGRATORIOS							
	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destruccón	Ubicación
Entradas al pais	NO							
Salida del pais								
Tiempo de permanencia en el pais								
Calidad migratoria								
Derechos de residencia								
Aseguramiento								
Repatriación								

Datos personales	PATRIMONIALES Y/O FINANCIEROS							
	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destruccón	Ubicación
Bienes muebles	✓	Formularios físicos y electrónicos		Para trámites patronales ante IMSS e INFONAVIT, para efectos de cumplimiento de obligaciones en dicha materia. Cálculos de finiquitos, liquidaciones, descuentos de amortizaciones. Timbrado de nómina.		Autoridades y entidades regulatorias internas y externas. Secretaría de la Función Pública, Secretaría de Hacienda y Crédito Público y Secretaría de Economía.		Servicios informáticos administrados por la Dirección Informática de Bnajercito, ubicado en A.v. Industria Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo
Bienes Inmuebles	✓							
Información fiscal								
Número de seguridad social (NSS)	✓		✓					
Número de crédito Infonavit	✓		✓					
Créditos	✓							
Salario diario integrado (SDI)	✓							
Egreso	✓							
Cuentas bancarias	✓							
No. De tarjetas de crédito	✓							
Seguro	✓							
Afores	✓							

Datos personales	IDEOLÓGICOS							
	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destruccón	Ubicación
Postura religiosa/ideológica	NO							
Pertenencia a un partido/postura política								
Sindicato								

Datos personales	DE SALUD

	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destrucción	Ubicación
Antecedentes personales patológicos	✓	Formularios físicos, electrónicos y texto libre físico para prescribir las recetas médicas.	De conformidad con lo establecido en el artículo 3, fracción X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), todos los datos personales mencionados en este apartado, son considerados datos personales sensibles.	El objetivo primordial se basa en satisfacer el cumplimiento de la NOM/024 del expediente clínico electrónico, para ser una herramienta que permita llevar el control de las atenciones que se realizan en el Servicio Médico de Banjercito		Autoridades y entidades regulatorias, Instituto Mexicano del Seguro Social, Prestadores, proveedores de servicio de salud y empresas administradoras que sean contratadas por Banjercito, instituciones de seguros, asimismo, son compartidos con las sociedades de información crediticia a fin de verificar el historial crediticio.		Servicios informáticos, administrados por la Dirección Informática de Banjercito, ubicado en Av. Industrial Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo, y diferentes archiveros del Consultorio 2, 3, 4 y 5.
Médicos, quirurgicos;	✓							
Antecedentes personales no patológicos	✓							
Prenatales	✓							
Grupo sanguineo	✓							
Perinatales	✓							
Desarrollo psicosomético	✓							
Alergias	✓							
Medicamentos	✓							
Exposición a biomas	✓							
Hábitos higiénicos	✓							
Alimentación	✓							
Antecedentes ginecoobstétricos	✓							
Esquema de vacunación	✓							
Cardiovascular	✓							
Digestivo	✓							
Metabólico	✓							
Respiratorio	✓							
Neurológico	✓							
Hematológico	✓							
Musculo esquelético	✓							
Renal	✓							
Exploración física	✓							
Signos vitales	✓							
Laboratorios, gabinete, otros.	✓							
Resultado de estudios.	✓							
Indicaciones terapéuticas	✓							
Valoración clínica	✓							
Menarca	✓							
Adicciones	✓							

Datos personales	SOBRE VIDA SEXUAL							
	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destruccón	Ubicación
Inicio de vida sexual	✓	Formularios físicos, electrónicos y texto libre físico para prescribir las recetas médicas.	✓	El objetivo primordial se basa en satisfacer el cumplimiento de la NOM/024 del expediente clínico electrónico, para ser una herramienta que permita llevar el control de las atenciones que se realizan en el Servicio Médico de Banjercito		Autoridades y entidades regulatorias, Instituto Mexicano del Seguro Social, Prestadores, proveedores de servicio de salud y empresas administradoras que sean contratadas por Banjercito.		Servicios informáticos, administrados por la Dirección Informática de Banjercito, ubicado en Av. Industrial Militar, 1055, Col. Lomas de Sotelo, Alcaldía Miguel Hidalgo, y diferentes archiveros del Consultorio 2, 3, 4 y 5.
Padecimiento actual	✓		✓					
Papanicolaou	✓		✓					
Fecha de última mestruación	✓		✓					
Practicas o hábitos sexuales								

