DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DE IMPRESORA Y ENCUADERNADORA PROGRESO, S.A. DE C.V.

ÍNDICE

INTRODUCCIÓN..... 3
OBJETIVO..... 4
MARCO NORMATIVO..... 5
ÁMBITO DE APLICACIÓN..... 6
GLOSARIO DE TÉRMINOS..... 7
INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO..... 10
FUNCIONES Y OBLIGACIONES DE LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATAN DATOS PERSONALES..... 16
ANÁLISIS DE RIESGO..... 52
ANÁLISIS DE BRECHA..... 77
PLAN DE TRABAJO..... 100
MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD..... 105
PROGRAMA GENERAL DE CAPACITACIÓN..... 115
ANEXO 1, RESULTADO DEL CUESTIONARIO POR UNIDAD ADMINISTRATIVA DE LAS MEDIDAS A IMPLEMENTAR..... 118
ANEXO 2, ACUERDO DE CONFIDENCIALIDAD..... 123
ANEXO 3, REGISTRO DE INCIDENCIAS..... 124

INTRODUCCIÓN

El derecho a la protección de datos personales se encuentra previsto en el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, este derecho le confiere a las personas control sobre su información personal, faculta al individuo a decidir quién, cómo, cuándo y hasta qué punto utilizará su información personal, asimismo, protege el manejo justo de su información personal al garantizarle el acceso, rectificación, cancelación u oposición de sus datos personales.

Las reformas que ha tenido dicho precepto legal, propiciaron la publicación de la Ley Federal de Protección de Datos en Posesión de los Particulares, así como la emisión de una Ley General respecto de la información en posesión de los entes públicos.

Bajo este tenor, surge la 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, misma que establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de los entes públicos de los tres órdenes de Gobierno, con la cual se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición mediante procedimientos sencillos y expeditos (Derechos ARCO).

Posteriormente se publicaron los 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, en los que se contemplan las obligaciones exigibles respecto de la protección de datos personales en el sector público federal.

Con la publicación de las disposiciones normativas citadas anteriormente, todas las dependencias y entidades al realizar el tratamiento de datos personales de personas físicas adquieren el carácter de *Responsables* por lo que deben tratar los datos personales bajo los principios jurídicos de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, además deben adoptar medidas de seguridad en atención a los sistemas de datos que traten.

La Ley General de Protección de Datos en Posesión de Sujetos Obligados prevé elaborar un documento de seguridad en el cual se describa y de cuenta de manera general sobre las medidas de seguridad, técnicas físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran en la Entidad.

Impresora y Encuadernadora Progreso, S.A. de C.V. en cumplimiento a las disposiciones legales aplicables en materia de Protección de Datos, tuvo a bien elaborar el presente Documento de Seguridad que garantizará el debido tratamiento de los datos personales, con responsabilidad y bajo medias de seguridad adecuadas.

OBJETIVO

De conformidad con el numeral 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que establece:

De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación

Se presenta el siguiente documento de seguridad que tiene por objeto identificar los datos personales que posee Impresora y Encuadernadora Progreso, S. A. de C.V., el tipo de datos que contiene cada sistema o inventario de datos, los responsables, administradores, encargados y usuarios de cada sistema así como las medidas de seguridad concretas implementadas y proveer un marco de trabajo para el tratamiento de datos personales, que permita mantener y mejorar el cumplimiento de la legislación sobre la protección de datos personales.

MARCO NORMATIVO

Para efectos del presente documento la normatividad aplicable de manera enunciativa, más no limitativa, es la siguiente:

- Constitución Política de los Estados Unidos Mexicanos, (publicada en el Diario Oficial de la Federación el 5 de febrero de 1917).
- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, (Publicada en el Diario Oficial de la Federación el 26 de enero de 2017).
- Ley General de Transparencia y Acceso a la Información Pública, (Publicada en el Diario Oficial de la Federación el 04 de mayo de 2015).
- Ley Federal de Transparencia y Acceso a la Información Pública, (Publicada en el Diario Oficial de la Federación el 09 de mayo de 2016).
- Lineamientos Generales para la 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 procedimientos para la portabilidad de datos personales (Publicados en el Diario Oficial de la Federación el 12 de febrero de 2018).
- Ley Orgánica de la Administración Pública Federal. (Publicada en el Diario Oficial de la Federación el 29 de diciembre de 1976)
- Ley General de Responsabilidades Administrativas (Publicada en el Diario Oficial de la Federación el 18 de julio de 2016)
- Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas. (Publicados en el Diario Oficial de la Federación el 15 de abril de 2016)
- Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V.

ÁMBITO DE APLICACIÓN

El presente Documento de Seguridad es aplicable a todas las Unidades Administrativas y a las personas servidoras públicas de Impresora y Encuadernadora Progreso, S.A. de C.V., que en el ejercicio de sus atribuciones y funciones administren, manejen y/o tengan acceso a los expedientes físicos así como a los archivos electrónicos que contengan datos personales, y a las personas externas que debido a la prestación de un servicio, tengan acceso a los sistemas, documentos o al sitio donde se ubiquen los mismos.

Asimismo, están obligados a conocer y aplicar las medidas de seguridad propias de cada sistema o documento independiente del soporte en que se encuentren, y a resguardar la confidencialidad, aún después de que los involucrados hayan finalizado su participación en el tratamiento de los datos personales, deberán estar capacitados en materia de tratamiento de datos personales y dar aviso a los superiores jerárquicos, cualquier acción que pueda poner en riesgo los datos personales o la seguridad de los mismos.

Derivado de lo anterior, con la finalidad de identificar las funciones y obligaciones de las personas servidoras públicas que tratan los datos personales de la Entidad, para el presente documento se utilizaran los siguientes roles:

- **Responsable del Sistema:** Se refiere a la persona titular de la Unidad Administrativa encargada del tratamiento de los datos personales.

- **Administrador del Sistema:** Será el servidor público que designe de manera expresa el Titular de la Unidad Administrativa, quien maneje directamente el documento o sistema.

- **Usuarios:** Se refiere a las Personas servidoras públicas que manejen, manipulen o tengan acceso al sistema o documento que contiene datos personales.

El incumplimiento a lo establecido en el presente documento de seguridad, o en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, causará la aplicación de medidas de apremio y/o sanciones que detalla el citado instrumento normativo.

GLOSARIO DE TÉRMINOS

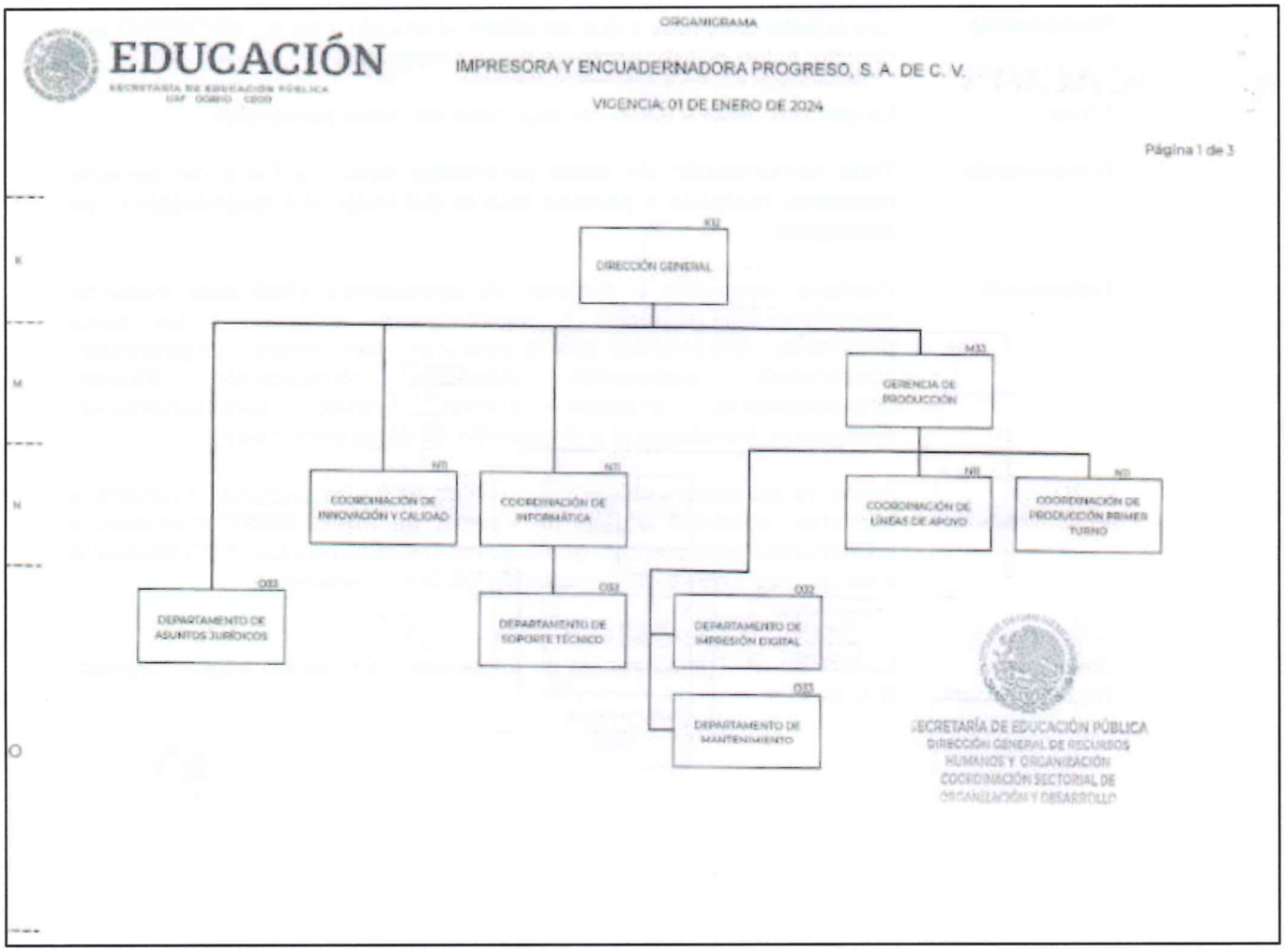
Aviso de privacidad:	Documento a disposición del titular de forma física, electrónica o en cualquier formato, generado por el responsable, a partir del momento en el cual se recaban sus datos personales, con el objeto de informarle los propósitos de tratamiento de los mismos.
Bases de datos:	Conjunto 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 recabadas, 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.
Cómputo en la nube:	Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.
Comité de Transparencia:	Instancia colegiada a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.
Consentimiento:	Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.
Datos Personales:	Cualquier información concerniente a una persona física identificada o identificable.
Datos Personales Sensibles:	Información que se refieren a la esfera más íntima de su titular, o cuya utilización indebida puedan 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:	Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus Personas servidoras públicas e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico.
Derechos Arco:	Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
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.
Días:	Días hábiles.
Expediente:	Unidad documental constituida por uno o varios documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados.
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.
IEPSA:	Impresora y Encuadernadora Progreso, S.A. de C.V.
Instituto:	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.
LFTAIP:	Ley Federal de Transparencia y Acceso a la Información Pública.
LGPDPPSO:	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
LINEAMIENTOS:	Lineamientos Generales de Protección de Datos Personales para el Sector Público.
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.
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.
PNT:	Plataforma Nacional de Transparencia.
Remisión:	Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.
Responsable:	Los sujetos obligados a que se refiere el artículo 1 de la LGPDPPSO que deciden sobre el tratamiento de datos personales.
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:	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.
Unidades administrativas:	Áreas de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos, manual de organización, manuales o instrumentos equivalentes, que cuenten o puedan contar, dar tratamiento y ser responsables o encargadas de los datos personales.
Unidad de Transparencia:	La Unidad de Transparencia de Impresora y Encuadernadora Progreso, S.A. de C.V.

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

Enseguida se señalan las Unidades Administrativas que conforman Impresora y Encuadernadora Progreso, S.A. de C.V., de acuerdo al Organigrama y el Manual de Organización de la Entidad.



ORGANIGRAMA

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

IMPRESORA Y ENCUADERNADORA PROGRESO, S. A. DE C. V.

