Ferromex

POLÍTICA PROTECCIÓN DE DATOS PERSONALES

ÍNDICE

1. OBJETIVO

La Política de Protección de Datos Personales tiene como objetivo la seguridad de la información personal en posesión de Ferrocarril Mexicano S.A. de C.V. (FXE), el tratamiento de los mismos y ejercicio de los derechos ARCO en los términos que fija la Ley de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo "Ley de Protección de Datos") y su Reglamento.

La Política de Protección de Datos Personales (Política PDP) establece los lineamientos para la protección de datos personales, su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Con la Política PDP, todo Personal de FXE podrá detectar los posibles riesgos y vulneraciones relacionados con el tratamiento de la información y así reforzar el Sistema de Gestión de Seguridad de los Datos Personales apegándose a los principios plasmados en la Ley de Protección de Datos. La aplicación de la Política se entenderá complementada con el Aviso de Privacidad publicado en la página de FERROMEX (www.ferromex.mx).

2. APLICACIÓN DE LA POLÍTICA PDP

El cumplimiento y aplicación de la Política PDP será obligatoria para toda persona que tenga en su posesión datos personales de Terceros en términos de la Ley de Protección de Datos Personales y su Reglamento, o que trabaje de forma directa o indirecta con FXE. La Política PDP es de carácter obligatorio para accionistas, consejeros, directivos y empleados, así como para clientes, proveedores, consultores y todas aquellas personas que mantengan una relación comercial con FXE (en adelante "Sujetos obligados").

Toda persona que contratada por FXE deberá contar con un certificado de conocimiento y cumplimiento de la Política PDP (anexo A). Los acuses en formato digital serán resguardados y quedarán en posesión de la Dirección de Recursos Humanos (para el caso del Personal de FXE), Abastecimientos (para el caso de proveedores), Comercial (para el caso de clientes) y Finanzas (para los pagos de y para Terceros), en los términos dispuestos en la Política PDP.

3. PRINCIPIOS RECTORES DE LA POLÍTICA PDP

Los Responsables en el tratamiento de datos personales deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en el artículo 6 de la Ley de Protección de Datos. Todo acto relacionado con los datos personales tendrá que apegarse a estos principios:

1. **Licitud**. El principio que obliga al Responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto en lo relacionado con tratamiento de datos personales en posesión de los particulares por la legislación mexicana y el derecho internacional.

2. **Consentimiento**. Manifestación de la voluntad del particular encaminada a crear consecuencias de derecho.

3. **Consentimiento expreso**. El consentimiento del particular manifestado verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos.

4. **Consentimiento tácito**. Se entenderá por consentimiento tácito cuando habiendo puesto a disposición el aviso de privacidad necesario para el tratamiento de los datos del titular, éste no haya expresado oposición alguna.

5. **Información**. Principio que obliga a informar a los titulares de los datos personales las características principales del tratamiento al que será cometida su información personal.

6. **Calidad**. Principio que define a los datos personales como de manera exacta, completa, pertinente, actualizada y correcta.

7. **Finalidad**. Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad o por los que hayan sido consentidos.

8. **Lealtad**. Principio que establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad con respecto a la confianza que le deposita una persona a otra.

9. **Proporcionalidad**. Principio que establece la obligación del Responsable de tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con la finalidad para las cuales se obtuvieron.

10. **Responsabilidad**. El principio establece la obligación de los Responsables de velar por el cumplimiento del resto de los principios y demostrar ante titulares y la autoridad que cumple con sus obligaciones en torno a la protección de los datos personales.

4. DEFINICIONES

1. **Alta Dirección**. Directores de Ferrocarril Mexicano S.A. de C.V.

2. **Anonimización**. El resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación.

3. **Anti exploit**. Herramienta que detiene ataques de explotación de vulnerabilidades a aplicaciones y navegadores.

4. **Antispam**: Herramienta que identifica y bloquea el correo no deseado, mejor conocido como “correo basura”.

5. **Antispyware**. Herramienta que protege al equipo de cómputo contra software espía, el cual envía información confidencial a un atacante.

6. **Aviso de privacidad**. Documento físico, electrónico o en cualquier otro formato generado por el Responsable que es puesto a disposición del titular de la información, previo al tratamiento de sus datos personales, de conformidad con lo dispuesto en el artículo 15 de la Ley de Protección de Datos.

7. **Bases de datos**. El conjunto de datos personales referentes a una persona identificada o identificable.

8. **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 corresponde.

9. **Cómputo en la nube**. Modelo de abastecimiento y entrega externa de servicios de acceso a recursos informáticos y su tecnología.

10. **Datos personales biométricos**. Propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.

11. **Datos personales sensibles**. Aquellos datos personales que afecten a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran datos sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas o preferencia sexual.

12. **Datos personales**. Cualquier información concerniente a una persona física identificada o identificable.

13. **Derechos ARCO**. El derecho al acceso, rectificación, cancelación y oposición de toda persona con respecto a sus datos personales.

14. **Disociación**. Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

15. **Dispositivos de almacenamiento extraíble**. Componente utilizado para el almacenamiento de información. Ejemplo: Discos compactos, memorias USB, o discos duros externos.

16. **Encargado**. La persona física o moral que sola o con otras personas trate datos personales por cuenta del Responsable.

17. **Equipo de cómputo**. Dispositivo electrónico asignados por la empresa a usuarios internos o externos como Laptops, computadoras de escritorio, teléfonos móviles (Smartphone) y dispositivos de almacenamiento extraíbles.

18. **GMXT**. GMéxico Transportes S.A.B. de C.V. y sus subsidiarias, Ferrocarril Mexicano, S.A. de C.V. (FXE), Ferrosur, S.A. de C.V. (FSRR), Intermodal México, S.A. de C.V. (IMEX), Texas Pacifico LP. (TXPF), Terminales Transgolfo, S.A. de C.V. (TTG), Florida East Coast Railway Corp. (FEC), Raven Transport Company, Inc. (RAVEN), Grupo Ferroviario Mexicano, S.A. de C.V. (GFM), Intermodal México Arrendadora, S.A. de C.V. USAIMEX LLC; Infraestructura y Transportes México, S.A. de C.V., Líneas Ferroviarias de México, S.A. de C.V. y Chepexplora S.A. de C.V.

19. **Instituto**. Instituto Federal de Acceso a la Información y Protección de Datos.

20. **Las Partes**. El Titular de los datos, el Responsable, Encargado y Tercero (en su caso) del tratamiento de datos personales.