Datos personales	DE ORIGEN ÉTNICO O RACIAL							
	¿Da tratamiento a estos datos?	Medios de obtención	Datos sensibles	Finalidad del tratamiento	Terceros receptores (Remisiones)	Terceros receptores (Transferencias)	Bloqueo, Cancelación, Supresión o Destruccón	Ubicación
Pertecencia a un pueblo, etnia o región	NO							

Servidores públicos con acceso al Sistema de Recursos Humanos (SIRH)						
Administrador (a)	Responsable	Enlace de Datos Personales	Encargado de Datos	Operador (a)		
				Nombre	Cargo	Privilegios
Gerente de Desarrollo De Sistemas Interinstitucionales, Cap. 1/ro I.C.E. Flavio Solís López. Mantener actualizado el sistema, autorizar los accesos de los servidores públicos, determinar los privilegios y llevar un registro de los mismos	Director de Factor Humano. Myr. Inf. D.E.M. Outy Gómez Gómez. Supervisar los procedimientos de Factor Humano.	Subdir. Gestión del Factor Humano, Mtra. Yamel Gpe. Yaber Velez. Conocer el inventario de datos personales que se recaban y el flujo del tratamiento	Director Consultor de JACSU Consultores, S.C. Javier Chávez Suárez. Investigación socioeconómica de candidatos	CABRERA CUEVAS GUSTAVO	GERENTE DE ORGANIZACIÓN Y GESTIÓN DEL FACTOR HUMANO	o,c,u
				AGUILAR MENDOZA MARIA LETICIA	JEFE DE DEPARTAMENTO DE RECLUTAMIENTO Y CONTRATACIÓN	o,u,i
				CLEMENTE PAREDES OLGA	ANALISTA DEL DEPARTAMENTO DE GESTIÓN DEL DESEMPEÑO Y COMPETENCIAS	o,u,i
				ALCANTAR SEBASTIAN ANACARE	TÉCNICO ESPECIALIZADO DEL DEPARTAMENTO DE RECLUTAMIENTO Y CONTRATACIÓN	o,i,u
				GALINDO ZAMORA DANIEL	TÉCNICO ESPECIALIZADO DEL DEPARTAMENTO DE MOVILIDAD INTERNA	o
				JORGE RODRIGUEZ REGALADO	ENCARGADO DE OPERACIÓN	o,i,u
				GOMEZ GONZALEZ ERNESTO	ANALISTA DEL DEPARTAMENTO DE PRESTACIONES Y OBLIGACIONES DE SEGURIDAD SOCIAL	o
				VALENCIA DIAZ OSCAR	TECNICO ESPECIALIZADO DE DEPARTAMENTO DE RECLUTAMIENTO Y CONTRATACIÓN	o
				NAVA AVENDAÑO IGNACIO	ANALISTA DEL DEPARTAMENTO DE MOVILIDAD INTERNA	i,o,u,p
				DE LA CRUZ HERNANDEZ ABEL	ENCARGADO DE OPERACIÓN DEL DEPARTAMENTO DE PRESTACIONES Y OBLIGACIONES DE SEGURIDAD SOCIAL	o,u
				RAMIREZ RODRIGUEZ DEBORAH ALEJANDRA	ANALISTA DEL DEPARTAMENTO DE RECLUTAMIENTO Y ORGANIZACIÓN	o,i
				MURILLO AVILA PERLA LETICIA	GERENTE DE GESTIÓN DE NÓMINA Y PRESTACIONES	o,a,u,p
				VALDOVINOS AGUILAR THALIA SUSANA	ANALISTA DEL DEPARTAMENTO DE PRESTACIONES Y OBLIGACIONES DE SEGURIDAD SOCIAL	o,u
				FLORES VAZQUEZ CLAUDIA ODETH	ANALISTA DEL DEPARTAMENTO DE PRESTACIONES Y OBLIGACIONES DE SEGURIDAD SOCIAL	o,u
				RUIZ AVENDAÑO PABLO MARTIN	ANALISTA DEL DEPARTAMENTO DE NÓMINAS Y OBLIGACIONES FISCALES	o,u
				ESTRADA CANELA GABRIELA	JEFE DE DEPARTAMENTO DE GESTIÓN DE NÓMINAS Y OBLIGACIONES FISCALES	o,u
				RAMOS MOSCOSA MIRIAM STEPHANIE	ANALISTA DE LA DIRECCIÓN DE FACTOR HUMANO	o,u
				BENITEZ ROJO ALEJANDRA	ANALISTA DEL DEPARTAMENTO DE NOMINAS Y OBLIGACIONES FISCALES	o,u
				FRANCO AGUILAR MIRIAM	GERENTE DE DESARROLLO DEL FACTOR HUMANO	o,u
				PIZA CHIMAL MARIA DE LOS ANGELES	JEFE DE DEPARTAMENTO DE INDUCCIÓN Y FORMACIÓN	o,u
				SANTOS GUTIERREZ KEREN EUNICE	JEFE DE DEPARTAMENTO DE INDUCCIÓN Y FORMACIÓN	o,u
				TORRES MARIN IVONNE	ANALISTA DEL DEPARTAMENTO DE INDUCCIÓN Y FORMACIÓN	o,u
				LOPEZ SANCHEZ JESSYCA LUCIA	JEFE DEL DEPARTAMENTO DE MOVILIDAD INTERNA	i,o,u,p
				BARRIOS ESTRADA ARMANDO	TÉCNICO ESPECIALIZADO DEL DEPARTAMENTO DE MOVILIDAD INTERNA	o
				GONZALEZ JUAREZ ISMAEL	ANALISTA DEL DEPARTAMENTO DE MOVILIDAD INTERNA	o
				YABER VELEZ YAMEL GUADALUPE	SUBDIRECTORA DE GESTIÓN DEL FACTOR HUMANO	u
				CARRILLO FRANCO LENELLY AURORA	JEFE DEL DEPARTAMENTO DE ORGANIZACIÓN	o,c,u