VIGENCIA: 01 DE ENERO DE 2024

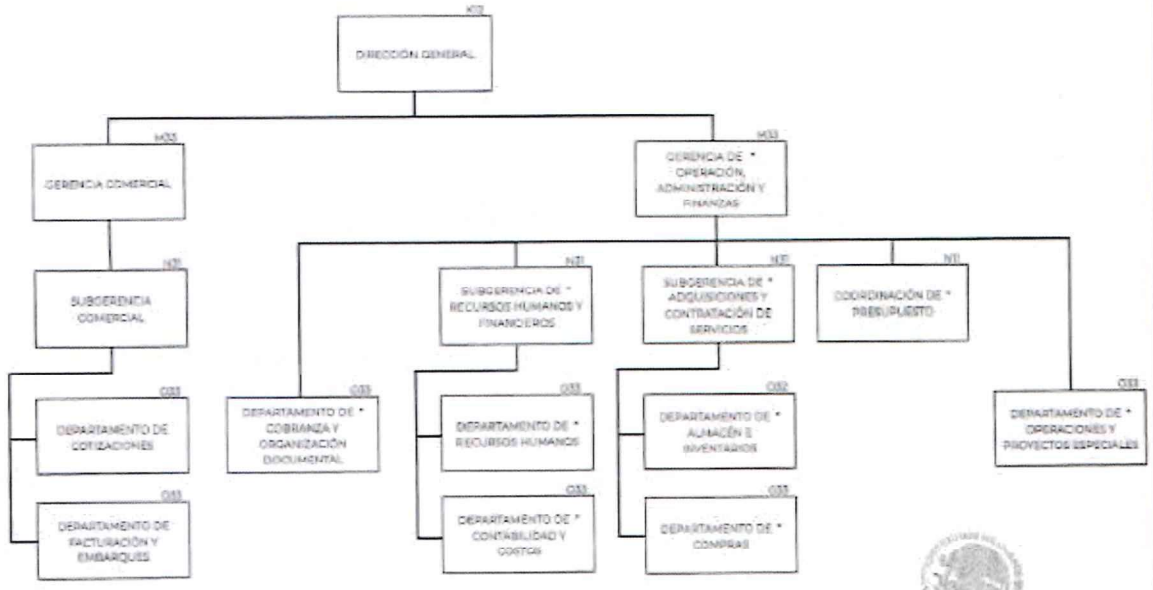
Página 2 de 3

K

M

N

O



SECRETARÍA DE EDUCACIÓN PÚBLICA
DIRECCIÓN GENERAL DE RECURSOS HUMANOS Y ORGANIZACIÓN
COORDINACIÓN SECTORIAL DE ORGANIZACIÓN Y DESARROLLO

* Designación directa

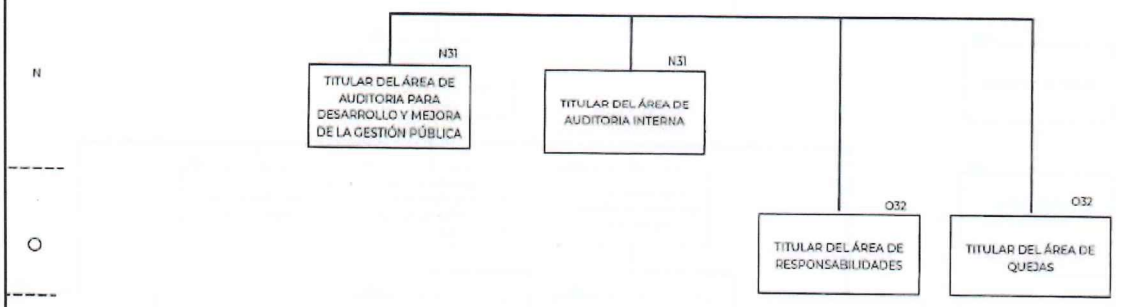
ORGANIGRAMA

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA
UAF 00200 C000

IMPRESORA Y ENCUADERNADORA PROGRESO, S. A. DE C. V.

VIGENCIA: 01 DE ENERO DE 2024

Página 3 de 3



SECRETARÍA DE EDUCACIÓN PÚBLICA
DIRECCIÓN GENERAL DE RECURSOS HUMANOS Y ORGANIZACIÓN
COORDINACIÓN SECTORIAL DE ORGANIZACIÓN Y DESARROLLO

I. Dirección General

II. Unidad de Transparencia/Gerencia de Operación, Administración y Finanzas

II.1 Solicitudes de Acceso a la Información y de ejercicios de Derechos ARCO

Aviso de Privacidad Integral de Solicitudes de Acceso a la Información y Datos Personales

III. Gerencia de Operación, Administración y Finanzas

III.1 Sistema Contpaqi

IV. Departamento de Recursos Humanos

IV.1 Expediente de personal
IV.2 Software BioStar
IV.3 Software Fortia

Aviso de privacidad para el personal de IEPSA.

V. Departamento de Contabilidad y Costos

VI. Subgerencia de Adquisiciones y Contratación de Servicios

VI.1 Contratos
VI.2 Sistema Compras-IEPSA

Aviso de privacidad para la contratación de servicios, arrendamientos y adquisición de bienes.

VII. Departamento de Compras

VII.1 Pedidos, Órdenes de Maquila y Solicitudes de Servicio
VII.2 Expediente de Proveedor

Aviso de Privacidad para el proceso de contratación de bienes de consumo, bienes muebles, materias primas, refacciones, servicios e integración de expedientes de proveedores.

VIII. Departamento de Almacén e Inventarios

VIII.1 Reporte de entrada al almacén (compra)

IX. Departamento de Operaciones y Proyectos Especiales

X. Departamento de Cobranza y Organización Documental

X.1.- Sistema de Cuentas por Cobrar

XI. Coordinación de Presupuesto

XII. Gerencia Comercial

XII.1 Expedientes de Contratos

Aviso privacidad para formalización de pedidos o contratos

XIII. Subgerencia Comercial

XIII.1. Seguimiento y atención a clientes

Aviso de privacidad para la comunicación, seguimiento y atención a clientes

XIV. Departamento de Cotizaciones

XIV.1. Elaboración de cotizaciones, órdenes de trabajo y carta de aceptación.

Aviso de privacidad para la elaboración de cotizaciones, órdenes de trabajo y carta de aceptación.

XV. Departamento de Facturación y Embarques

XV.1 Sistema de Facturación

Aviso de privacidad para facturas y notas de remisión

XVI. Gerencia de Producción

XVII. Coordinación de Producción Primer Turno

XVIII. Coordinación de Líneas de Apoyo

XVIII.1.- Expedientes de órdenes de trabajo

Aviso de privacidad para entrega de materiales y visitas a líneas de apoyo

XIX. Departamento de Impresión Digital

XX. Departamento de Mantenimiento

XX.1 Cotizaciones de Proveedores de Refacciones y/o Servicios

Aviso de privacidad de control de refacciones

XXI. Coordinación de Informática

XXI.1 Entradas y Salidas de Bienes Informáticos

Aviso de privacidad para posibles proveedores, registro de entradas y salidas de bienes informáticos.

XXII. Departamento de Soporte Técnico

XXII.1 DVR/Videograbación

Aviso de privacidad de Videograbación

XXIII. Coordinación de Innovación y Calidad

XXIII.1 Documento de actualización de la Licencia Ambiental
XXIII.2 Sistema COA web

XXIV. Departamento de Asuntos Jurídicos

XXIV.1 Escrituras Públicas de la Entidad
XXIV.2 Carpetas de estudios, dictámenes e informes/Incobrables
XXIV.3 Carpetas de juicios.

XXV. Órgano Interno de Control

*Los avisos de privacidad pueden consultarse en la página web de la Entidad en la sección de Datos Personales, https://www.iepsa.gob.mx/Datos_Pesonales.html

1.1. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATAN DATOS PERSONALES

Denominación de la Unidad Administrativa: **II.- Unidad de Transparencia /Gerencia de Operación, Administración y Finanzas**	
Nombre del sistema o inventario de Datos:	**II.1. Plataforma Nacional de Transparencia/ Solicitudes de Acceso a la Información y de ejercicios de Derechos ARCO.**
Finalidad u objetivo del sistema o documento:	Contar con un registro y dar seguimiento a las solicitudes de información o de derechos ARCO.
Fundamento:	Artículo 45, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, 61, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, 85, fracción II de la Ley General de Protección de Datos Personales, 86 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, y el numeral 5 fracción II del Manual de Integración y Funcionamiento de la Unidad de Transparencia y el Comité de Transparencia de Impresora y Encuadernadora Progreso, S.A. de C.V.
Datos personales contenidos en el sistema:	1. Nombre de la persona solicitante 2. Domicilio 3. Teléfono 4. Correo Electrónico 5. Sexo 6. Fecha de Nacimiento 7. Ocupación 8. Nivel Educativo 9. Nacionalidad
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Gerencia de Operación Administración y Finanzas y Titular de la Unidad de Transparencia
Funciones específicas al tratamiento de datos personales:	Coordinar las acciones relativas a la Unidad de Transparencia
Obligaciones:	Asegurar el resguardo de la información personal correspondiente a las solicitudes de acceso a la información así como a las de derechos ARCO
Administrador del Sistema o documento	
Cargo :	Titular de la Jefatura del Departamento de Asuntos Jurídicos y Servidor Público Habilitado en la Unidad de Transparencia
Funciones:	Coordinar las acciones relativas a la Unidad de Transparencia
Obligaciones:	Asegurar el resguardo de la información personal correspondiente a las solicitudes de acceso a la información así como a las de derechos ARCO
Usuarios del documento del sistema	
Cargo:	Secretaria A del Departamento de Asuntos Jurídicos.
Funciones :	Recepción y envío de solicitudes de acceso a la información y derechos ARCO a través de la Plataforma Nacional de Transparencia.
Obligaciones:	1.- Resguardar la documentación que contiene los datos personales.

Eliminado: 8 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	2.- Resguardar la confidencialidad de los datos personales de las personas solicitantes.
Cargo :	Secretaria del Departamento de Asuntos Jurídicos.
Funciones:	Acceso a las carpetas de la Unida de Transparencia para Archivo, resguardo y consulta de información.
Obligaciones:	1.- Resguardar la documentación que contiene los datos personales. 2.- Resguardar la confidencialidad de los datos personales de las personas solicitantes.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico y electrónico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos: (las características del sistema permite la portabilidad a su titular) en caso afirmativo especificar.	No, el sistema de la Plataforma Nacional de Transparencia es administrado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, no la Entidad.
Transferencia de Datos:	No
Encargado de Datos:	No

Denominación de la Unidad Administrativa: **III.- Gerencia de Operación, Administración y Finanzas**	
Nombre del sistema o inventario de Datos:	**III.1 Contpaqi**
Finalidad u objetivo del sistema o documento:	El Sistema es fundamental para el registro de los ingresos y gastos de la entidad para generar la información financiera y presupuestal que permita la toma de decisiones
Fundamento Legal:	Titulo Tercero Capitulo 1 de la Ley General de Contabilidad Gubernamental
Datos personales contenidos en el sistema o documento:	Nombre o Razón Social, Registro Federal de Contribuyente (RFC), Domicilio y Cuenta Bancaria.
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Gerencia de Operación, Administración y Finanzas
Funciones:	Análisis de Información
Obligaciones:	Supervisar el registro de las operaciones financieras-presupuestales
Cargo :	Titular de la Coordinación de Presupuesto
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar el registro de las operaciones financieras-presupuestales
Cargo:	Titular de la Subgerencia de Recursos Humanos y Financieros
Funciones	Generar y Analizar Información

Obligaciones	Supervisar el registro de las operaciones financieras-presupuestales
Cargo:	Titular de la Jefatura del Departamento de Cobranza y Organización Documental
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar el registro de las operaciones financieras-presupuestales
Cargo:	Titular de la Jefatura del Departamento de Contabilidad y Costos
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar el registro de las operaciones financieras-presupuestales
Administrador del Sistema o documento	
Cargo :	Analista
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Técnico Especializado
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo:	Analista
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Analista
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo:	Titular de la Jefatura del Departamento de Contabilidad y Costos
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar
Cargo :	Titular de la Subgerencia de Recursos Humanos y Financieros
Funciones:	Generar y Analizar Información
Obligaciones:	Supervisar
Cargo :	Titular de la Coordinación de Presupuesto
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar
Cargo :	Analista
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Titular de la Jefatura del Departamento de Cobranza y Organización Documental
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar
Cargo :	Analista Especializado
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Usuarios del documento de sistema de datos	
Cargo :	Analista
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Técnico Especializado
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Analista
Funciones:	Capturar Información