21. **Ley de Protección de Datos.** Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

22. **PHVA**. Principios usados por el Sistema de Gestión de Seguridad de los Datos Personales concernientes en planificar, hacer, verificar y actuar.

23. **Personal de FXE**. Se entenderá por personal a los empleados de FXE, o toda persona que cuente con contrato laboral de tiempo determinado o indeterminado celebrado con dicha empresa, contemplando la alta dirección, consejo de administración, empleados, representantes y cualquier persona que actúe en nombre y cuenta de FXE.

24. **Reglamento**. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

25. **Remisión**. Toda comunicación de datos realizada entre el Responsable del tratamiento de los datos personales al encargado de estos.

26. **Responsable**. Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

27. **Servidor**. Sistema que proporciona recursos, datos, servicios o programas a otros equipos de cómputo, a través de una red.

28. **Sistema de gestión de seguridad de los datos personales (SGSDP)**. Conjunto de medidas y procesos implementados por la empresa para lograr una protección efectiva de la información.

29. **Software antivirus**. Programa cuyo objetivo es detectar y eliminar virus informáticos.

30. **Tercero**. Se refiere a la persona físicas o moral especializada con perfil técnico, social, legal o económico contratada por FXE para brindar o contribuir a dar servicios a sus cliente y/o colaboradores.

31. **Titular**. Persona física a quien corresponden los datos personales.

32. **Transferencia**. Toda comunicación de datos que realiza el Responsable del tratamiento a un tercero, distinto del titular, del mismo Responsable o del encargado.

33. **Tratamiento de datos**. Cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionados con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra formade habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales.

34. **Vulneración de datos**. Cualquier alteración, modificación, daño, pérdida, consulta, uso, acceso o tratamiento no autorizado o fraudulento, pérdida o destrucción no autorizada, robo, extravío o copia no autorizada de los datos personales.

5. RESPONSABILIDADES GENERALES

5.1 Disposiciones Generales

1. Será responsabilidad el cumplimiento de lo dispuesto en la Política PDP para todo Personal de FXE y Terceros que traten o tengan acceso a datos personales de cualquier persona física identificada o identificable, de forma habitual o esporádica, del Personal de FXE o Tercero.

2. Será responsabilidad de la Dirección de Recursos Humanos y Dirección Jurídica, con apoyo del Área de Cumplimiento, la implementación, actualización y orientación de la Política PDP.

3. Para dar cumplimiento al inciso anterior, será responsabilidad de las Direcciones enviar sus comentarios al Área de Cumplimiento a efecto de preparar un informe por escrito para la Dirección General y al Comité de Auditoría mediante el cual se señalen, de ser el caso, las posibles deficiencias encontradas y/o recomendaciones de mejora. Dichos informes serán enviados periódicamente por lo menos cada seis meses.

4. Todo nuevo contrato celebrado con un Tercero que implique la transferencia de datos personales del Titular y/o Tercero, deberá contener las cláusulas mencionadas en la Política de Elaboración y/o Revisión de Contratos y Convenios siguiendo en todo momento las reglas plasmadas en la Política PDP.

5.2 Implementación de la Política PDP

1. Cualquier Tercero que pretenda establecer una relación comercial con FXE deberá apegarse a lo establecido en la Política PDP como los lineamientos mínimos para el tratamiento de los datos personales del Personal de FXE.

2. El tratamiento de los datos personales deberá de seguir en todo momento los principios plasmados en la Política PDP y los principios de confidencialidad, integridad, disponibilidad y protección de los datos. Para tales efectos, todas las áreas de FXE deberán aplicar el Sistema de Gestión de Seguridad de los Datos Personales (SGSDP) a efecto de evitar cualquier vulneración a los datos personales.

3. En caso de que el Responsable del tratamiento de los datos personales contrate con un Tercero que funja como Encargado de estos, éste no podrá tratar los datos con finalidad distinta a la autorizada por el titular. En caso de vulneración, el Responsable se reserva el derecho de ejercer acciones legales contra el tercero (persona física o moral) de conformidad con la Ley de Protección de Datos y su Reglamento.

4. La Dirección Jurídica y la Dirección Digital serán las áreas encargadas de actualizar el Aviso de Privacidad y darlo a conocer por los diferentes medios electrónicos con que cuenta FXE.

5. Los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable (cuadro inciso 8.2.10).

6. Todo Sujeto Obligado que omita realizar el procedimiento enunciado en la Política PDP será sujeto a sus sanciones especificadas en el apartado 12.2 De las Sanciones de la Política PDP.

7. La alta Dirección deberá autorizar los planes y estrategias de protección de información, con el fin de que la Dirección Digital implemente los mismos, con base en las mejores prácticas tales como la Metodología de Evaluación de Privacidad de Datos, a fin de generar controles de seguridad para mitigar riesgos.

6. RESPONSABILIDAD DEL PERSONAL DE FXE

6.1. Actos Prohibidos

1. FXE condena cualquier acto relacionado con la vulneración de los datos personales, por lo que regula los procesos de implementación del Sistema de Gestión de Seguridad de los Datos Personales y el ejercicio de los derechos ARCO con sus restricciones.

2.

6.2. De la Capacitación y Orientación

1. Para efectos del cumplimiento de la Política PDP, se establecen mecanismos para garantizar que se comunique de forma efectiva al Personal de FXE, a través de:

    A) Capacitaciones periódicas mediante cursos impartidos por Terceros, y/o

    B) Capacitaciones periódicas impartidas directamente por FXE por medio de la Dirección de Recursos Humanos.

2. Con la finalidad de dotar de capacidad técnica necesaria para lograr prevenir, detectar y reportar cualquier divulgación o vulneración de los datos personales del titular y garantizar el cumplimiento de la Política PDP, el Personal de FXE contará con la capacitación necesaria. Toda capacitación estará documentada por medio de certificados y/o constancias:

    A) Las certificaciones y/o certificados digitales de las capacitaciones del Personal de FXE quedarán en custodia de la Dirección de Recursos Humanos, y podrán ser solicitados por el Área de Cumplimiento en todo momento.

    B) Todo el Personal de FXE, en activo o de reciente ingreso, deberá llenar el documento contenido en el Anexo A de la Política PDP.

3. Corresponde a la Dirección de Recursos Humanos dar a conocer la Política PDP y sus alcances como parte de la inducción al Personal de nuevo ingreso.