Servidores públicos con acceso al Sistema de Recursos Humanos (SIRH)						
Administrador (a)	Responsable	Enlace de Datos Personales	Encargado de Datos	Operador (a)		
				Nombre	Cargo	Privilegios
Gerente de Desarrollo De Sistemas Interinstitucionales, Cap. 1/ro I.C.E. Flavio Solís López. Mantener actualizado el sistema, autorizar los accesos de los servidores públicos, determinar los privilegios y llevar un registro de los mismos	Director de Factor Humano. Myr. Inf. D.E.M. Outy Gómez Gómez. Supervisar los procedimientos de Factor Humano.	Subdir. Gestión del Factor Humano, Mtra. Yamel Gpe. Yaber Velez. Conocer el inventario de datos personales que se recaban y el flujo del tratamiento	Director Consultor de JACSU Consultores, S.C. Javier Chávez Suárez. Investigación socioeconómica de candidatos	CABRERA CUEVAS GUSTAVO	GERENTE DE ORGANIZACIÓN Y GESTIÓN DEL FACTOR HUMANO	O,C,U
				HERNANDEZ ALVARADO NANCY DOLORES	ENCARGADO DE OPERACIÓN DE LA GERENCIA DE ORGANIZACIÓN Y GESTIÓN DEL FACTOR HUMANO	O
				ANTONIO INES ANDRES HECTOR	TÉCNICO ESPECIALIZADO DEL DEPARTAMENTO DE PRESTACIONES Y OBLIGACIONES DE SEGURIDAD SOCIAL	O,U
				BAEZ HERNANDEZ GUILLERMO	JEFE DEL DEPARTAMENTO DE PRESTACIONES Y OBLIGACIONES DE SEGURIDAD SOCIAL	O,U
				JARQUIN PACHECO RAFAEL	TECNICO ESPECIALIZADO DEL DEPARTAMENTO DE NOMINAS Y OBLIGACIONES FISCALES	O,U
				PEREZ VALENCIA LUIS FRANCISCO	TÉCNICO ESPECIALIZADO DEL DEPARTAMENTO DE NÓMINAS Y OBLIGACIONES FISCALES	O,U
				HERNANDEZ VEGA OSCAR RODRIGO	ANALISTA DEL DEPARTAMENTO DE NOMINAS Y OBLIGACIONES FISCALES	O,U
				HERNANDEZ PACHECO SILVIA IRAIS	ANALISTA DEL DEPARTAMENTO DE ORGANIZACIÓN	O,U
				ESLAVA GARCIA ZENON EDUARDO	TÉCNICO ESPECIALIZADO DEL DEPARTAMENTO DE ORGANIZACIÓN	O,U
				LAGUNA GONZALEZ BRENDA MALLELI	ENCARGADO DE OPERACIÓN DEL DEPARTAMENTO DE ORGANIZACIÓN	O,U
				ANICETO LAGUNA LUIS ALBERTO	ANALISTA DEL DEPARTAMENTO DE INDUCCIÓN Y FORMACIÓN	O,U
				PIZA CHIMAL MARIA DE LOS ANGELES	JEFE DE DEPARTAMENTO DE INDUCCIÓN Y FORMACIÓN	O,U
				TORRES MARIN IVONNE	ANALISTA DEL DEPARTAMENTO DE INDUCCIÓN Y FORMACIÓN	O,U
				VELARDE GARDUÑO MARY ANNA	ENCARGADO DE OPERACIÓN DEL DEPARTAMENTO DE INDUCCIÓN Y FORMACIÓN	O,U
				CASTRO PONCE MARIA MAGDALENA	SUBDIRECTOR DE AREA DE REMUNERACIONES	O,U
				ESPIDIO BARRAGAN JUAN MANUEL	TÉCNICO ESPECIALIZADO DEL DEPARTAMENTO DE GESTIÓN DEL DESEMPEÑO Y COMPETENCIAS	O,U
				GONZALEZ JUAREZ DIANA PAOLA	ENCARGADO DE OPERACIÓN DEL DEPARTAMENTO DE GESTIÓN DEL DESEMPEÑO Y COMPETENCIAS	O,U
				Oliver Hervy Castillo Velasquez	Derechohabiencia y Pago de Hospitales	O,U
				Valeria Suarez Dorantes	Enfra. Mautino	O,U
				Alma Patricia Ortiz Galicia	Enfra. Vespertino	O,U
				Gabriela Aurora Hernandez Vergara	Pago a proveedores	O,U
				Diana Karina Tapia Guadarrama	Pago de Hospitales	O,U
				Jairo Javier Puente Romero	Pago a farmacias y laboratorios	O,U
				Janeth Dejanaira Martínez Moreno	Médico General	
				Laura Cecilia Hernández Hernández	Enfermería	