Eliminado: 4 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Analista
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Titular de la Jefatura del Departamento de Contabilidad y Costos
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar
Cargo :	Titular de la Subgerencia de Recursos Humanos y Financieros
Funciones:	Generar y Analizar Información
Obligaciones:	Supervisar
Cargo :	Titular de la Coordinación de Presupuesto
Funciones:	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar
Cargo :	Analista
Funciones:	Capturar Información
Obligaciones:	Registrar las operaciones de la entidad
Cargo :	Titular de la Jefatura del Departamento de Cobranza y Organización Documental
Funciones :	Generar, Analizar y Capturar Información
Obligaciones:	Supervisar
Cargo :	Analista Especializado
Funciones :	Capturar Información
Obligaciones:	Registrar las operaciones de la Entidad
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Combinado (Físico y electrónico)
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No
Transferencia de Datos	No
Encargado de Datos	No

Denominación de la Unidad Administrativa: **IV.- Departamento de Recursos Humanos**	
Nombre del sistema o inventario de Datos:	**IV.1. Expediente de Personal**
Finalidad u objetivo del sistema o documento:	Recabar datos personales para poder realizar los trámites correspondientes a la contratación del nuevo personal y resguardar los documentos que vinculan la relación laboral.
Fundamento Legal:	Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V. Función 9 del apartado correspondiente al Departamento de Recursos Humanos.
Datos personales contenidos en el sistema o documento:	▪ Carátula de expediente ◆ No. de empleado

	◆ Nombre ■ Contraportada con pestaña ◆ No. de empleado ◆ Nombre ◆ Fotografía ■ Solicitud de Empleo de IEPSA ◆ Nombre ◆ Fotografía ◆ Edad ◆ Sexo ◆ Domicilio Particular ◆ Estado Civil ◆ Fecha de Nacimiento ◆ Teléfono Particular ◆ Correo Electrónico ◆ Nacionalidad ◆ CURP ◆ RFC ◆ NSS ◆ Tipo de Sangre ◆ Último Grado de Estudios ◆ Ocupación ◆ Edad ◆ Fecha de Nacimiento ◆ Parentesco ◆ Crédito Infonavit ■ Requisición de Talento Humano ◆ Datos Económicos (sueldo) ■ Constancia de No Inhabilitación ◆ RFC ◆ Código QR ◆ Cadena de autenticidad ■ Acta de Nacimiento ◆ Fecha de Nacimiento ◆ Lugar de Nacimiento ◆ Sexo ◆ Edad ◆ Nombre ◆ Nacionalidad ◆ Edad ◆ Domicilio ◆ Fecha de Registro ◆ Año de Registro ◆ Cadena de Autenticidad ◆ Huella Digital ◆ Firma ■ Acta de Matrimonio ◆ Fecha de Nacimiento ◆ Lugar de Nacimiento ◆ Sexo ◆ Edad ◆ Nombre ◆ Nacionalidad ◆ Edad ◆ Domicilio ◆ Fecha de Registro ◆ Año de Registro ◆ Cadena de Autenticidad ◆ Huella Digital ◆ Firma ■ Constancia de Situación Fiscal

	◆ RFC ◆ Código QR ◆ CURP ◆ Domicilio Particular ◆ Cadena Original Sello ◆ Sello Digital ▪ Afore ◆ No. Afore ◆ Domicilio Particular ◆ NSS ◆ CURP ◆ RFC ◆ Código de barras ▪ Carta Laboral y/o Recomendación ◆ No. Empleado ◆ Nombre ◆ Domicilio Particular ◆ Teléfono Particular ◆ RFC ◆ Firma ▪ Comprobante de Domicilio ◆ Domicilio Particular ◆ Número de Cuenta ◆ Nombre ◆ Teléfono Particular ◆ Código de Barras ▪ Credencial para Votar ◆ Domicilio Particular ◆ Fotografía ◆ Edad ◆ Sexo ◆ Folio ◆ Clave de Elector ◆ CURP ◆ Código Bidimensional ◆ Código QR ◆ Huella Digital ◆ Número identificador OCR ◆ Firma ◆ Código de Barras Unidimensional ◆ Código de Barras Bidimensional ▪ Comprobante de Estudios ◆ CURP ◆ Fotografía ◆ Promedio ◆ Calificaciones ◆ Folio de Boleta ▪ Carnet de Citas Médicas ◆ NSS ◆ Fotografía ◆ CURP ◆ Edad ◆ Domicilio Particular ◆ Fecha de Nacimiento ◆ Lugar de Nacimiento ◆ Unidad de Atención Médica ▪ Formato CURP ◆ Nombre ◆ Fecha de Inscripción ◆ Entidad Federativa ◆ Clave CURP

	◆ Código QR ◆ Folio ✱ Currículum Vitae ◆ Fotografía ◆ Domicilio Particular ◆ Teléfono Particular ◆ Correo Electrónico ◆ CURP ◆ RFC ◆ NSS ✱ Formato Fondo de Ahorro ◆ No. Empleado ◆ Domicilio Particular ◆ Nombre ◆ Parentesco ✱ Formato Seguro de Vida ◆ RFC ◆ Sexo ◆ Estado Civil ◆ CURP ◆ Nombre ◆ Parentesco ✱ Movimiento de Personal en Nómina ◆ No. de Empleado ✱ Constancia de Situación Patrimonial ◆ RFC ◆ Homoclave ◆ Cadena ✱ Constancia de Habilidades Laborales DC-3 ◆ CURP ◆ RFC ◆ NSS ◆ Nombre ◆ Firma ✱ Alta IMSS ◆ Serial del Certificado ◆ Huella Digital ◆ Sello Digital ◆ CURP ✱ Contrato de Apertura de No. de Cuenta Bancaria ◆ CURP ◆ RFC ◆ Fecha de Nacimiento ◆ Nacionalidad ◆ Lugar de Nacimiento ◆ Domicilio Particular ◆ No. de Cliente ◆ Clabe Interbancaria ◆ No. de Cuenta ◆ No. de Tarjeta ◆ Teléfono Particular ◆ Correo Electrónico ✱ Contrato Individual de Trabajo ◆ No. de Empleado ◆ Fecha de Nacimiento ◆ Lugar de Nacimiento ◆ Nacionalidad ◆ Sexo ◆ Estado Civil ◆ Domicilio Particular

	◆ RFC ◆ CURP ◆ Salario ◆ Nombre ◆ Teléfono ◆ Parentesco ◆ Correo Electrónico ▪ Formato Finiquito ◆ No. de Empleado ◆ Salario Diario ◆ CURP ◆ RFC ◆ NSS ◆ Datos Económicos ◆ Huella Digital ▪ Carta Patronal ◆ CURP ◆ RFC ◆ NSS ◆ No. de Empleado ▪ Oficio de Pensión Alimenticia ◆ No. de Expediente ◆ Nombre ◆ Datos Económicos ▪ Estado de Cuenta Bancaria ◆ RFC ◆ No. de Cliente ◆ Domicilio Particular ◆ No. de Contrato ◆ Clabe Interbancaria ◆ No. de Tarjeta ◆ No. de Cheques ◆ Datos Económicos ▪ Carta de Renuncia ◆ Huella Digital ▪ Formato de Pago de Pensión Alimenticia ◆ Nombre ◆ Firma ◆ Datos Económicos ▪ Convenio Fuera de Juicio ◆ No. de Convenio ◆ Clave de Elector ◆ Nombre ◆ Datos económicos ◆ Firma ▪ Licencia de Conducir ◆ No. de Licencia ◆ Tipo de Licencia ◆ Vigencia ◆ Área de Adscripción ◆ Fecha de Expedición ◆ Nacionalidad ◆ RFC ◆ Fotografía ◆ Código QR ◆ Huella Digital ▪ Credencial de Trabajo ◆ No. de Empleado ◆ NSS ◆ CURP ◆ RFC

Eliminado: 11 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	Credencial IMSS • CURP • NSS • Código barras Cartilla Militar • Nombre • Fecha de Nacimiento • Lugar de Nacimiento • Estado Civil • CURP • Ocupación • Último grado de Estudios • Domicilio Particular • Fotografía • Matrícula • Huella Digital
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Jefatura del Departamento de Recursos Humanos
Funciones:	Autorizar los formatos de ingreso a la Entidad de cada persona trabajadora.
Obligaciones:	Supervisar y Resguardar los datos personales que las personas trabajadoras proporcionan.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura del Departamento de Recursos Humanos
Funciones:	Autorizar los formatos de ingreso a la Entidad de cada persona trabajadora.
Usuarios del documento de sistema de datos	
Cargo:	Recepcionista
Funciones:	Abrir expediente de la persona trabajadora, generar y capturar los datos personales para los formatos correspondientes de ingreso a la Entidad, archivar los documentos proporcionados por las personas trabajadoras que contengan información relevante para el pago de prestaciones y/o cálculo de nómina.
Obligaciones:	Archivar y resguardar los datos personales que proporcionen las personas trabajadoras en su expediente.
Cargo:	Profesionista Especializado
Funciones:	Dar de alta en el Sistema a la persona trabajadora con los datos proporcionados en el expediente para el correcto cálculo de nómina, archivar altas, bajas y movimientos de IMSS, archivar documentos relacionados a prestaciones (INFONAVIT, FONACOT, ETC).
Obligaciones:	Capturar Información
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	

Eliminado: 2 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	[redacted]
Portabilidad de datos:	No
Transferencia de Datos:	Sí. Se otorgan datos personales a proveedores para el pago de vales de despensa y para la cotización de seguro de vida de las personas trabajadoras. ▪ Contrato suministro de vales ▪ Contrato seguro de vida
Encargado de Datos:	No

Denominación de la Unidad Administrativa:	
IV.- Departamento de Recursos Humanos	
Nombre del sistema o inventario de Datos:	**IV.2 .- Software BioStar**
Finalidad u objetivo del sistema o documento:	Administrar y gestionar la asistencia de entradas y salidas de las personas trabajadoras de la Entidad.
Fundamento Legal:	Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V. Función 1 del apartado correspondiente al Departamento de Recursos Humanos.
Datos personales contenidos en el sistema o documento:	▪ Huella Digital ▪ Registro facial
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura del Departamento de Recursos Humanos
Funciones:	Registro de datos personales de las personas trabajadoras en el sistema.
Obligaciones:	Supervisar y Resguardar la confidencialidad de la información.
Administrador del Sistema o documento	
Cargo :	Titular de la Jefatura del Departamento de Recursos Humanos
Funciones:	Registro de datos personales de las personas trabajadoras en el sistema.
Obligaciones:	Supervisar y Resguardar la confidencialidad de la información
Usuarios del documento de sistema de datos	
Cargo :	Recepcionista
Funciones:	Registro de datos personales de las personas trabajadoras en el sistema
Obligaciones:	Resguardar la confidencialidad de la información
Cargo :	Profesionista Especializado
Funciones:	Registro de datos personales de las personas trabajadoras en el sistema
Obligaciones:	Resguardar la confidencialidad de la información
Cargo :	Analista
Funciones:	Registro de datos personales de las personas trabajadoras en el sistema
Obligaciones:	Resguardar la confidencialidad de la información
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Electrónico

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No
Transferencia de Datos	No
Encargado de Datos:	No

Denominación de la Unidad Administrativa: **IV.- Departamento de Recursos Humanos**	
Nombre del sistema o inventario de Datos:	**IV.3.-Software Fortia**
Finalidad u objetivo del sistema o documento:	Administrar los diferentes procesos de la nómina.
Fundamento Legal:	Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V. Función 1 del apartado correspondiente al Departamento de Recursos Humanos.
Datos personales contenidos en el sistema o documento:	* RFC * CURP * NSS * Fecha de Nacimiento * Sexo * Estado Civil * Domicilio Particular * Fotografía * Cuenta Bancaria
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura del Departamento de Recursos Humanos
Funciones:	Coordinar, Supervisar y generar Información
Obligaciones:	Supervisar que los datos que se capturan de las personas trabajadoras estén correctos.
Administrador del Sistema o documento	
Cargo :	Titular de la Jefatura del Departamento de Recursos Humanos
Funciones:	Coordinar, Supervisar y generar Información
Obligaciones:	Supervisar la captura de Información al Sistema
Usuarios del documento de sistema de datos	
Cargo :	Profesionista Especializado
Funciones:	Dar de alta a las personas trabajadoras en el Sistema, capturar los datos correspondientes para el cálculo de la nómina, generar el cálculo correspondiente para el pago de la nómina.
Obligaciones:	Calcular el pago correspondiente de la nómina de las personas trabajadoras.
Cargo :	Recepcionista
Funciones:	Capturar incidencias para el cálculo de la nómina, actualizar la información de las personas trabajadoras en el sistema y generar reportes del sistema para una correcta gestión en el cálculo de la nómina.
Obligaciones:	Capturar incidencias y mantener actualizada la información de las personas trabajadoras.
Cargo :	Analista