4. Cualquier Tercero que pretenda establecer una relación comercial con FXE deberá comprometerse a apegarse al Programa de Cumplimiento Normativo de FXE.

5. Los Sujetos Obligados que omitan realizar los procedimientos enunciados en la Política PDP serán sujetos a las sanciones especificadas en el numeral 12 del Incumplimiento de la Política PDP.

7. DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES

1. El Sistema de Gestión de Seguridad de los Datos Personales (SGSDP) es el conjunto de medidas de seguridad administrativas, técnicas y físicas que garantizan la protección de los datos personales para evitar cualquier vulneración de datos personales.

2. La creación, aplicación y actualización constante del SGSDP quedará bajo la responsabilidad de la Dirección de Digital con las aprobaciones correspondientes de la Alta Dirección para la implementación de los controles de este sistema. El SGSDP tendrá las siguientes funciones y características:

    A) Monitorear los procesos cada 12 meses e informar los resultados a la Dirección de área responsable para su revisión e implementación de medidas que consideren pertinentes la Dirección de Digital.

B) Mejorar y actuar mediante capacitaciones y medidas de protección.

3. Como parte de la implementación del SGSDP, se deberán seguir mecanismos cuyo objeto es mitigar cualquier riesgo, de forma enunciativa mas no limitativa, pueden ser los siguientes:

   A) Gestión de Contraseña (creación de políticas de contraseñas robustas para aplicaciones y servicios, cambio de contraseña de forma periódica, etc.).

   B) Seguridad dentro de las instalaciones: Uso estricto de credenciales, gafetes o identificación dentro de las instalaciones por parte del personal de FXE y de terceros.

   C) Acceso restringido a la red, archivos o carpetas necesarias y autorizadas.

   D) Acceso limitado a internet.

   E) Monitoreo por medio de cámaras de vigilancia.

   F) Liberación de impresiones sólo con clave o contraseña, y

   G) Escritorios limpios, no dejar desatendido en áreas de trabajo documentos/activos con información confidencial (datos personales).

   H) Para el caso de equipo de cómputo de usuario final será necesario contar con software y licencias legales autorizadas, antivirus, agente de cifrado de datos para disco duro, agente de borrado de información, así como apegarse a las reglas y políticas que indique FXE.

   I) Contar con una herramienta de prevención de pérdida de datos para evitar una fuga de información de los datos personales considerando los siguientes puntos:

      - Datos en reposo: Datos almacenados en cualquier medio y con los cuales no existe interacción alguna con el usuario en un momento específico.

      - Datos en tránsito: Flujo de datos a través de cualquier medio.

      - Datos en uso: Datos que están siendo accedidos o manipulados por un usuario o programa.

   J) Contar con mecanismos de prevención de pérdida de datos que salen de la organización:

      - Bloqueo de los datos personales, que se envían por medio de servicios de Office 365: correo electrónico, Microsoft Teams, entre otros.

      - Alertar y bloquear cualquier instancia de transferencia de archivos donde sean detectados datos personales.

K) Mecanismos de prevención de datos críticos en uso en equipos de usuario final:

- Deshabilitar la transferencia de datos personales a medios extraíbles, como un dispositivo de almacenamiento externo: memoria USB, disco externo o un dispositivo móvil.
- Bloqueo de la transferencia, si el dispositivo de almacenamiento no se encuentra totalmente cifrado.
- Inhabilitar la impresión de datos personales a usuarios no autorizados.
- Copia de datos confidenciales en aplicaciones no autorizadas.
- Publicar datos críticos en redes sociales.
- Transferencia de datos críticos a través de correo electrónico basado en web que no es gestionado por la empresa.

L) Para esta solución de seguridad se deberán:

- Generar alertas hacia el administrador de esta solución, a Seguridad Digital y al Responsable de protección de la información de cada área de negocio sobre el evento de intento de fuga de información.
- Creación de registros de auditoría.
- Envío de cuadros de dialogo al usuario para notificación y/o confirmación de alguna acción.
- Colocar en modo de cuarentena un mensaje para su revisión y autorización de envío.

4. La Dirección Digital, deberá asegurar que todos los equipos de cómputo (laptops y computadoras de escritorio), dispositivos de almacenamiento extraíbles y servidores utilizados en la red de FXE tengan instalado un software antimalware y antispyware; que el servicio de correo cuente con los controles de seguridad ya mencionados y un mecanismo de antispam; así como otros controles de seguridad como actualización del sistema operativo para evitar la explotación de una vulnerabilidad en los equipos.

5. Será responsabilidad de la Dirección Jurídica, incluir en los contratos una cláusula de confidencialidad y de no revelación de información; así como otras cláusulas de seguridad de la Política de Elaboración y/o Revisión de Contratos y Convenios, tanto para personal de FXE como con terceros, según su área de competencia.

6. La Dirección Digital, deberá asegurar que cualquier acción realizada por los usuarios dentro de los sistemas de FXE deje constancia y sea rastreable. De igual forma se deberán implementar condiciones de seguridad que impidan borrar o alterar los registros indispensables.

7. Se podrá dar acceso al personal de FXE o a un Tercero a las aplicaciones y/o servicios de FXE, los cuales deberán contar con los permisos de mínimo privilegio para sus actividades y ser planeados para prevenir interrupciones en la operación.

8. El SGSDP deberá de tomar en cuenta las diferentes clases de datos personales para la implementación de diferentes niveles de seguridad y de acceso a los mismos, considerando para tales efectos los artículos 60 y 61 del Reglamento.

8. DEL TRATAMIENTO DE LOS DATOS PERSONALES

8.1. De la obtención de los datos

1. En caso de que el Tercero se niegue a proporcionar la información para efectos de la debida diligencia, Ferromex se reserva el derecho de no considerar al Tercero en las licitaciones y/o terminar la relación comercial de forma anticipada sin penalización alguna.

2. El tratamiento de datos personales deberá observar en todo momento los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad a fin de dar cumplimiento a las disposiciones legales aplicables.

3. Previo a la obtención de los datos personales, es necesario que el Responsable del tratamiento ponga a disposición del titular de los datos personales el Aviso de Privacidad, su identidad y domicilio y la finalidad del tratamiento que se le darán a los datos personales.

4. Cuando se realice cualquier cambio al Aviso de Privacidad, el Responsable del tratamiento de los datos personales notificará al Titular por medios físicos, electrónicos o cualquier otro que garantice el conocimiento de este.