C. Myr. Inf. D.E.M. Outy Gómez Gómez. Director de Factor Humano	C. Lic. Ariadna Pamela Prior Velázquez Titular de la Unidad de Transparencia	Lic. Gerardo Luna Naveda Oficial de Protección de Datos Personales

Servidores públicos que dan tratamiento al Sistema Médico de Banjercito (SISMED).

Administrador (a)	Responsable	Enlace de Datos Personales	Encargado de Datos	Operador (a)		Privilegios
				Nombre	**Cargo**	
Gerente de Salud Organizacional, M.C. y M.A.S. Fabián Arturo Cabrera Bertoni. Administrar, supervisar y controlar el servicio médico y llevar un buen control del uso y manejo de la información administrativa.	Director de Factor Humano. Myr. Inf. D.E.M. Outy Gómez Gómez. Supervisar los procedimientos de contratación.	Jefe de Dpto. de Servicio Médico, M.C. Elí García Sánchez y Jefa de Gestión Operativa del Servicio Médico, Cap. 1/ro C.D. María Eugenia Valverde Hernández.	Staff interno del Servicio Médico Banjercito. relativo a la prestación de servicios con el Proveedor Axa Assistance S.A. de C.V.	Oliver Hervy Castillo Velasquez	Derechohabiencia y Pago de Hospitales	O,U
				Valeria Suarez Dorantes	Enfra. Mautino	O,U
				Alma Patricia Ortiz Galicia	Enfra. Vespertino	O,U
				Gabriela Aurora Hernandez Vergara	Pago a proveedores	O,U
				Diana Karina Tapia Guadarrama	Pago de Hospitales	O,U
				Jairo Javier Puente Romero	Pago a farmacias y laboratorios	O,U
				Janeth Dejanaira Martínez Moreno	Médico General	U
				Laura Cecilia Hernández Hernández	Enfermería	U