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Funciones:	Capturar incidencias para el cálculo de la nómina, actualizar la información de las personas trabajadoras en el sistema y generar reportes del sistema para una correcta gestión en el cálculo de la nómina.
Obligaciones:	Capturar incidencias de las personas trabajadoras.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Electrónico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No
Transferencia de Datos:	No
Encargado de Datos:	No

Denominación de la Unidad Administrativa: **VI.- Subgerencia de Adquisiciones y Contratación de Servicios**	
Nombre del sistema o inventario de Datos:	**VI.1 CONTRATOS**
Finalidad u objetivo del sistema o documento:	Formalizar la adquisición de bienes y la contratación de servicios.
Fundamento Legal:	Artículo 45 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 81 y 82 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
Datos personales contenidos en el sistema o documento:	1.- Nombre 2.- RFC 3.- Domicilio 4.- Cuentas y/o clabes interbancarias
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Subgerencia de Adquisiciones y Contratación de Servicios
Funciones:	*Adquisición de bienes y servicios de acuerdo a la norma aplicable. *Proveer de los insumos necesarios para el proceso de producción y desarrollo de las actividades de las áreas que conforman IEPSA.
Obligaciones:	Vigilar el correcto uso y resguardo de los contratos que contienen datos personales.
Administrador del Sistema o documento	
Cargo:	Analista
Funciones:	Integración de los expedientes de contratación
Obligaciones:	Resguardar correctamente los expedientes de contratación por los datos personales que contienen.
Usuarios del documento de sistema de datos	
Cargo:	Titular de la Jefatura del Departamento de Compras
Funciones:	Realización de los contratos
Obligaciones:	Utilizar los datos personales únicamente para la suscripción de los contratos y no compartir dicha información.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico y electrónico
Descripción:	[redacted]

Eliminado: 5 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Características del lugar en donde se resguardan los soportes:	[redacted]
Portabilidad de datos:	NO APLICA
Transferencia de Datos	NO APLICA
Encargado de Datos:	NO APLICA

Denominación de la Unidad Administrativa: **VI.- Subgerencia de Adquisiciones y Contratación de Servicios**	
Nombre del sistema o inventario de Datos:	**VI.2 SISTEMA DE COMPRAS**
Finalidad u objetivo del sistema o documento:	Realizar pedidos, órdenes de maquila, solicitudes de servicio, concentrar el catálogo de proveedores y de materiales
Fundamento Legal:	Título Primero, Capítulo III "Uso de Tecnologías de la Información y Comunicaciones", del Acuerdo por el que se modifica el diverso por el que se establecen las disposiciones en Materia de Recursos Materiales y Servicios Generales.
Datos personales contenidos en el sistema o documento:	*Nombre *RFC *Domicilio *Teléfono
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Subgerencia de Adquisiciones y Contratación de Servicios
Funciones:	Coordinar la realización de las adquisiciones de bienes como materia prima y promocional, así como la contratación de servicios de mantenimiento para IEPSA mediante la captura de pedidos, órdenes de maquila y solicitudes de servicio en el Sistema de Adquisiciones y Contratación de Servicios.
Obligaciones:	Vigilar que el uso de los datos personales que contienen los pedidos, órdenes de maquila y solicitudes de servicio, sea únicamente para la suscripción de los mismos.
Administrador del Sistema o documento	
Cargo :	Titular de la Jefatura del Departamento de Compras
Funciones:	Supervisión de la correcta captura y realización de los pedidos, órdenes de maquila y solicitudes de servicio, mediante el Sistema de Adquisiciones y Contratación de Servicios.
Obligaciones:	Vigilar que el uso de los datos personales que contienen los pedidos, órdenes de maquila y solicitudes de servicio, sea únicamente para la suscripción de los mismos.
Usuarios del documento de sistema de datos	
Cargo :	Analista
Funciones	Contratación de los trabajos de maquila y concentración del catálogo de proveedores
Obligaciones:	No divulgar los datos personales que son utilizados para la suscripción de los pedidos, órdenes de maquila y solicitudes de servicio, en el Sistema de Adquisiciones y Contratación de Servicios.
Cargo :	Técnico Especializado
Funciones:	1.- Adquisición de materia prima

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	2.- Contratación de productos promocionales
Obligaciones:	No divulgar los datos personales que son utilizados para la suscripción de los pedidos, órdenes de maquila y solicitudes de servicio, en el Sistema de Adquisiciones y Contratación de Servicios.
Cargo :	Profesionista Especializado
Funciones:	Contratación del Servicio de Mantenimiento para IEPSA y la Planta de Producción.
Obligaciones:	No divulgar los datos personales que son utilizados para la suscripción de los pedidos, órdenes de maquila y solicitudes de servicio, en el Sistema de Adquisiciones y Contratación de Servicios.
Cargo :	Analista
Funciones:	1.- Contratación de la Materia Prima (Proceso Productivo). 2.- Contratación de productos de consumo interno como medicamentos y papelería.
Obligaciones:	No divulgar los datos personales que son utilizados para la suscripción de los pedidos, órdenes de maquila y solicitudes de servicio, en el Sistema de Adquisiciones y Contratación de Servicios.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Electrónico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	NO APLICA
Transferencia de Datos:	NO APLICA
Encargado de Datos:	NO APLICA

Denominación de la Unidad Administrativa: **VII.- Departamento de Compras**	
Nombre del sistema o inventario de Datos:	**VII.1 Pedidos, Órdenes de Maquila y Solicitudes de Servicio**
Finalidad u objetivo del sistema o documento:	Formalizar las adquisiciones de bienes o la contratación de servicios.
Fundamento Legal:	Artículo 41 fracción XII y 42 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
Datos personales contenidos en el sistema o documento:	*Nombre *RFC *Domicilio
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura del Departamento de Compras
Funciones:	Vigilar la realización de las adquisiciones de bienes de materia prima, productos para consumo interno de la Entidad, así como promocionales y la contratación de servicios de mantenimiento, para IEPSA y la planta productiva.
Obligaciones:	Vigilar que el uso de los datos personales que contienen los pedidos, órdenes de maquila y solicitudes de servicio, sea únicamente para la suscripción de los mismos.

Eliminado: 9 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura del Departamento de Compras
Funciones:	Realizar la supervisión de la correcta integración documental de los expedientes de pedidos, órdenes de maquila y solicitudes de servicio.
Obligaciones:	Vigilar que los expedientes de contratación sean reguardados por los usuarios de manera correcta por los datos personales que contienen.
Usuarios del documento de sistema de datos	
Cargo :	Analista Técnico
Funciones:	Contratación de los trabajos de maquila
Obligaciones:	Resguardo de los expedientes de las Órdenes de Maquila, por los datos personales que contienen.
Cargo :	Técnico Especializado
Funciones:	1.- Adquisición de materia prima 2.- Contratación de productos promocionales
Obligaciones:	Resguardo de los expedientes que conforman los Pedidos, por los datos personales que contienen.
Cargo :	Profesionista Especializado
Funciones:	Contratación del Servicio de Mantenimento para IEPSA y la Planta de Producción.
Obligaciones:	Resguardo de los expedientes que conforman los Pedidos, por los datos personales que contienen.
Cargo :	Analista Técnico
Funciones:	1.- Contratación de la Materia Prima (Proceso Productivo) 2.- Contratación de productos de consumo interno como medicamentos y papelería
Obligaciones:	Resguardo de los expedientes que conforman los Pedidos, por los datos personales que contienen.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Electrónico y físico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	NO APLICA
Transferencia de Datos	NO APLICA
Encargado de Datos:	NO APLICA

Denominación de la Unidad Administrativa: **VII.- Departamento de Compras**	
Nombre del sistema o inventario de Datos:	**VII.2 Expediente de Proveedor**
Finalidad u objetivo del sistema o documento:	Concentrar los datos básicos de identificación de los proveedores
Fundamento Legal:	Punto 6 de las funciones de la Subgerencia de Adquisiciones y Contratación de Servicios y los puntos 1 y 4 de las funciones del Departamento de Compras del Manual de Organización de IEPSA
Datos personales contenidos en el sistema o documento:	1.- Nombre 2.- CURP 3.- Acta de nacimiento (Fecha de nacimiento, número de acta, lugar de nacimiento, Clave de Registro de

Eliminado: 9 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	Población, género, fecha de registro, datos de los padres del registrado como son domicilios y nombres, datos de los abuelos del registrado como son nombres y domicilios, además de nombres de personas físicas que participaron como testigos en el registro, firmas autógrafas y huellas dactilares) 4.- Edad 5.-Credencial para votar (Fotografía, domicilio, Folio de la identificación, Clave de Elector, CURP, edad, género y firma autógrafa) 6.- Teléfono particular 7.- Claves bancarias 8.- Comprobante de domicilio (Calle, número de inmueble, colonia, Alcaldía o Municipio, Entidad Federativa y Código Postal) 9.- Nombres de Accionistas y número de acciones. 10.- Cédula de Identificación Fiscal (RFC, CURP, domicilio, número móvil)
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Jefatura del Departamento de Compras
Funciones:	Instruir la debida integración de los expedientes de los proveedores.
Obligaciones:	Supervisar la integración del expediente del proveedor para el correcto resguardo de los documentos que contienen datos personales.
Administrador del Sistema o documento	
Cargo :	Titular de la Jefatura del Departamento de Compras
Funciones:	Coadyuvar a la integración de los expedientes de los proveedores.
Obligaciones:	Vigilar el tratamiento de los datos personales contenidos en los expedientes de los proveedores, corroborando que sean usados únicamente para la suscripción de pedidos, órdenes de maquila, solicitudes de servicio y contratos.
Usuarios del documento de sistema de datos	
Cargo :	Analista
Funciones:	Integración documental de los expedientes de los proveedores y captura de los datos necesarios en el Sistema de Adquisiciones y Contratación de Servicios en el apartado de Catálogo de Proveedores.
Obligaciones:	Resguardar y controlar el uso de los expedientes de los proveedores y controlar la base de registro de proveedores contenida en el Sistema de Adquisiciones y Contratación de Servicios, por los datos personales que ahí se encuentran.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico y Electrónico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	NO APLICA
Transferencia de Datos	NO APLICA
Encargado de Datos:	NO APLICA

Denominación de la Unidad Administrativa: VIII.- Departamento de Almacén e Inventarios	
Nombre del sistema o inventario de Datos:	**VIII.1.- Reporte de entrada al almacén (compra)**
Finalidad u objetivo del sistema o documento:	Comprobar el ingreso de los materiales al Almacén
Fundamento Legal:	Manual de Procedimientos Almacén e Inventarios. F-AL-01-04, página 40
Datos personales contenidos en el sistema o documento:	Nombre, Domicilio, Teléfono y Correo Electrónico.
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura del Departamento Almacén e Inventarios
Funciones:	Que los procesos de control, recepción y revisión de activo fijo, materia prima y/o materiales que ingresan al Almacén de la entidad se apliquen correctamente, a fin de que el abastecimiento recepción y entrega de los mismos se realice en tiempo y forma.
Obligaciones:	Verificar que la entrada de materia prima y/o materiales este soportada y sea congruente con la factura y/o remisión que ampara la entrega de dichos bienes, así mismo, corroborará con la captura en el Sistema de Inventarios que éste coincida con la remisión de compra.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura del Departamento Almacén e Inventarios
Funciones:	Que los procesos de control, recepción y revisión de activo fijo, materia prima y/o materiales que ingresan al Almacén de la entidad se apliquen correctamente, a fin de que el abastecimiento recepción y entrega de los mismos se realice en tiempo y forma.
Obligaciones:	Verificar que la entrada de materia prima y/o materiales este soportada y sea congruente con la factura y/o remisión que ampara la entrega de dichos bienes, así mismo, corroborará con la captura en el Sistema de Inventarios que éste coincida con la remisión de compra.
Usuarios del documento de sistema de datos	
Cargo:	Titular de la Subjefatura de Almacén
Funciones:	Recibir, verificar, acomodar, entregar, atender y manejo del Sistema de Almacén.
Obligaciones:	Resguardar datos personales.
Cargo:	Analista Especializado
Funciones:	Recibir, verificar, acomodar, entregar, atender y manejo del Sistema de Almacén.
Obligaciones:	Resguardar datos personales.
Cargo:	Analista
Funciones:	Recibir, verificar, acomodar, entregar, atender y manejo del Sistema de Almacén.
Obligaciones:	Resguardar datos personales.
Cargo:	Técnico Especializado
Funciones:	Recibir, verificar, acomodar, entregar, atender y manejo del Sistema de Almacén.
Obligaciones:	Resguardar datos personales.
Cargo:	Mensajero
Funciones:	Recibir, verificar, acomodar, entregar, atender y manejo del Sistema de Almacén.
Obligaciones:	Resguardar datos personales.