5. Siguiendo en todo momento el principio de proporcionalidad, únicamente se le solicitará al titular los datos estrictamente necesarios para cumplir con la finalidad requerida, siendo así los datos necesarios, adecuados y relevantes.

6. Las finalidades primarias y secundarias se encontrarán distinguidas en el Aviso de Privacidad y el Titular de los datos podrá negarse al tratamiento secundario de sus datos, sin entenderse que se retire el consentimiento del tratamiento primario.

7. Cuando los datos no hayan sido obtenidos directamente del Titular, el Responsable deberá de darle a conocer el cambio de Aviso de privacidad, salvo que el tratamiento sea con fines históricos, estadísticos o científicos en los que haya un proceso previo de disociación.

8. Todo tratamiento de datos personales estará sujeto al consentimiento de su Titular, el consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

9. Se entenderá que el Titular ha otorgado su consentimiento tácitamente al tratamiento de sus datos cuando habiéndose puesto a su disposición el Aviso de Privacidad no manifiesta su oposición.

10. Se requerirá del consentimiento del Titular cuando se cambie el tratamiento de los datos, cuando se pretendan transferir, cuando así lo acuerden previamente el Titular y el Responsable y/o cuando cambie la finalidad del tratamiento de los datos, y demás supuestos establecidos en la regulación de la materia.

11. Para el tratamiento de los datos personales sensibles, financieros y/o patrimoniales, el Responsable deberá obtener el consentimiento expreso y por escrito del Titular para su tratamiento, ésta se podrá dar a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autentificación que se establezca para ese efecto, salvo los artículos 10 y 37 de la Ley de Protección de Datos.

12. No se requerirá del consentimiento del Titular para el tratamiento de los datos personales en los siguientes casos, de conformidad con el artículo 10 de la Ley de Protección de Datos:

    A) Esté previsto en una Ley;

    B) Datos que figuren en fuentes de acceso público;

    C) Datos personales que se sometan a un procedimiento previo de disociación;

    D) Cuando los datos tengan el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el Responsable;

    E) Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

    F) Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente;

    G) Se dicte resolución de autoridad competente;

    H) Los demás que exprese la Ley.

13. El consentimiento podrá ser revocado por parte del Titular en cualquier momento, sin que se le atribuyan efectos retroactivos. Los mecanismos para la revocación estarán especificados en el Aviso de Privacidad.

14. En caso de reclutamiento de nuevo personal, la Dirección de Recursos Humanos recabará los datos personales de los diferentes aspirantes y seguirá el principio de confidencialidad y seguridad de los datos para evitar cualquier vulneración de estos.

15. Los datos biométricos del personal de FXE quedarán en resguardo de la Dirección de Recursos Humanos, el cuál será almacenado de acuerdo con los mecanismos autorizados por la Dirección Digital.

8.2. Del Almacenamiento de la Información

1. Será responsabilidad de la Dirección de Recursos Humanos el resguardo de los datos personales del Personal de FXE.

2. El almacenamiento de los datos patrimoniales de Terceros será responsabilidad de las direcciones de Abastecimientos, Comercial y/o Finanzas según el ámbito de sus competencias y responsabilidades de acuerdo con el SGSDP.

3. Todo Personal de FXE de cada Dirección, en ejercicio de sus funciones y en el ámbito de sus responsabilidades, deberá almacenar la información recabada en los sistemas y mecanismos autorizados por la Dirección Digital y de acuerdo con el SGSDP.

4. En los casos en los que la información se requiera en original, el mismo será almacenado de forma física. En los casos en los que la información sea recabada de forma digital, será resguardada por el Responsable, en el cómputo en la nube o de acuerdo con los mecanismos y software autorizados e implementados por la Dirección Digital.

5. La Dirección Digital designará el (los) software y mecanismo(s) de almacenamiento y resguardo de la información como mecanismo del SGSDP.

6. Para el tratamiento de datos personales en aplicaciones e infraestructura en el cómputo en la Nube en los que el Responsable contrata por medio de contratos de adhesión a condiciones o cláusulas generales de contratación con Terceros, sólo podrá utilizarse aquellos servicios en los que el proveedor cumpla con lo establecido en el número I incisos a) a la e) del artículo 52 del Reglamento. Quedará prohibida cualquier plataforma no autorizada para el resguardo de los datos personales por parte de la Dirección Digital, verificando en todo momento que cumpla con lo establecido en el artículo citado.

7. Se podrá contratar con un servidor de almacenamiento de datos externo a FXE como el almacenamiento en la nube, siguiendo en todo momento los requisitos mínimos plasmados en el numeral anterior.

8. Todo almacenamiento de los datos personales podrá ser resguardado de acuerdo con la anonimidad del acceso a la información:

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

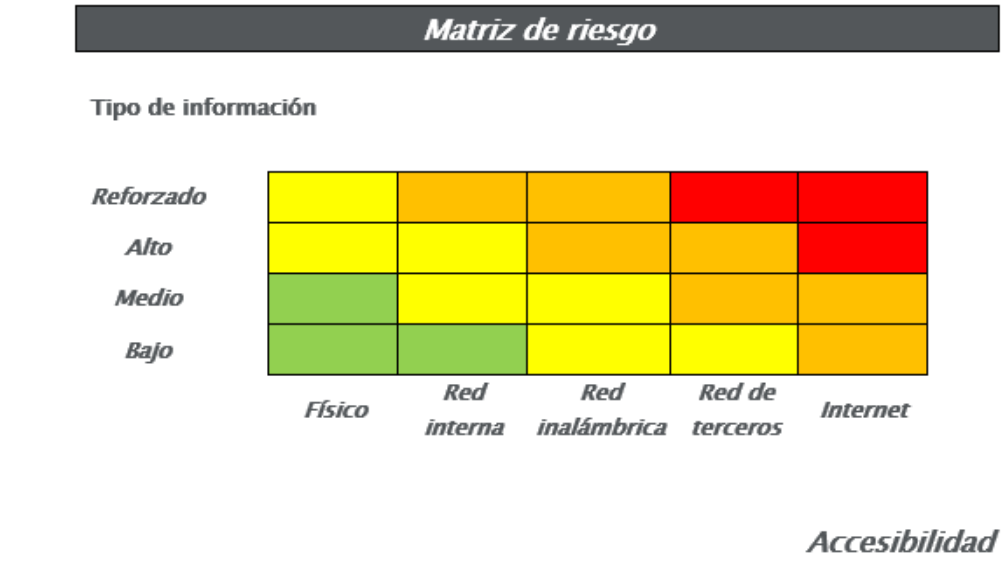
9. Todo Responsable deberá identificar con qué tipo de información cuenta de acuerdo con lo establecido en la tabla siguiente[1]:

Nivel de riesgo inherente	Tipo de dato
Bajo	1. Información concerniente a una persona física *identificada o identificable*: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional y/o información migratoria.
Medio	1. Datos que permite conocer la *ubicación física* de la persona: 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 (beneficiarios). 2. Datos que permiten inferir el *patrimonio* de una persona: saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios y/o servicios contratados. 3. Datos de *autenticación*: datos de usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz), firma autógrafa y electrónica, fotografías y/o identificaciones oficiales. 4. Datos *jurídicos*: antecedentes penales, amparos, demandas, contratos y/o litigios.
Alto	1. Datos personales sensibles que de acuerdo con la Ley incluye datos de salud física o mental (información médica), pasado, presente o futuro, información genérica, origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales o cualquier otra información que pudiese causar algún tipo de discriminación.
Reforzado	1. Con respecto a la *información*: información adicional de tarjeta bancaria: número de la tarjeta de crédito y/o débito, fecha de vencimiento de las tarjetas, código de seguridad, datos debanda magnética o número de identificación personal (PIN). 2. Con respecto al titular: cualquier información concerniente a las personas de alto riesgo respeto al oficio/profesión en la que trabaja por beneficios económicos, políticos o religiosos.

[1] La Política se apega a la clasificación del riesgo establecido por el Instituto Nacional de Acceso a la Información (INAI) en su Metodología de Análisis de Riesgo BAA y la Ley de Protección de Datos.

10. Derivado de la identificación del tipo de información que cuenta, el Responsable deberá de realizar un análisis de riesgo con base a la matriz de riesgos:

11. Una vez almacenada la información en la plataforma indicada por la Dirección Digital



para tales efectos, el Responsable especificará qué nivel de autorización y/o quién podrá tener acceso con las restricciones de uso a los datos.

12. Tendrán acceso a la base de datos almacenados únicamente las personas cuyos usuarios estén autorizados para tales efectos por parte de la Dirección Digital o quien esta designe.

13. Todo tratamiento de datos personales deberá seguir los lineamientos del SGSDP.

14. En caso de que se requiera una actualización de los datos personales será necesario que el Responsable que tiene contacto con el Titular solicite la información a actualizar.

15. Cada Dirección de FXE que cuente en su poder datos personales de Terceros o personal de FXE, deberá realizar un análisis de éstos cada año para verificar la utilidad del dato y en su caso iniciar su proceso de destrucción.

8.3. Del Proceso y Uso de la Información

1. Para el proceso de la información, el Responsable podrá recurrir a un Tercero para fungir como Encargado, en términos de la Ley de Protección de Datos y su Reglamento, el cual únicamente podrá usar y tratar los datos con la finalidad que sea expresada por parte del Responsable y por la finalidad que autorizó y dio su consentimiento el Titular.

2. El Responsable del tratamiento de datos personales, deberá procesar los datos con la finalidad con la que fueron recabadas y consensuadas por el Titular y expresadas en el Aviso de Privacidad.

3. El Titular de la Dirección Digital, deberá asegurar que los derechos de acceso y autorizaciones de aprobación en los sistemas de información de personal a su cargo estén debidamente revisados y actualizados.

8.4. De la Actualización y/o Rectificación de los Datos

1. Cuando exista un cambio en los datos personales del Titular, éste deberá notificarlo al Responsable por medio del procedimiento del ejercicio de los derechos ARCO para actualizar los mismos.

8.5. Transferencia y Remisión de los Datos

1. Queda prohibida cualquier transferencia o remisión de datos que no sea previamente autorizada por el Titular. La autorización deberá ser por escrito de conformidad con lo establecido en el Aviso de Privacidad.

2. El Responsable podrá remitir la información al Encargado, el cual únicamente podrá tratar los datos personales con los fines que determine el Responsable.

3. El Personal de FXE que cambie de puesto deberá informar y remitir los datos personales que tenga en su poder incluyendo las contraseñas de archivos, folders, entre otras, a la persona que ocupará el puesto o a su jefe inmediato, según sea el caso.

4. En caso de transferencia de datos personales, es necesario se sigan los procedimientos de los artículos 68, 71, 72 y 73 del Reglamento, así como el 36 de la Ley.

5. El Titular de los datos podrá autorizar al Responsable y Encargado la transferencia de los datos personales entre las subsidiarias de GMXT.

6. Se podrá realizar la transferencia de datos nacional o internacional, sin necesidad del consentimiento del Titular en los supuestos que marca la Política PDP y la Ley de Protección de Datos y su Reglamento, así como en aquellos casos que así lo exija alguna autoridad.

7. El Responsable podrá transferir los datos personales sin autorización del Titular en los siguientes casos, mismos que se enlistan de manera enunciativa más no limitativa a continuación:

    A) Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

    B) Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

    C) Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

    D) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial,

    E) Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el personal responsable y el titular, y

    F) Demas casos del artículo 37 de la Ley de Protección de Datos.

8.6. Bloqueo de los Datos Personales

1. Una vez terminado el propósito por el cual se obtuvieron los datos personales, la información deberá de ser bloqueada durante el periodo especificado en el Anexo B, previa la cancelación y destrucción.

2. El periodo de bloqueo de los datos personales deberá ser equivalente al plazo de prescripción de las acciones que deriven de la relación jurídica que se tenga con el Titular.

3. Cada Dirección de Área será responsable de la destrucción de los datos que tenga en su posesión. Para tales efectos, deberá verificar cada año si ya transcurrió el tiempo de bloqueo y se deberá generar una evidencia de tal destrucción.

8.7. Cancelación, Suspensión o Destrucción de la Información

1. Transcurrido el periodo de bloqueo, los datos personales deberán ser eliminados de manera irrecuperable. La destrucción por medios electrónicos implica borrar del sistema todo rastro de información, de tal manera que sea imposible de reproducir o recuperar, la destrucción de los datos que consten en medios físicos, deberán ser irrecuperables por los métodos existentes para tales efectos y obteniendo una evidencia de su destrucción.

2. La información será clasificada de acuerdo con la naturaleza de los datos, de conformidad con la clasificación respecto de su utilidad:

A) Información que legalmente debe ser conservada por periodos de tiempo prescritos;

B) Información necesaria para la operación del negocio y proyectos;

C) Información incidental y de otros tipos generada en el curso del negocio;

D) Información personal o no relacionada con el negocio;

9. DERECHOS ARCO

9.1. Implementación de los derechos ARCO

1. Los derechos ARCO podrán ser ejercidos por parte del Titular por medio de las personas autorizadas en el artículo 89 del Reglamento.