C. Myr. Inf. D.E.M. Outy Gómez Gómez. Director de Factor Humano	**C. Lic. Ariadna Pamela Prior Velázquez** Titular de la Unidad de Transparencia	**Lic. Gerardo Luna Naveda** Oficial de Protección de Datos Personales

INVENTARIO DE DATOS PERSONALES Y DE SISTEMAS DE TRATAMIENTO
CLIENTES

DATOS PERSONALES	DE IDENTIFICACIÓN Y CONTACTO							
	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN SISTEMAS DE TRATAMIENTO
NOMBRE COMPLETO	✓	Formularios físicos y electrónicos		Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a los productos de crédito, captación o servicios bancarios contratados. Todos los datos recabados integran las bases de datos de los sistemas automatizados utilizados por Banjercito, a efecto de cumplir con las tareas encomendadas a cada uno de los puestos de la estructura y de esa manera apoyar en el desempeño de sus funciones: Gestión integral del riesgo de crédito, operacional, de mercado y liquidez de Banjercito; así como el Sistema de Gestión de Continuidad del Negocio, a fin de que las actividades propias de la Institución se realicen con niveles de riesgo autorizados y se garantice la continuidad de los servicios. Asegurar que la Institución proporcione los servicios de banca y crédito al sector objetivo. Prestar los Servicios Bancarios Fronterizos, a fin de garantizar la expedición de los permisos de importación e internación temporal de vehículos. Operaciones crediticias, instrumentos de pago y tesorería; así como de las operaciones que instruyan movimientos de recursos o valores de la Institución. Otorgar de productos de crédito al sector objetivo. Administrar y liquidar los Fondos de Ahorro y de Trabajo, así como el pago de haberes de retiro, compensación, pensión y otros beneficios a que tengan derecho los miembros del Ejército, Fuerza Aérea y Armada, así como a los derechohabientes o beneficiarios. Prestación de servicios de banca y crédito al sector objetivo, a través de dispositivos móviles, cajeros automáticos, terminales punto de venta, tarjetas bancarias y las que se adicionen en el futuro. Proyectos estratégicos de la Institución. Contar con los recursos líquidos en moneda nacional y extranjera a través de los instrumentos financieros de inversión, mediante el diseño de estrategias y su implementación, conforme a los requerimientos de la operación sustantiva de la Institución, en apego a los lineamientos emitidos por las autoridades financieras y económicas. Registro y control contable de las operaciones y actos que realiza Banjercito. Integración de sistemas de información. Procesos de planeación, ingreso, permanencia y remuneraciones del capital humano. Suministro de los recursos materiales y los servicios generales necesarios para la operación de la Institución, la seguridad y protección de las personas y sus bienes. Sistema de gestión de seguridad de la información. Diseño, implementación y actualización de medidas y controles internos. Mecanismos para la prevención de fraudes, lavado de dinero y financiamiento al terrorismo.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable.		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. 1 Sistema Integral Bancario (SIBA) 2 Sistema IST-SWITCH 3 Sistema de pagos electrónicos interbancarios dólares (SPID) Enlace 4 Sistema de pagos electrónicos interbancarios (SPEI) Enlace 5 Sistema de Banca Electrónica 6 Sistema de Plataforma y ventanilla SOFT-M , Sockets y sistema de firmas 7 Sistema de validación de nóminas (SISVALN) 8 Sistema de consultas de Comités de Crédito 9 Sistema de Tesorería Bancario (SITEB) 10 Sistema de consultas de créditos (SISCC) 11 SIBUCB-BANJERCITO 12 Sistema de digitalización de Contratos (LASSER FICHE) 13 Sistema de evaluación de créditos (Tek origination) 14 Sistema de digitalización de solcitudes de crédito en sucursales (SHUFFLE) 15 IMAGE CHECK 16 Sistema de Web fiduciario Efisoft 17 Sistema Administrativo de Mensajería (SISMEN) 18 Sistema de Administración Integral de Riesgos (SAIR MATHEMATICA) (SAIR WEB) 19 Sistema Integral de asuntos jurídicos (SIAJ) 20 Sistema de riesgo operacional (SPIRO) 21 Sistema Interactivo de Evaluaciones (SIE) 22 Sistema para el módulo de ingresos y egresos (MIET) 23 Sistema de conciliación bancaria (SICABAN) 24 Sistema IITV Internet 25 Sistema IITV 26 Pre validador NEPE (SAT) 27 Sistema de Registro de Requerimientos (SISEREN) 28 Sistema de Gestión de Aclaraciones (SIGA) 29 Sistema de Limpieza de Datos (SILD) 30 CARDMAN 31 CA2 32 SMETF 33 Sistema Integral de Recursos Humanos (SIRH) 34 Sistema de Conciliación de Cajeros Automáticos 35 Sistema de Activo Fijo 36 Sistema de Administración de servicios de traslado de valores (SASTV) 34 Sistema de calificación de riesgos para PLD 35 ALTAIR 36 Módulo de Reportes de Operaciones Sospechosas de Clientes y Empleados 37 TSYS PRIME 38 Sistema ODWEK 39 Monitor Plus-Analizadores Alertas y Workflow Simulador interfaces 39 Sistema para la consulta de castigos y quebrantos (SPACCQ)
FECHA DE NACIMIENTO	✓							
NACIONALIDAD	✓							
DOMICILIO PARTICULAR	✓							
TELÉFONO PARTICULAR	✓							
TELÉFONO CELULAR	✓							
NUMERO DE CUENTA DE AFORE								
NUMERO DE CARTILLA MILITAR	✓							
CORREO ELECTRÓNICO	✓							
FIRMA AUTÓGRAFA								
FIRMA ELECTRÓNICA	✓							
SEXO	✓							
MATRICULA	✓							
EDAD	✓							
FOTOGRAFÍA	✓							
REFERENCIAS PERSONALES	✓							
RÉGIMEN MATRIMONIAL	✓							
DATOS DE NACIMIENTO	✓							
ID FISCAL (NIF)	✓							
DEPENDIENTES ECONÓMICOS	✓							