Eliminado: 4 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Estructura y Descripción del sistema o documento	
Tipo de soporte:	Combinado
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No
Transferencia de Datos	No
Encargado de Datos	No

Denominación de la Unidad Administrativa: **X.- Departamento de Cobranza y Organización Documental**	
Nombre del sistema o inventario de Datos:	**X.1.- Sistema de Cuentas por Cobrar**
Finalidad u objetivo del sistema o documento:	Registro, control y seguimiento de pago de facturas emisión de reportes de cobro y antigüedad de saldos.
Fundamento Legal:	Funciones 1, 2, 3,4 y 5 del Departamento de Cobranza y Organización Documental del Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V. Manual de Procedimientos. Cobranza, numerales 1 "Objetivo" y 8 "Descripción del Procedimiento".
Datos personales contenidos en el sistema o documento:	CLIENTES, Personas físicas 1.- Nombre 2.- Domicilio 3.- RFC
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Jefatura del Departamento de Cobranza y Organización Documental
Funciones:	1.-Gestionar la labor de cobranza con los clientes de IEPSA. 2.- Realizar la cobranza extrajudicial. 3.- Llevar el control y seguimiento de las facturas que han sido generadas a los clientes, para gestionar el cobro de las mismas. 4.- Realizar estadísticas, indicadores, informes y reportes de Cobranza y antigüedad de saldos.
Obligaciones:	1.- Verificar la incorporación de las facturas electrónicas en el sistema de cuentas por cobrar y revisarlas. 2.-Gestionar con los clientes el cobro de facturas. 3.- Registrar en el sistema de cuentas por cobrar la cobranza realizada.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura del Departamento de Cobranza y Organización Documental
Funciones:	1.- Gestionar la labor de cobranza con los clientes de IEPSA. 2.- Realizar la cobranza extrajudicial. 3.- Llevar el control y seguimiento de las facturas que han sido generadas a los clientes, para gestionar el cobro de las mismas. 4.- Realizar estadísticas, indicadores emisión de facturas para su cobro.
Obligaciones:	1.- Verificar la incorporación de las facturas electrónicas en el sistema de cuentas por cobrar y revisarlas. 2.- Gestionar con los clientes el cobro de facturas. 3.- Registrar en el sistema de cuentas por cobrar la cobranza realizada.

Eliminado: 5 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en matería de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Usuarios del documento de sistema de datos	
Cargo :	Analista Especializado
Funciones:	1.- Actualizar la cobranza en el sistema con base en los depósitos identificados en las cuentas bancarias de IEPSA. 2.- Elaborar el reporte semanal de cobranza. 3.- Elaborar los complementos de pago. 4.- Elaborar la conciliación de ingresos y cuentas por cobrar con el área de Contabilidad.
Obligaciones:	Mantener actualizado el sistema de cobranza
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Electrónico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	NO
Transferencia de Datos	NO
Encargado de Datos.	NO

Denominación de la Unidad Administrativa: **XII.- Gerencia Comercial**	
Nombre del sistema o inventario de Datos:	**XII.1.- Expedientes de Contratos.**
Finalidad u objetivo del sistema o documento:	Recabar y custodiar los contratos y convenios modificatorios así como sus términos de referencia.
Fundamento Legal:	Numeral 13 de las Funciones de la Gerencia Comercial establecidas en el Manual de Organización de Impresora y Encuadernadora Progreso, S.A de C.V.
Datos personales contenidos en el sistema o documento:	1. Nombre 2. Correo electrónico 3. Número telefónico 4. Datos contenidos en la credencia para votar • Edad • Sexo • Domicilio • Clave de elector • CURP • Firma • Fecha de Nacimiento
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Gerencia Comercial
Funciones:	Coordinar las actividades de la fuerza de ventas, los planes de comercialización y mercadeo, a fin de lograr posicionamiento de la empresa, con base en las políticas establecidas para la promoción, distribución venta de productos y servicios.
Obligaciones:	1. Resguardo de la documentación que contiene los datos personales. 2. Utilizar los datos personales unicamente para los fines que fueron recabados. 3. Guardar la confidencialidad de los datos personales.
Administrador del Sistema o documento	
Cargo :	Auxiliar Administrativo
Funciones:	Integración y resguardo de los expedientes de Contratos.

Eliminado: 5 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Obligaciones:	1.- Resguardo de la documentación que contiene los datos personales. 2.- Guardar la confidencialidad de los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico.
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No.
Transferencia de Datos:	No.
Encargado de Datos:	No.

Denominación de la Unidad Administrativa **XIII.- Subgerencia Comercial**	
Nombre del sistema o inventario de Datos:	**XIII.1. Seguimiento y Atención a Clientes**
Finalidad u objetivo del sistema o documento:	Elaboración de bitácoras para dar seguimiento al producto y atención a clientes.
Fundamento Legal:	Manual de Procedimientos, Ventas y Atención Institucional (P-CO-06). 6.1 Lineamientos para gestión de materiales y comunicación con el cliente con el formato Agenda de Ventas (F-CO-06-02 Rev. 1).
Datos personales contenidos en el sistema o documento:	1.- Nombre. 2.- Correo Electrónico. 3.- Domicilio. 4.- Número Telefónico.
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Subgerencia Comercial.
Funciones:	Ejecutar la labor de venta y la atención de clientes así como coordinar las estrategias de comercialización.
Obligaciones:	Resguardar la documentación que contiene datos personales correspondientes a las ventas.
Administrador del Sistema o documento	
Cargo :	Titular de la Subgerencia Comercial.
Funciones:	Recabar información de las instancias con las que se haya iniciado una labor de venta.
Obligaciones:	Resguardar la documentación que contiene datos personales correspondientes a las ventas.
Usuarios del documento de sistema de datos	
Cargo:	Analista Especializado.
Funciones:	• Recabar información de las instancias con las que se haya iniciado una labor de venta.
Obligaciones:	• Resguardar la documentación que contiene datos personales correspondientes a las ventas. • Guardar confidencialidad respecto a los datos personales.
Cargo :	Analista Especializado
Funciones:	• Recabar información de las instancias con las que se haya iniciado una labor de venta.
Obligaciones:	• Resguardar la documentación que contiene datos personales correspondientes a las ventas. • Guardar confidencialidad respecto a los datos personales.

Eliminado: 5 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Cargo :	Analista Especializado
Funciones:	• Recabar información de las instancias con las que se haya iniciado una labor de venta.
Obligaciones:	• Resguardar la documentación que contiene datos personales correspondientes a las ventas. • Guardar confidencialidad respecto a los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico y electrónico.
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No aplica.
Transferencia de Datos:	No aplica.
Encargado de Datos:	No aplica.

Denominación de la Unidad Administrativa: **XIV.- Departamento de Cotizaciones**	
Nombre del sistema o inventario de Datos:	**XIV.1. Elaboración de cotizaciones, Órdenes de Trabajo y Carta de Aceptación**
Finalidad u objetivo del sistema o documento:	Dirigir, remitir e identificar las cotizaciones así como las órdenes de trabajo y en su caso contacto con las Instancias, Entidades y personas físicas.
Fundamento Legal:	Manual de Procedimientos Gestión, Revisión y Seguimiento del Pedido (P-CO-01), Instructivo del llenado Formato Cotización (F-CO-01-01), Instructivo de llenado Formato Orden de trabajo (F-CO-01-04). 6.3 de los Lineamientos para la elaboración de Cotizaciones, numeral 25 y 6.4 de los Lineamientos para la elaboración de órdenes de Trabajo numeral 3.
Datos personales contenidos en el sistema o documento:	1.-Nombre 2.- Correo electrónico 3.- Domicilio 4.-Número telefónico
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura de Departamento de Cotizaciones
Funciones:	Elaborar las cotizaciones de los productos, servicios de impresión y acabados que vende IEPSA; así como la elaboración y entrega oportuna de órdenes de trabajo y el resguardo de la documentación que respalda dicho proceso.
Obligaciones:	1. Resguardo de la documentación que contiene los datos personales. 2. Utilizar los datos personales únicamente para los fines que fueron recabados. 3. Guardar la confidencialidad de los datos personales.
Administrador del Sistema o documento	
Cargo :	Analista especializado
Funciones:	Integración y resguardo de los expedientes de cotizaciones.
Obligaciones:	1. Resguardo de la documentación que contiene los datos personales.

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	2. Guardar la confidencialidad de los datos personales.
Usuarios del documento de sistema de datos	
Cargo :	Analista especializado
Funciones:	Control y manejo de la información.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas.
Cargo :	Analista especializado
Funciones :	Control y manejo de la información.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico.
Tipo de soporte:	Físico.
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No.
Transferencia de Datos:	No.
Encargado de Datos:	No.

Denominación de la Unidad Administrativa: **XV.- I. Departamento de Facturación y Embarques**	
Nombre del sistema o inventario de Datos:	**XV.1. Sistema de Órdenes de Trabajo y Facturación**
Finalidad u objetivo del sistema o documento:	Emitir los CFDI'S (Facturación y notas de crédito) por la venta realizada con las instancias y personas así como la consulta de Órdenes de Trabajo.
Fundamento Legal:	(P-CO-05) MANUAL DE PROCEDIMIENTOS. Facturación: • FACTURA. Numeral 8, p. 9 y 10. • NOTA DE CRÉDITO. Numeral 8, p. 11 y 12.
Datos personales contenidos en el sistema o documento:	1.- Nombre. 2.- RFC. 3.- CIF (datos fiscales) 4.- Correo electrónico.
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura del Departamento de Facturación y Embarques
Funciones:	• Llevar a cabo el proceso de facturación oportunamente, el cual soporte monto de los trabajos entregados a los clientes, así como expedir Notas de Crédito que permitan respaldar la operación.
Obligaciones:	• Ejecutar el procedimiento desde la emisión y entrega de las facturas y Notas de Crédito al cliente, con el propósito de dar seguimiento al proceso de cobranza. • Resguardar de la documentación que contiene datos personales.

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Administrador del Sistema o documento	
Cargo;	Titular de la Jefatura del Departamento de Facturación y Embarques
Funciones:	• Llevar a cabo el proceso de facturación oportunamente, el cual soporte monto de los trabajos entregados a los clientes, así como expedir Notas de Crédito que permitan respaldar la operación.
Obligaciones:	• Ejecutar el procedimiento desde la emisión y entrega de las facturas y Notas de Crédito al cliente, con el propósito de dar seguimiento al proceso de cobranza. • Resguardar de la documentación que contiene datos personales.
Usuarios del documento de sistema de datos	
Cargo	Analista Especializado.
Funciones	• Elaborar la factura (o las que sean necesarias) de cada obra terminada y entregada, o servicios que IEPSA decida.
Obligaciones	• Resguardo de la documentación que contiene los datos personales. • Guardar confidencialidad respecto a los datos personales.
Cargo	Analista Especializado
Funciones:	• Elaborar la factura (o las que sean necesarias) de cada obra terminada y entregada, o servicios que IEPSA decida.
Obligaciones:	• Resguardo de la documentación que contiene los datos personales. • Guardar confidencialidad respecto a los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico y electrónico.
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No aplica.
Transferencia de Datos :	No aplica.
Encargado de Datos:	No aplica.