2. La Dirección de Recursos Humanos será responsable de la atención de las solicitudes de los derechos ARCO del personal de FXE.

3. Todo Personal de FXE que no sea el Responsable del tratamiento de los datos, que reciba una solicitud de aplicación de los derechos ARCO deberá canalizarlo con la Dirección de Recursos Humanos.

4. El Titular podrá ejercer los derechos ARCO por sí o por medio de su representante de acuerdo con el proceso establecido en el Aviso de Privacidad.

5. Cuando el Titular ejerza sus derechos ARCO, la Dirección de Recursos Humanos, contará con 20 días naturales para dar atención a la solicitud. Ésta podrá contar con 15 días adicionales en caso de modificar la resolución.

6. El ejercicio de los derechos ARCO por parte del Titular podrá ejercerse con respecto del tratamiento de sus datos tratados directamente por el Responsable, Encargado o Tercero.

9.2. Acceso, Rectificación y Cancelación

1. El Titular tiene derecho de acceder a sus datos personales con la finalidad de corroborar que éstos sean correctos y actualizados y/o verificar qué tratamiento se le han dado.

2. El Titular tendrá derecho a solicitar la rectificación de sus datos personales. En caso de que sean incompletos o inexactos o desactualizados, proporcionar los datos correctos.

3. El Titular podrá solicitar se eliminen sus datos personales de la base de datos del Responsable, en caso de considerar que sus datos personales no son utilizados o tratados conforme a lo establecido en el Aviso de Privacidad o al tratamiento por el cual dio su consentimiento. Para el cumplimiento de la petición de cancelación, el Responsable deberá de cesar el tratamiento de los datos.

9.3. Oposición

1. El Titular tendrá derecho a oponerse al tratamiento de los datos personales o exigir el cese del mismo, por alguna causa legítima o para que no se lleven a cabo el tratamiento para fines específicos.

2. El numeral anterior no aplicará en los casos en los que el tratamiento específico sea para el cumplimiento de una obligación legal impuesta al Responsable.

9.4. Restricción de los derechos ARCO

1. El Responsable podrá restringir los derechos ARCO en los siguientes supuestos:

    A) Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;

    B) Cuando en su base de datos, no se encuentren los datos personales del solicitante;

    C) Cuando se lesionen los derechos de un tercero;

    D) Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y

    E) Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

2. Aunado a las restricciones enlistadas en el numeral anterior, el Responsable y el Titular de los derechos podrán acordar más restricciones al ejercicio de los derechos ARCO.

10. DE LA LÍNEA DE DENUNCIA

Todo Sujeto Obligado tendrá conocimiento de la línea de denuncia y tendrá acceso a la misma.

El Sistema Integral de Denuncias quedará abierto al público en general, el cual operará de manera independiente y, administrado por un consultor externo contratado por la Dirección de Auditoría, el cual guardará la privacidad y confidencialidad del reporte respetando de forma conjunta las Políticas que integran el Programa de Cumplimiento Normativo de GMXT.

El Sistema Integral de Denuncias opera:

1. Página web:

    A) gmt.lineadedenuncia.net

    B) www.ferromex.mx (dar clic en "Gobierno Corporativo", "Integridad y Cumplimiento").

2. Línea telefónica dedicada a recibir denuncias: 800 1088 869

    C) Horarios de atención: de lunes a viernes de 8 a.m. a 10 p.m.

    D) Buzón de voz en días festivos, fines de semana y horarios fuera de los horarios de atención.

3. Correo electrónico: gmt@lineadedenuncia.net

Para efectos del Sistema Integral de Denuncias, habrá un Comité de Ética integrado de la forma que enuncia el Código de Ética.

11. PROCEDIMIENTO DE DENUNCIA

Toda denuncia tendrá su debido seguimiento:

A) Las denuncias serán recibidas por medio del Sistema Integral de Denuncias de FXE y los diferentes medios de recepción de las denuncias enlistadas en el apartado *10. De la Línea de Denuncia*.

B) Se asignará un folio de denuncia por cada una de las denuncias que se reciba, salvo aquellas que sean para un mismo hecho y/o acto, las cuales serán atendidas de forma conjunta.

C) Cada denuncia será clasificada conforme a su relevancia, la cual podrá ser alta, media o baja. Las denuncias altas tendrán prioridad de seguimiento, las cuales serán las denuncias de situación laboral y soborno.

D) Para efectos de investigación, el Comité de Ética será el órgano encargado de nombrar al área de FXE responsable para el proceso de investigación. El área involucrada responsable de realizar la investigación deberá entregar un reporte al Comité de Ética con respecto al proceso de la investigación.

E) El Comité de Ética revisará y recabará toda la información necesaria para confirmar y/o comprobar la veracidad de los hechos denunciados y tomar las consecuencias que considere pertinente.

F) Se mantendrá en todo momento la confidencialidad e identidad del denunciante sobre la posible violación. De igual forma, nadie será despedido, degradado, suspendido, acosado o discriminado por denunciar de buena fe una posible violación a la Política.

G) En los casos en los que se tengan pruebas sobre algún hecho denunciado, FXE dará el Aviso de Corrupción, de conformidad con lo descrito en la definición correspondiente.

H) Las decisiones del Comité de Ética se tomarán por mayoría calificada de votos presentes por parte de los miembros del Comité de Ética.

I) El Comité de Ética sesionará cada 3 meses y/o cuando el caso que se trate así lo amerite.

J) El quorum necesario para que las sesiones del Comité de Ética sean válidas será del 50% de los integrantes.

K) Cuando existiera un conflicto de interés en la denuncia entre los integrantes del Comité de Ética y el caso, se le dará a conocer al Comité y el miembro en cuestión no podrá votar.

12. DEL INCUMPLIMIENTO DE LA POLÍTICA PDP

12.1. De la Política PDP

1. Todo Sujeto Obligado que tenga conocimiento de cualquier riesgo, incidente, amenaza o vulneración de los datos personales o vulneración al sistema, deberá dar aviso, conforme al SGSDP a la Dirección Digital para eliminar cualquier riesgo o violación al sistema de seguridad.