DATOS PERSONALES	LABORALES							
	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN
PUESTO O CARGO QUE DESEMPEÑA	✓	Formularios físicos y electrónicos		Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a los productos de crédito, captación o servicios bancarios contratados.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable.		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. • Sistema Integral Bancario Automatizado (SIBA ID 4.0)
TIPO DE PLAZA QUE OCUPA								
FECHA DE OCUPACIÓN DEL PUESTO	✓							
MOTIVO DE RENUNCIA								
DOMICILIO DE TRABAJO								
CORREO ELECTRÓNICO INSTITUCIONAL								
TELÉFONO INSTITUCIONAL	✓							
REFERENCIAS LABORALES								
EXPERIENCIA/CAPACITACIÓN								
GRADO MILITAR	✓		✓					
ZONA MILITAR DE PERTENENCIA	✓							
SITUACIÓN MILITAR	✓		✓					
ARMA O SERVICIO	✓							
FAMILIAR DE PPE	✓		✓					
PERSONA POLÍTICAMENTE EXPUESTA (PPE)	✓		✓					
ANTIGÜEDAD LABORAL	✓							
EMPRESA EN LA QUE LABORA	✓							

OCUPACIÓN O ACT. ECONÓMICA	✓						
OFICINA PAGADORA	✓						
FECHA DE ALTA	✓						
FECHA DE BAJA	✓						
ESPECIALIDAD MILITAR	✓						
DIPLOMADO MILITAR	✓						