Denominación de la Unidad Administrativa: **XVIII.- Coordinación de Líneas de Apoyo**	
Nombre del sistema o inventario de Datos:	**XVIII.1- Expedientes de órdenes de trabajo**
Finalidad u objetivo del sistema o documento:	Llevar un control de las órdenes de trabajo que remiten/ envían a Líneas de Apoyo.
Fundamento Legal:	Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público artículo 1 párrafo sexto, artículo 4 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el primer párrafo de las responsabilidades de Coordinación de Líneas de Apoyo (P4), así como el numeral ocho, descripción del procedimiento del Manual de Procedimientos Líneas de Apoyo P-PR-03,).
	Nombre RFC

Eliminado: 4 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Datos personales contenidos en el sistema o documento:	Domicilio Teléfono particular Correo electrónico particular Firma
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Coordinación de Líneas de Apoyo
Funciones:	Identificar y resguardar las órdenes de trabajo que son enviadas a Líneas de Apoyo para realizar los procesos requeridos (en coordinación con la SACS).
Obligaciones:	Resguardar la documentación correspondiente a la orden de trabajo con la finalidad de dar seguimiento a los trabajos realizados, así como resguardar la información confidencial de los datos personales.
Administrador del Sistema o documento	
Cargo:	Analista Especializado
Funciones:	Dar trámite a los oficios requeridos para la solicitud de maquiladores y llevar los expedientes.
Obligaciones:	Archivo y resguardo de la documentación correspondiente a las órdenes de trabajo y confidencialidad de los datos personales.
Usuarios del documento de sistema de datos	
Cargo:	Supervisor
Funciones:	Consulta del expediente, supervisar los procesos de producción externa.
Obligaciones:	Dar seguimiento a las órdenes de trabajo asignadas a Líneas de Apoyo, informar o reportar cualquier anomalía así como resguardar la documentación que contiene datos personales y utilización de los datos personales para los fines necesarios.
Cargo:	Analista
Funciones:	Entrega de materiales a las Líneas de Apoyo asignada, supervisión de los procesos.
Obligaciones:	Dar seguimiento a las órdenes de trabajo asignadas a Líneas de Apoyo, informar o reportar cualquier anomalía así como resguardar la documentación que contiene datos personales y utilización de los datos personales para los fines necesarios.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No
Transferencia de Datos:	No
Encargado de Datos:	No

Denominación de la Unidad Administrativa: **XX.- Departamento de Mantenimiento**	
Nombre del sistema o inventario de Datos:	**XX.1.- Cotizaciones de Proveedores de Refacciones y/o Servicios**
Finalidad u objetivo del sistema o documento:	Llevar un control de los servicios de mantenimiento y reparación en maquinaria e instalaciones.
Fundamento Legal:	Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público artículo 1 párrafo quinto, artículo 42 del

Eliminado: 5 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el primer párrafo de las responsabilidades Mantenimiento Correctivo (P2) y Mantenimiento Preventivo (P1), así como el numeral ocho, descripción del procedimiento de los Manuales de Procedimientos Mantenimiento Preventivo (P-MA-01) y Mantenimiento Correctivo (P-MA-02,).
Datos personales contenidos en el sistema o documento:	Nombre, RFC, Domicilio, Teléfono, Correo electrónico particular, Firma.
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura de Mantenimiento
Funciones:	Identificar y resguardar la cotización de servicios y/ o refacciones para la realización de los procesos de los servicios de mantenimiento y reparación de maquinaria e instalaciones, en coordinación con la Subgerencia de Adquisiciones y Contratación de Servicios.
Obligaciones:	Resguardar la documentación correspondiente a los servicios y/o refacciones de los procesos de maquinaria e instalaciones, así como resguardar la información confidencial de los datos personales.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura de Mantenimiento
Funciones:	Identificar y resguardar la cotización de servicios y/ o refacciones para la realización de los procesos de los servicios de mantenimiento y reparación de maquinaria e instalaciones, en coordinación con la Subgerencia de Adquisiciones y Contratación de Servicios.
Obligaciones:	Resguardar la documentación correspondiente a los servicios y/o refacciones de los procesos de maquinaria e instalaciones, así como resguardar la información confidencial de los datos personales.
Usuarios del documento de sistema de datos	
Cargo:	Titular de la Coordinación de Producción Primer Turno
Funciones:	Dar trámite a los servicios y/o refacciones requeridos para el mantenimiento Preventivo y Correctivo. Mantenimiento de la maquinaria y equipo de la planta productiva para preservar las condiciones de operación.
Obligaciones:	Archivo y resguardo de la documentación correspondiente a las refacciones y/o servicios correspondiente a las instalaciones y maquinaria de la planta productiva.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	NO
Transferencia de Datos	NO
Encargado de Datos:	NO

Eliminado: 3 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Denominación de la Unidad Administrativa: XXI.- Coordinación de Informática	
Nombre del sistema o inventario de Datos:	**XXI.1. Entradas y Salidas de Bienes Informáticos**
Finalidad u objetivo del sistema o documento:	Llevar un control sobre los bienes informáticos que ingresan o salen de la Coordinación de Informática.
Fundamento Legal:	Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración pública Federal en su Capítulo VI Artículo 76.
Datos personales contenidos en el sistema o documento:	1.-Nombre 2.- Firma
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Coordinación de Informática
Funciones:	Coordinar la operación de los servicios informáticos de IEPSA.
Obligaciones	La implementación de los controles mínimos de seguridad de la información y resguardo de datos personales.
Administrador del Sistema o documento	
Cargo	Técnico especializado
Funciones :	Coordinar con empresas contratadas la salida y entrada de equipo de cómputo e impresión para su mantenimiento preventivo y/o correctivo que sean necesarios.
Obligaciones:	1.- Resguardar la documentación que contiene los datos personales.
Usuarios del documento de sistema de datos	
Cargo :	Titular de la Jefatura del Departamento de Soporte Técnico
Funciones:	Coordinar con empresas contratadas la salida y entrada de equipo de cómputo e impresión para su mantenimiento preventivo y/o correctivo que sean necesarios.
Obligaciones:	1.- Resguardar la documentación que contiene los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No
Transferencia de Datos	No
Encargado de Datos:	No

Denominación de la Unidad administrativa: XXII.- Departamento de Soporte Técnico	
Nombre del sistema o inventario de Datos:	**XXII.1.-DVR/Videograbación**
Finalidad u objetivo del sistema o documento:	Preservar la seguridad de las personas y las instalaciones de IEPSA.
Fundamento Legal:	Artículo 6 y 16 segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos; artículo 68 de la Ley General de Transparencia y Acceso a la Información Pública; artículo 9 de la Ley Federal de Transparencia y Acceso a la Información Pública; y función 9 del Manual

Eliminado: 3 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V., Departamento de Soporte Técnico.
Datos personales contenidos en el sistema o documento:	Imagen de personas.
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Jefatura de Departamento de Soporte Técnico
Funciones:	Administrar el sistema de video vigilancia que controla las cámaras instaladas en el Entidad.
Obligaciones:	Tratar los datos personales de acuerdo con el tratamiento autorizado, mantener la confidencialidad e integridad de los datos personales.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura de Departamento de Soporte Técnico
Funciones:	Administrar el sistema de video vigilancia que controla las cámaras instaladas en el Entidad.
Obligaciones:	Tratar los datos personales de acuerdo con el tratamiento autorizado, mantener la confidencialidad e integridad de los datos personales.
Usuarios del documento de sistema de datos	
Cargo:	Titular de la Coordinación de Informática
Funciones:	Revisar el video grabado y crear copia del video grabado.
Obligaciones:	Tratar los datos personales de acuerdo con el tratamiento autorizado, mantener la confidencialidad e integridad de los datos personales.
Cargo :	Técnico especializado
Funciones:	Revisar video grabado; Crear copia del video grabado.
Obligaciones:	Tratar los datos personales de acuerdo con el tratamiento autorizado, mantener la confidencialidad e integridad de los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Digital
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No.
Transferencia de Datos:	No.
Encargado de Datos:	Contrato de prestación de servicios de seguridad, protección y vigilancia; el resguardo de este documento está a cargo de la Subgerencia de Adquisiciones y Contratación de Servicios.

Denominación de La Unidad Administrativa: **XXIII.- Coordinación de Innovación y Calidad**	
Nombre del sistema o inventario de Datos:	**XXIII.1 Expediente Para Actualizar Licencia Ambiental**
Finalidad u objetivo del sistema o documento:	Regular ambientalmente a los responsables de las fuentes fijas de competencia de la Cuidad de México, mediante la determinación y seguimiento del cumplimento de sus obligaciones ambientales.
Fundamento Legal:	Artículo 61 bis, 61 bis 1, 61 bis 2, de la Ley Ambiental de Protección a la tierra del Distrito Federal Artículo 55 fracción X del Reglamento Interior de la Administración Pública del Distrito Federal. Artículo 1, 16 fracción X y 35 fracción XV de la Ley Orgánica del Poder Ejecutivo y de la Administración Pública de la Cuidad de México.

Datos personales contenidos en el sistema o documento:	1.- Datos contenidos en el pasaporte: • Nombre completo. • Fecha y lugar de nacimiento. • Nacionalidad. • Sexo. • CURP. • Fotografía. • Firma. • Número de pasaporte. 2.- Datos contenidos en la credencial para votar: • Nombre completo. • Clave de elector. • Domicilio. • Fecha de nacimiento. • CURP. • Sexo. • Fotografía. • Firma. • Folio de credencial. 3.- Datos Contenidos en el poder notarial: • Nombre completo. • Domicilio. • Fecha y lugar de nacimiento. • Estado civil. • Sexo. • Edad. • Ocupación. • Régimen patrimonial (en caso de estar casado)
Responsable del Sistema o documento que contiene Datos Personales	
Cargo	Titular de la Coordinación de Innovación y Calidad
Funciones	Llevar a cabo el trámite de la actualización de la Licencia Ambiental Única de la Ciudad de México
Obligaciones	Cumplir con los requerimientos solicitados por diferentes organismos (STPS, SEMARNAT, CONNUE, etc.), con el objetivo de lograr que las actividades que se realizan en IEPSA se apeguen a las normas estipuladas para su operación.
Administrador del Sistema o documento	
Cargo	Titular de la Coordinación de Innovación y Calidad
Funciones	Integrar la información, documentación y estudios técnicos necesarios para realizar el trámite de actualización de la Licencia Ambiental Única para la Ciudad de México.
Obligaciones	Cumplir con los requerimientos solicitados por diferentes organismos (STPS, SEMARNAT, CONNUE, etc.), con el objetivo de lograr que las actividades que se realizan en IEPSA se apeguen a las normas estipuladas para su operación, así como resguardar los datos personales contenidos en dicho documento.
Usuarios del documento de sistema de datos	
Cargo	Analista Técnico
Funciones	Revisar información y compilar los documentos.
Obligaciones	Resguardar y archivar la información y documentación integrada de cada área, como soporte del trámite de actualización de la Licencia Ambiental Única para la Ciudad de México.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No
Transferencia de Datos:	SI El trámite se realiza por medio de un proveedor externo para el trámite, entrega y gestoría ante la Secretaría del Medio Ambiente de la Ciudad de México hasta su conclusión.
Encargado de Datos:	SI El instrumento normativo para la formalización de servicio es mediante la Orden de Servicio.

Denominación de la Unidad Administrativa: **XXIII.- Coordinación de Innovación y Calidad**	
Nombre del sistema o inventario de Datos:	**XXIII.2. Expediente para actualizar la Cédula de Operación Anual/Sistema COA web**
Finalidad u objetivo del sistema o documento:	Obtener e informar a la SEMARNAT el reporte de las emisiones y transferencias de contaminantes a la atmosfera, suelo, agua y de residuos peligros de IEPSA
Fundamento Legal:	Artículo 111 Bis segundo párrafo de Ley General del Equilibrio Ecológico y la Protección al Ambiente. Artículos 17 Bis inciso K) y 21 Reglamento de la Ley General del Equilibrio Ecológico y la Protección al Ambiente en Materia de Prevención y Control de la Contaminación de la Atmósfera. Artículo 9 del Reglamento de la Ley General del Equilibrio Ecológico y la Protección al Ambiente en Materia de Registro de Emisiones y Transferencia de Contaminantes. Artículo 72 del Reglamento de la Ley General para la Prevención y Gestión Integral de los Residuos. Artículo 87 de la Ley General de Cambio Climático. Artículo 9 fracción V del Reglamento de la Ley General de Cambio Climático en materia del Registro Nacional de Emisiones.
Datos personales contenidos en el sistema o documento:	1.- Datos contenidos en el pasaporte: • Nombre completo. • Fecha y lugar de nacimiento. • Nacionalidad. • Sexo. • CURP. • Fotografía. • Firma. • Número de pasaporte. 2.- Datos contenidos en la credencial para votar: • Nombre completo. • Clave de elector. • Domicilio. • Fecha de nacimiento. • CURP. • Sexo. • Fotografía. • Firma. • Folio de credencial.