2. Será responsable del tratamiento adecuado de los datos el Responsable, sin embargo, podrá repetir contra el encargado por el mal uso de la información y/o incumplimiento de los lineamientos establecidos para tales fines.

3. En caso de controversia por la vulneración de los datos personales, Las Partes podrán dirigirse a un mediador o al Instituto Nacional de Acceso a la Información (INAI) para la resolución de la controversia.

4. Cualquier vulneración o uso indebido de los datos personales, se aplicarán las sanciones establecidas en la Ley de Protección de Datos, su Reglamento y el Código Penal Federal, con respecto al uso indebido de los datos personales. Así como lo establecido en la Política PDP.

12.2. De las Sanciones

1. El Personal de FXE, a través de la capacitación, conocerán las consecuencias y sanciones de la Política PDP y demás que se encuentren publicadas, por lo que tendrá la obligación de reportar a su superior directo, y en su caso al Área de Cumplimiento cualquier incumplimiento de los principios del Programa de Cumplimiento Normativo de GMXT del que tenga conocimiento.

2. Nadie será despedido, degradado, suspendido, acosado o discriminado por denunciar de buena fe una posible violación a la Política PDP y su marco normativo.

3. Los Sujetos Obligados que tengan conocimiento de cualquier incumplimiento a la Política PDP o la normatividad en la materia, y no den aviso oportuno, podrá evaluarse como un acto de colusión, aplicando las sanciones específicas para el caso.

4. Las sanciones serán:

    A) Proporcionales al incumplimiento.

    B) Revisado por los Comités de Ética y Conducta y Auditoría, conforme a sus lineamientos.

    C) Para el Personal de FXE podrá ser desde una llamada de atención, levantamiento de un acta administrativa, hasta la recisión del contrato laboral.

    D) La aplicación de actos de sanción para Terceros y, para los casos que aplique, se respetará en todo momento lo dispuesto en la Ley Reglamentaria del Servicio Ferroviario y su Reglamento.

    E) La presentación de acciones legales ante los tribunales y/o autoridades competentes.

5. FXE se reserva el derecho de iniciar un proceso judicial y/o administrativo en contra de cualquier Sujeto Obligado que incumpla y vulnere el marco normativo de la materia.

6. El desconocimiento por parte del Personal de FXE a lo dispuesto en la Política PDP no los exime de su cumplimiento.

7. En caso de controversia, se tendrá que remitir a la Ley de Protección de Datos y su Reglamento.

8. El Responsable del tratamiento de los datos personales será responsable en caso de mal uso de la información y en caso de incumplimiento de la Política PDP y demás normas aplicables sobre la materia. De igual forma, el Responsable deberá de tomar los mecanismos establecidos por la Dirección de Digital y será el encargado de salvaguardar las contraseñas de los diversos sistemas a los que tenga acceso las cuales sean confidenciales e intransferibles.

9. Toda terminación laboral debe apegarse a los procesos involucrados de la Dirección de Recursos Humanos y la Dirección de Digital, promoviendo que la separación del puesto sea de una manera ordenada, disminuyendo así el riesgo hacia los activos de información que son propiedad de FXE.

13. ANEXOS

A – Formato para la suscripción del "Certificado de Conocimiento y Cumplimiento"

Ferromex

_____, a _____

A todos los Sujetos Obligados,

Adjunto a la Política para la Protección de Datos Personales y sus Anexos de FXE, a la cual todos los accionistas, consejeros, directivos y empleados, así como a clientes, proveedores, consultores y todas aquellas personas que mantengan una relación comercial con FXE deben conocer y apegarse.

Es importante que se dé lectura al mismo y, sé que de existir algún conflicto de intereses y/o evento que contravenga este documento, lo reporten de inmediato de conformidad con el procedimiento de la Política Anticorrupción.

Agradeciendo su atención y observación a estas disposiciones oficiales internas de FXE aprovecho la oportunidad para enviarle un cordial saludo.

Atentamente,

El Director General

_____

Recibí y estudié la Política y me comprometo a cumplir cabalmente con él, así como reportar cualquier anomalía que observe:

Nombre: _____

Empresa: _____

Número de proveedor/empleado: _____

Fecha: _____

B) Tiempos de bloqueo de la Información

Documentos que deben conservarse y posteriormente eliminarse una vez terminada su fecha de retención.

	TIPO DE REGISTRO	PERIODO DE RETENCIÓN
CONTRATOS	Acuerdos	Diez años después del vencimiento[2]
INGENIERIA	Planos originales o medios de origen de diseños asistidos por computadora	Duración del producto o duración de la patente, incluyendo su extensión, lo que sea mayor
	Documentación técnica y de ingeniería (incluidas notas de diseño, notas de investigación, otros registros que indiquen el historial de desarrollo del producto)	Duración del producto o duración de la patente, incluyendo su extensión, lo que sea mayor
	Datos de pruebas e informes externos (terceros)	Duración del producto o duración de la patente, incluyendo su extensión, lo que sea mayor
FINANZAS	Planes de negocios	Cinco años después de la finalización del programa/proyecto
	Planes estratégicos	Permanente (sólo el Director Financiero, el Director General y el Contralor deben retener copias. Todas las demás deben ser destruidas al emitir nuevos planes)
	Informes de auditores	Permanente
	Presupuestos	Dos años
	Estados financieros anuales	Permanente
	Estados financieros trimestrales / mensuales	Cinco años

[2] Con base en el artículo 38 de Código de Comercio. Además, se deberá mantener la documentación original (art. 49 Código de Comercio). Es importante señalar, que la prescripción ordinaria en materia comercial es de 10 años (art. 1047 del Código de Comercio).

	Declaraciones de impuestos, cheques cancelados	Permanente
	Pólizas de seguro	Cinco años a partir de las fechas de vencimiento[3]
	Declaraciones de siniestro, evaluaciones, informes	Cinco años
	Cuentas por pagar (libro mayor y documentos complementarios)	Cinco años
	Cuentas por cobrar (libro mayor y documentos complementarios)	Cinco años después del pago final
	Cuentas anuladas/incobrables	Diez años
	Comprobantes de depósitos bancarios, estados de cuenta bancarios, cheques cancelados, incluidos los cheques de nómina cancelados	Cinco años
	Notas de crédito, facturas de ventas	Diez años
	Facturas de proveedores, informes de gastos de empleados	Diez años en caso de facturas de proveedores[4], Cinco años para informes de gastos de empleados
	Depreciación, registros de bajas de activos	Cinco años
	Datos de contabilidad de costos	Cinco años
	Hojas de balance de comprobación	Permanente
NÓMINA	Declaraciones de impuestos sobre nóminas	Cinco años, contado a partir de la fecha en la que se presentaron o debieron haberse presentado las declaraciones.[5]
	Resúmenes internos de nómina de pagos acumulada	Seis años
	Autorizaciones de deducciones a las nóminas de pagos, incluidas las voluntarias, asignaciones, etc.	Cinco años después del término del contrato

[3] De acuerdo con el artículo 81 de la Ley sobre el Contrato de Seguro, todas las acciones que deriven de este tipo de contrato prescriben en cinco años, tratándose de la cobertura de fallecimiento en los seguros de vida y en dos años, en los demás casos; y corren a partir de la fecha del acontecimiento que les dio origen.