ACADEMICOS								
DATOS PERSONALES	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN
NIVEL DE ESTUDIOS		Formularios físicos y electrónicos		Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a los productos de crédito, captación o servicios bancarios contratados.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable.		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. • Sistema Integral Bancario Automatizado (SIBA ID 4.0)
NOMBRE DE LOS ESTUDIOS								
GRADO DE AVANCE								
TÍTULOS								
CÉDULA PROFESIONAL								
CERTIFICADOS								
RECONOCIMIENTOS								
PROFESIÓN	✓							
IDIOMAS QUE MANEJA								

MIGRATORIOS								
DATOS PERSONALES	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN
ENTRADAS AL PAÍS		Formularios físicos y electrónicos		Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a los productos de crédito, captación o servicios bancarios contratados.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. • Sistema Integral Bancario Automatizado (SIBA ID 4.0)
SALIDA DEL PAÍS								
TIEMPO DE PERMANENCIA EN EL PAÍS								
CALIDAD MIGRATORIA	✓							
DERECHOS DE RESIDENCIA	✓							
ASEGURAMIENTO								
PAÍS DE RESIDENCIA	✓							
REPATRIACIÓN								

PATRIMONIALES Y/O FINANCIEROS								
DATOS PERSONALES	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN
BIENES MUEBLES		Formularios físicos y electrónicos		Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a los productos de crédito, captación o servicios bancarios contratados.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. • Sistema Integral Bancario Automatizado (SIBA ID 4.0)
BIENES INMUEBLES								
INFORMACIÓN FISCAL	✓							
LLAVE ISSFAM	✓							
NÚMERO DE CRÉDITO INFONAVIT								
CRÉDITOS	✓							
SALARIO DIARIO INTEGRADO (SDI)	✓							
EGRESO	✓							
CUENTAS BANCARIAS	✓							
NO. DE TARJETAS DE CRÉDITO	✓							
SEGURO								
AFORES								
INGRESOS	✓							
PENSIONES	✓							
TIPO DE VIVIENDA QUE HABITA	✓							

DE SALUD								
DATOS PERSONALES	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN
ANTECEDENTES PERSONALES PATOLÓGICOS	✓	Formularios físicos y electrónicos	✓	Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a los productos de crédito, captación o servicios bancarios contratados.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. Sistema Integral de Asuntos Jurídicos (SIAJ)

DATOS PERSONALES	DE PROCEDIMIENTOS ADMINISTRATIVOS O JURISDICCIONALES							
	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN
INTERRUPCIONES (MILITARES)	✓	Formularios físicos y electrónicos	✓	Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a los productos de crédito, captación o servicios bancarios contratados.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. • Sistema Integral Bancario Automatizado (SIBA ID 4.0)
ANTECEDENTES PENALES	✓		✓					

DATOS PERSONALES	DE MENORES DE EDAD							
	¿DA TRATAMIENTO A ESTOS DATOS?	MEDIOS DE OBTENCIÓN	DATOS SENSIBLES	FINALIDAD DEL TRATAMIENTO	TERCEROS RECEPTORES (REMISIONES)	TERCEROS RECEPTORES (TRANSFERENCIAS)	BLOQUEO, CANCELACIÓN, SUPRESIÓN O DESTRUCCIÓN	UBICACIÓN
NOMBRE COMPLETO	✓	Formularios físicos y electrónicos		Banjercito utilizará los datos personales proporcionados para que conocimiento de los clientes que acceden a a los productos de crédito, captación o servicios bancarios contratados.		Banjercito no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos debidamente fundados y motivados, provenientes de una autoridad competente, de acuerdo a la normatividad aplicable		Banco Nacional del Ejercito Fuerza Aérea y Armada, S.N.C. • Sistema Integral Bancario Automatizado (SIBA ID 4.0)
REGISTRO FEDERAL DE CONTRIBUYENTES (RFC)	✓							
CLAVE ÚNICA DE REGISTRO DE POBLACIÓN (CURP)	✓							
FECHA DE NACIMIENTO	✓							