Eliminado: 2 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	3.- Datos contenidos en la Acta constitutiva o de asamblea • Nombre completo de los accionistas. • RFC. • Aportaciones de los accionistas. • Estado civil. • Edad. • Ocupación. • Nacionalidad. 4.- Datos Contenidos en el poder notarial: • Nombre completo. • Domicilio. • Fecha y lugar de nacimiento. • Estado civil. • Sexo. • Edad. • Ocupación. • Régimen patrimonial (en caso de estar casado) 5.- Firma electrónica avanzada (e-firma).
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Coordinación de Innovación y Calidad
Funciones:	Llevar a cabo el trámite de la actualización de la Cédula de Operación Anual ante la Secretaría del Medio Ambiente y Recursos Naturales a nivel federal.
Obligaciones:	Cumplir con los requerimientos solicitados por diferentes organismos (STPS, SEMARNAT, CONNUE, etc.), con el objetivo de lograr que las actividades que se realizan en IEPSA se apeguen a las normas estipuladas para su operación.
Administrador del Sistema o documento	
Cargo :	Titular de la Coordinación de Innovación y Calidad
Funciones:	Integrar la información, documentación y estudios técnicos necesarios para realizar el trámite de actualización de la Cédula de Operación Anual ante la Secretaría del Medio Ambiente y Recursos Naturales a nivel federal.
Obligaciones:	Cumplir con los requerimientos solicitados por diferentes organismos (STPS, SEMARNAT, CONNUE, etc.), con el objetivo de lograr que las actividades que se realizan en IEPSA se apeguen a las normas estipuladas para su operación, así como resguardar los datos personales contenidos en dicho documento.
Usuarios del documento de sistema de datos	
Cargo :	Analista Técnico en el Coordinación de Innovación y Calidad.
Funciones:	Revisar información y compilar los documentos.
Obligaciones	Resguardar y archivar la información y documentación integrada de cada área, como soporte del trámite de actualización de la Cédula de Operación Anual ante la Secretaría del Medio Ambiente y Recursos Naturales a nivel federal.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Electrónico
Descripción:	[redacted]

Eliminado: 8 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	[redacted]
Características del lugar en donde se resguardan los soportes:	[redacted]
Portabilidad de datos:	NO
Transferencia de Datos	SI El trámite se realiza por medio de un proveedor externo para el trámite, carga y modificación de la información requerida en el sistema SINATEC de la Secretaría del Medio Ambiente y Recursos Naturales a nivel federal.
Encargado de Datos:	SI El instrumento normativo para la formalización de servicio es mediante la Orden de Servicio.

Denominación de la Unidad Administrativa: **XXIV.- Departamento de Asuntos Jurídicos**	
Nombre del sistema o inventario de Datos:	**XXIV.1.- Escrituras Públicas de Impresora y Encuadernadora Progreso, S.A. de C.V.**
Finalidad u objetivo del sistema o documento:	Acreditar la legal constitución y funcionamiento de la empresa, así como el actuar de las personas servidoras públicas que representan a IEPSA.
Fundamento Legal:	Función 4 y 15 de las funciones del Departamento de Asuntos Jurídicos establecidas en el Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V.
Datos personales contenidos en el sistema o documento:	Nombres Domicilio RFC Edad Datos contenidos en la credencial para votar: * Edad * Sexo * Domicilio * Clave de elector * CURP * Firma * Fecha de Nacimiento Aportaciones de los accionistas Nombre de accionistas Estado civil Ocupación Nacionalidad
Responsable del Sistema o documento que contiene Datos Personales	
Cargo :	Titular de la Jefatura del Departamento de Asuntos Jurídicos
Funciones:	Resguardo de escrituras públicas. Revisar el aspecto jurídico de los proyectos de convenios, contratos y demás actos consensuales que generen derechos y obligaciones a la entidad, así como formularlos o intervenir en ellos en caso de ser requerido.

Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura del Departamento de Asuntos Jurídicos
Funciones:	Resguardo de escrituras públicas. Revisar el aspecto jurídico de los proyectos de convenios, contratos y demás actos consensuales que generen derechos y obligaciones a la entidad, así como formularlos o intervenir en ellos en caso de ser requerido.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Usuarios del documento de sistema de datos	
Cargo :	Secretaria
Funciones:	Control y manejo de la información.
Obligaciones:	1. Resguardo de la documentación que contiene los datos personales. 2. No transferir los datos personales a personas no autorizadas. 3. Utilizar los datos personales únicamente para los fines que fueron recabados. 4. Guardar la confidencialidad de los datos personales.
Cargo :	Analista Especializado
Funciones:	Control y manejo de la información.
Obligaciones:	1. Resguardo de la documentación que contiene los datos personales. 2. No transferir los datos personales a personas no autorizadas. 3. Utilizar los datos personales únicamente para los fines que fueron recabados. 4. Guardar la confidencialidad de los datos personales.
Cargo :	Titular de la Gerencia Comercial
Funciones:	1. Solicita la documentación correspondiente a las escrituras de la Entidad con la finalidad de verificar y firmar los pedidos o contratos derivados de los procesos respectivos de obtener una licitación y/o generar una venta. 2. Autorizar el expediente que integra la documentación soporte para que IEPSA participe como proveedor, en las licitaciones públicas, concursos por invitación o procedimientos de cualquier organismo o institución pública o privada.
Obligaciones:	1. Resguardo de la documentación que contiene los datos personales. 2. No transferir los datos personales a personas no autorizadas. 3. Utilizar los datos personales únicamente para los fines que fueron recabados. 4. Guardar la confidencialidad de los datos personales.

Eliminado: 7 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Cargo :	Titular de la Coordinación de Innovación y Calidad
Funciones:	Solicita la documentación correspondiente a las escrituras de la Entidad con la finalidad realizar trámites respecto de licencias ambientales.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico.
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No.
Transferencia de Datos:	No.
Encargado de Datos: normativo con la que se formalizo la prestación de servicios:	No.

Denominación de la Unidad Administrativa: **XXIV.- Departamento de Asuntos Jurídicos**	
Nombre del sistema o inventario de Datos:	**XXIV.2.- Carpetas de estudios e informes/incobrables.**
Finalidad u objetivo del sistema o documento:	Resguardar la documentación legal que sirvió de base para generar un dictamen legal emitido por IEPSA.
Fundamento Legal:	1. Función 7, de las funciones del Departamento de Asuntos Jurídicos establecidas en el Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V. 2. Fracciones VI y VII del numeral Séptimo de las Normas y Bases para cancelar adeudos a cargo de terceros y a favor de Impresora y Encuadernadora Progreso, S.A. de C.V.
Datos personales contenidos en el sistema o documento:	1. Nombres 2. Domicilio 3. RFC 4. Edad 5. Datos contenidos en la credencial para votar: * Edad * Sexo * Domicilio * Clave de elector * CURP * Firma * Fecha de Nacimiento 6. Aportaciones de los accionistas 7. Nombre de accionistas 8. Estado civil 9. Ocupación

	10. Nacionalidad
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura del Departamento de Asuntos Jurídicos
Funciones:	Atender las resoluciones que pronuncien las autoridades jurisdiccionales o administrativas, solicitando el cumplimiento y prestando a las áreas de la entidad la asesoría necesaria para ello. El Área Jurídica procederá por sí o a través de un tercero, a revisar la debida integración del expediente respectivo y en su caso, a realizar las gestiones de cobro jurídicamente posibles, para tal efecto podrá solicitar a las unidades administrativas en el ámbito de sus competencias los documentos necesarios para realizar la exigencia del cobro judicialmente. Una vez que el Área Jurídica analizó la información contenida en el expediente y corroboró que se actualiza alguno de los supuestos de cancelación de una cuenta incobrables emitirá el dictamen correspondiente.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura del Departamento de Asuntos Jurídicos
Funciones:	Atender las resoluciones que pronuncien las autoridades jurisdiccionales o administrativas, solicitando el cumplimiento y prestando a las áreas de la entidad la asesoría necesaria para ello. El Área Jurídica procederá por sí o a través de un tercero, a revisar la debida integración del expediente respectivo y en su caso, a realizar las gestiones de cobro jurídicamente posibles, para tal efecto podrá solicitar a las unidades administrativas en el ámbito de sus competencias los documentos necesarios para realizar la exigencia del cobro judicialmente. Una vez que el Área Jurídica analizó la información contenida en el expediente y corroboró que se actualiza alguno de los supuestos de cancelación de una cuenta incobrables emitirá el dictamen correspondiente.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Usuarios del documento de sistema de datos	
Cargo:	Secretaria
Funciones:	Control y manejo de la información.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas.

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Cargo:	Analista Especializado
Funciones:	Control y manejo de la información.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico.
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No.
Transferencia de Datos:	Si, se realiza una transferencia al despacho jurídico externo contratado por la Entidad, por tal motivo, dicho despacho se compromete y firma para guardar la confidencialidad de la información que le es proporcionada y utilizarla para los fines establecidos en su contrato.
Encargado de Datos:	Sí, mientras se cuente con un despacho jurídico externo contratado.

Denominación de la Unidad Administrativa **XXIV.- Departamento de Asuntos Jurídicos**	
Nombre del sistema o inventario de Datos:	**XXIV.3.- Carpetas de juicios que tiene instaurados IEPSA.**
Finalidad u objetivo del sistema o documento:	Compilar y resguardar los expedientes de los juicios que se hayan instaurado por y en contra de IEPSA.
Fundamento Legal:	Función 7, de las funciones del Departamento de Asuntos Jurídicos establecidas en el Manual de Organización de Impresora y Encuadernadora Progreso, S.A. de C.V. Fracciones VI del numeral Séptimo de las Normas y Bases para cancelar adeudos a cargo de terceros y a favor de Impresora y Encuadernadora Progreso, S.A. de C.V.
Datos personales contenidos en el sistema o documento:	Nombres Domicilio RFC Edad Datos contenidos en la credencial para votar: * Edad * Sexo * Domicilio * Clave de elector * CURP * Firma * Fecha de Nacimiento Aportaciones de los accionistas Estado civil Ocupación Nacionalidad

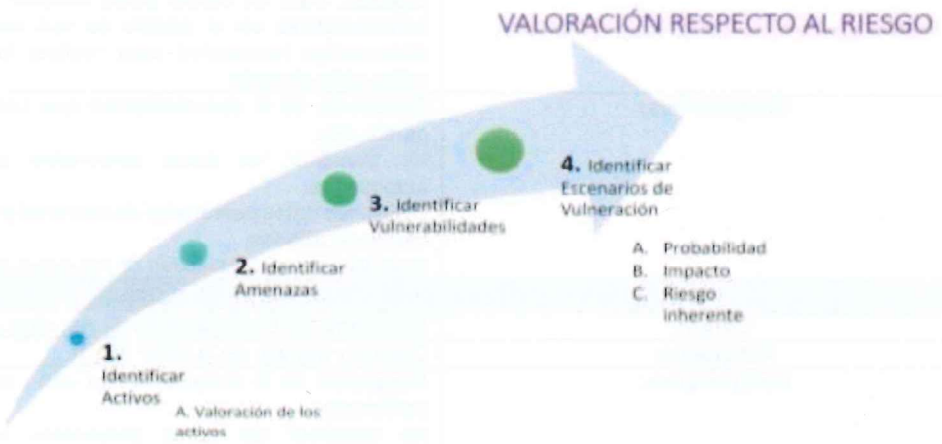
Responsable del Sistema o documento que contiene Datos Personales	
Cargo:	Titular de la Jefatura del Departamento de Asuntos Jurídicos
Funciones:	Atender las resoluciones que pronuncien las autoridades jurisdiccionales o administrativas, solicitando el cumplimiento y prestando a las áreas de la entidad la asesoría necesaria para ello. El Área Jurídica procederá por sí o a través de un tercero, a revisar la debida integración del expediente respectivo y en su caso, a realizar las gestiones de cobro jurídicamente posibles, para tal efecto podrá solicitar a las unidades administrativas en el ámbito de sus competencias los documentos necesarios para realizar la exigencia del cobro judicialmente.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Administrador del Sistema o documento	
Cargo:	Titular de la Jefatura del Departamento de Asuntos Jurídicos
Funciones:	Atender las resoluciones que pronuncien las autoridades jurisdiccionales o administrativas, solicitando el cumplimiento y prestando a las áreas de la entidad la asesoría necesaria para ello. El Área Jurídica procederá por sí o a través de un tercero, a revisar la debida integración del expediente respectivo y en su caso, a realizar las gestiones de cobro jurídicamente posibles, para tal efecto podrá solicitar a las unidades administrativas en el ámbito de sus competencias los documentos necesarios para realizar la exigencia del cobro judicialmente.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Usuarios del documento de sistema de datos	
Cargo:	Secretaria del Departamento de Asuntos Jurídicos
Funciones:	Control y manejo de la información.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados. Guardar la confidencialidad de los datos personales.
Cargo:	Secretaria A
Funciones:	Control y manejo de la información.
Obligaciones:	Resguardo de la documentación que contiene los datos personales. No transferir los datos personales a personas no autorizadas. Utilizar los datos personales únicamente para los fines que fueron recabados.