[4] La prescripción ordinaria en materia comercial es de 10 años (art. 1047 del Código de Comercio).

[5] Con base en el artículo 30 del Código Fiscal de la Federación.

	Registro de utilidades de la nómina de pagos	Indefinido (revisar cada diez años)
OPERACIONES DE INVERSIONES	Informes contables	Permanente
	Facturación, incluida la correspondencia y los datos de desempeño	Indefinido (revisar cada diez años)
	Publicaciones de inversiones	Indefinido (revisar cada diez años)
	Informes de transacciones	Indefinido (revisar cada diez años)
RECURSOS HUMANOS: BENEFICIOS	Archivos sobre beneficios por invalidez y enfermedad	Indefinido (revisar cada diez años)
	Datos de costos de seguros colectivos de empleados	Seis años
	Reclamaciones de seguros de vida y hospitalarios colectivos	Seis años
	Solicitud y reclamaciones de planes de pensiones	Indefinido (revisar cada diez años)
	Archivos de jubilación individual	Indefinido (revisar cada diez años)
RECURSOS HUMANOS: RELACIONES CON EMPLEADOS	Solicitudes y currículos para empleo: candidatos no seleccionados	Un año (o hasta la resolución si se presenta una reclamación)[6]
	Solicitudes y currículos para empleo: candidatos seleccionados	Un año después del término del contrato de empleo[7]
	Acuerdos o contratos de los empleados	Mientras dure la relación laboral y hasta un año después de que se extinga la relación laboral.
	Evaluaciones del personal	Mientras dure la relación laboral y hasta un año después
	Capacitación y desarrollo	Tres años[8]

[6] En la medida que dichos datos personales ya no sean necesarios, deberán ser cancelados. Esto con base en el artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[7] En la medida que dichos datos personales ya no sean necesarios, deberán ser cancelados. Esto con base en el artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Con base en el artículo 804 de la Ley Federal del Trabajo.

[8] Con base en el artículo 153-F Bis de la Ley Federal del Trabajo.

	Reclamaciones de compensación por desempleo	Dos años después de la resolución
	Autorizaciones de empleo, cambios en los salarios y sueldos, permisos de ausencia, término del empleo, etc.	Mientras dure la relación laboral y hasta un año después de que se extinga la relación laboral.
REGISTROS CORPORATIVOS	Reglamentos, estatutos, actas de las juntas del Consejo	Permanente[9]
	Actas de las juntas de los comités del Consejo de Administración	Permanente[10]
	Notificaciones de las asambleas de accionistas y juntas de directores	Permanente
	Libros corporativos de la sociedad	Permanente
LEGAL	Archivos de debida diligencia (auditorías legales)	Permanente
	Presentaciones en organismos regulatorios	Indefinido (revisar cada diez años)
	Archivos de litigios	Diez años después de la resolución
	Registros de derechos de autor y marcas registradas	Permanente

[9] De acuerdo con el artículo 30 del Código Fiscal de la Federación. Las actas de las juntas del consejo de administración deben de ser debidamente integradas en los libros corporativos de la sociedad.

[10] De acuerdo con el artículo 30 del Código Fiscal de la Federación. Las actas de las asambleas de accionistas deben de ser debidamente integradas en los libros corporativos de la sociedad.

C. Requisitos de seguridad en contratos con terceros

1. **Cláusula de Término del contrato.-** Duración del contrato, que puede ser de uno o varios años o indefinido hasta que una de las partes decida finalizarlo.

2. **Cláusula de acuerdo de confidencialidad.-** Confidencialidad con los siguientes puntos:

    A) Definición de la información a ser protegida.

    B) Duración del acuerdo, incluyendo casos donde la confidencialidad pueda necesitar ser mantenida indefinidamente.

3. **Cláusula de informes y documentación.-** Se indicará el tipo de informes que el proveedor deberá entregar a la empresa y la periodicidad de cada informe. Asimismo, se indicará que otra documentación entregará el proveedor en caso de que sea necesario, para mantener la protección de la información de datos personales.

4. **Cláusula de propiedad y retorno de datos.-** Se especificará la propiedad de los datos que FXE ceda al proveedor y el derecho de recuperarlos cuando expire el contrato

5. **Cláusula de auditoría.-** Ferromex se reserva el derecho a auditar los servicios prestados por el tercero para asegurar el cumpliendo de la seguridad a los datos personales que se encuentren en posesión, administrados, o con acceso a éstos.

6. **Cláusula de recuperación del servicio ante desastres o eventos de fuerza mayor.-** Es obligación del tercero implementar una gestión de continuidad del servicio ante desastres o causa de fuerza mayor y donde estén involucrados datos personales.

7. **Cláusula de accesos lógicos del tercero.-**

    A) Declaración de que todos los accesos que no son explícitamente autorizados son prohibidos

    B) Derecho de revocar cualquier usuario o proceso del proveedor que ponga en riesgo la confidencialidad, integridad y disponibilidad de los datos personales.

8. Cláusula de notificación sobre incidentes de seguridad.- Se involucran los datos personales de la empresa.

AUTORIZACIONES

DIRECCIÓN JURÍDICA	DIRECCIÓN DE AUDITORÍA	DIRECCIÓN DE FINANZAS
REVISÓ Y AUTORIZÓ	REVISÓ Y AUTORIZÓ	REVISÓ Y AUTORIZÓ

DIRECCIÓN DE RECURSOS HUMANOS	DIRECCIÓN DE ABASTECIMIENTOS	DIRECCIÓN DIGITAL
REVISÓ Y AUTORIZÓ	REVISÓ Y AUTORIZÓ	REVISÓ Y AUTORIZÓ

AUTORIZÓ
DIRECCIÓN GENERAL DE ADMINISTRACIÓN