Eliminado: 6 renglones correspondientes a la descripción y lugar en donde se resguardan los soportes que contienen los datos personales.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	Guardar la confidencialidad de los datos personales.
Estructura y Descripción del sistema o documento	
Tipo de soporte:	Físico.
Descripción:	[redacted]
Características del lugar en donde se resguardan los soportes:	
Portabilidad de datos:	No.
Transferencia de Datos:	Si, se realiza una transferencia al despacho jurídico externo contratado por la Entidad, por tal motivo, dicho despacho se compromete y firma para guardar la confidencialidad de la información que le es proporcionada y utilizarla para los fines establecidos en su contrato.
Encargado de Datos:	Sí, siempre y cuando se cuente con un despacho jurídico externo contratado.

ANÁLISIS DE RIESGO

Para lleva a cabo el análisis de riesgo se tomó en consideración la identificación de los activos, las amenazas, las vulnerabilidades así como los escenarios de vulneración como se muestra en la siguiente imagen:



Resultado de lo reportado por las Unidades administrativas, se presenta la siguiente información respecto al análisis de riesgo de conformidad con lo establecido por la normatividad aplicable:

Eliminado: 29 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Denominación de la Unidad Administrativa:	**Unidad de Transparencia /Gerencia de Operación Administración y Finanzas**
Nombre del sistema o inventario de Datos:	**II.1 Plataforma Nacional de Transparencia,** Solicitudes de Acceso a la Información y de ejercicios de Derechos ARCO
Tipo de Soporte:	Físico y electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración. Baja: menor a 20% Media baja: de 20.01% a 39.99% Media: De 40.0% a 59.99% Media Alta: De 60.0% a 79.99% Alta: De 80.0% a más	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No
A) Consecuencias:	N/A
B) Acciones:	N/A
C) Potencial/probabilidad:	N/A
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
Consecuencias:	
Acciones:	
Potencial/probabilidad	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía.	N/A
Consecuencias:	N/A

Eliminado: 11 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Acciones:	N/A
Potencial/probabilidad	N/A

Denominación de la Unidad Administrativa :	**Gerencia de Operación, Administración y Finanzas**
Nombre del sistema o inventario de Datos:	**III.1 Sistema Contpaqi**
Tipo de Soporte:	Combinado (físico y electrónico)
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	N/A
Consecuencias:	
Acciones	
C) Potencial/probabilidad	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	N/A
Consecuencias:	
Acciones:	
Potencial/probabilidad	

Denominación de la Unidad Administrativa	**Departamento de Recursos Humanos**
Nombre del sistema o inventario de Datos	**IV.1 Expediente de Personal**
Tipo de Soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	

Eliminado: 16 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No aplica
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	No aplica
Consecuencias:	
Acciones:	
Potencial/probabilidad	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No aplica
Consecuencias:	
Acciones:	
Potencial/probabilidad	

Denominación de la Unidad Administrativa :	**Departamento de Recursos Humanos**
Nombre del sistema o inventario de Datos:	**IV-2 Software BioStar**
Tipo de Soporte:	Electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad:	

Eliminado: 15 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	[redacted]
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No aplica
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	No aplica
A) Consecuencias	
B) Acciones:	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía.	No aplica
Consecuencias:	
Acciones:	
Potencial/probabilidad	

Denominación de la Unidad Administrativa :	**Departamento de Recursos Humanos**
Nombre del sistema o inventario de Datos:	**IV.3 Software Fortia**
Tipo de Soporte:	Electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	No aplica
A) Consecuencias:	
B) Acciones:	

Eliminado: 33 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No aplica
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad	

Denominación de la Unidad Administrativa :	**Subgerencia de Adquisiciones y Contratación de Servicios**
Nombre del sistema o inventario de Datos:	**VI.1 Contratos**
Tipo de Soporte:	Físico y electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	NO APLICA
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
A) Consecuencias:	

Eliminado: 31 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

B) Acciones:	[redacted]
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	NO APLICA
Consecuencias:	
Acciones:	
Potencial/probabilidad:	

Denominación de la Unidad Administrativa:	**Subgerencia de Adquisiciones y Contratación de Servicios**
Nombre del Sistema o Inventario de Datos:	**VI.2 Sistema de Compras**
Tipo de soporte:	Electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración. Baja: menor a 20% Media baja: de 20.01% a 39.99% Media: De 40.0% a 59.99% Media Alta: De 60.0% a 79.99% Alta: De 80.0% a más	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	NO APLICA
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	NO APLICA

Eliminado: 16 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Consecuencias:	
Acciones:	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía, etc.	NO APLICA
Consecuencias:	
Acciones:	
C) Potencial/probabilidad:	

Denominación de la Unidad Administrativa:	**Departamento de Compras**
Nombre del sistema o inventario de Datos:	**VII.1 Pedidos**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	
A) Consecuencias::	
B) Acciones	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	NO APLICA
Consecuencias:	
Acciones:	

Eliminado: 16 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Potencial/probabilidad:	

Denominación de la Unidad Administrativa:	**Departamento de Compras**
Nombre del sistema o inventario de Datos:	**VII.2 Expedientes de Proveedor**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	NO APLICA
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
A) Consecuencias::	
B) Acciones	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	NO APLICA
Consecuencias:	
Acciones:	
Potencial/probabilidad:	

Denominación de la Unidad Administrativa:	**Departamento de Almacén e Inventarios**
Nombre del sistema o inventario de Datos:	**VIII.1 Reporte de entrada al almacén (compra)**
Tipo de soporte:	Combinado

Eliminado: 22 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica:	No hay
Consecuencias:	
Acciones:	
Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	No hay
A) Consecuencias:	
b) Acciones:	
Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No hay
Consecuencias:	
Acciones:	
Potencial/probabilidad:	

Denominación de la Unidad Administrativa:	**Departamento de Cobranza y Organización Documental**
Nombre del sistema o inventario de Datos:	**X.1 Sistema de Cuentas por Cobrar**
Tipo de soporte:	Electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental:	[redacted]

Eliminado: 25 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	[redacted]
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No
Consecuencias:	No aplica
Acciones	No aplica
Potencial/Probabilidad	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
A) Consecuencias:	
b) Acciones:	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No
Consecuencias:	No aplica
Acciones:	No aplica
Potencial/probabilidad:	No aplica

Denominación de la Unidad Administrativa:	**Gerencia Comercial**
Nombre del sistema o inventario de Datos:	**XII.1 Expediente Contratos**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	

Eliminado: 21 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	[redacted]
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No
Consecuencias:	No aplica
Acciones	No aplica
Potencial/Probabilidad	No aplica
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
A) Consecuencias:	
b) Acciones:	
c) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía, etc.	No
Consecuencias:	No aplica
Acciones:	No aplica
Potencial/probabilidad:	No aplica

Denominación de la Unidad Administrativa:	**Subgerencia Comercial**
Nombre del sistema o inventario de Datos:	**XIII.1 Seguimiento y atención a clientes**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No aplica
Consecuencias:	

Eliminado: 23 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Acciones	
Potencial/Probabilidad	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
Consecuencias:	
Acciones	
Potencial/Probabilidad	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No aplica.
Consecuencias:	No aplica.
Acciones:	No aplica.
Potencial/probabilidad:	No aplica.

Denominación de la Unidad Administrativa:	**Departamento de Cotizaciones**
Nombre del sistema o inventario de Datos:	**XIV.1. Elaboración de cotizaciones, órdenes de Trabajo y Carta de Aceptación**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No
Consecuencias:	No aplica
Acciones	No aplica
: Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
A) Consecuencias:	

Eliminado: 24 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

:B) Acciones:	[redacted]
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No
Consecuencias:	No aplica
Acciones:	No aplica
Potencial/probabilidad:	No aplica

Denominación de la Unidad Administrativa:	**Departamento de Facturación y Embarques**
Nombre del sistema o inventario de Datos:	**XV.1 Sistema de Facturación**
Tipo de soporte:	Físico y electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No
Consecuencias:	No aplica
Acciones:	No aplica
: Potencial/probabilidad	No aplica
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
A) Consecuencias	
B) Acciones	
:C) Potencial/probabilidad	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos,	No.

Eliminado: 22 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

organización, burocracia, corrupción, autonomía, etc.	

Denominación de la Unidad Administrativa:	**Coordinación de Líneas de Apoyo**
Nombre del sistema o inventario de Datos:	**XVIII.1 Expedientes de órdenes de trabajo**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	Terremotos e Incendio
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	[redacted]
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	NO
Consecuencias:	No aplica
Acciones:	No aplica
Potencial/probabilidad:	No aplica
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social, etc.	[redacted]
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política:	No.
Consecuencias:	No aplica.
Acciones:	No aplica.

Eliminado: 21 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

C) Potencial/probabilidad:	No aplica.

Denominación de la Unidad Administrativa:	**Departamento de Mantenimiento**
Nombre del sistema o inventario de Datos:	**XX.1 Cotizaciones de Proveedores Refacciones y/o Servicios**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	NO
A) Consecuencias	No aplica
Acciones:	No aplica
C) Potencial/probabilidad	No aplica
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social,	[redacted]
Acciones:	
Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política:	No
Consecuencias:	No aplica
Acciones:	No aplica
Potencial/probabilidad:	No aplica

Eliminado: 11 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Denominación de la Unidad Administrativa:	**Coordinación de Informática**
Nombre del sistema o inventario de Datos:	**XXI.1 Entradas y Salidas de Bienes Informáticos**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración. Baja: menor a 20% Media baja: de 20.01% a 39.99% Media: De 40.0% a 59.99% Media Alta: De 60.0% a 79.99% Alta: De 80.0% a más	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No aplica
Consecuencias:	
Acciones:	
Potencial/probabilidad:	
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería social,	No aplica
Consecuencias:	
Acciones:	
Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No aplica
Consecuencias:	
Acciones:	
C) Potencial/probabilidad:	

Denominación de la Unidad Administrativa:	**Departamento de Soporte Técnico**
Nombre del sistema o inventario de Datos:	**XXII.1 DVR/Videograbación**
Tipo de soporte:	Electrónico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	

Eliminado: 34 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No se tienen.
A) Consecuencias:	N/A
B) Acciones:	N/A
C) Potencial/probabilidad:	N/A
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería	[redacted]
A) Consecuencias:	
B) Acciones:	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	
Consecuencias:	
Acciones:	

Eliminado: 10 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

C) Potencial/probabilidad:	[redacted]

Denominación de la Unidad Administrativa:	**Coordinación de Innovación y Calidad**
Nombre del sistema o inventario de Datos:	**XXIII.1 Documentos de actualización de la Licencia Ambiental**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	N/A
A) Consecuencias	N/A
B) Acciones	N/A
C) Potencial/probabilidad:	N/A
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería	N/A
A) Consecuencias	N/A
B) Acciones	N/A
C) Potencial/probabilidad:	N/A
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	N/A
A) Consecuencias	N/A
B) Acciones	N/A
C) Potencial/probabilidad:	N/A

Denominación de la Unidad Administrativa:	**Coordinación de Innovación y Calidad**
Nombre del sistema o inventario de Datos:	**XXIII.2 Sistema COA web**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades:	

Eliminado: 15 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	N/A
A) Consecuencias	N/A
B) Acciones	N/A
C) Potencial/probabilidad	N/A
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería	N/A
Consecuencias:	N/A
Acciones:	N/A
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	N/A
Consecuencias:	
Acciones:	
Potencial/probabilidad:	

Denominación de la Unidad Administrativa:	**Departamento de Asuntos Jurídicos**
Nombre del sistema o inventario de Datos:	**XXIV.1 Escrituras Públicas de la Entidad**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	

Eliminado: 18 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No
A) Consecuencias	No aplica
B) Acciones	No aplica
C) Potencial/probabilidad:	No aplica
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería	[redacted]
A) Consecuencias	
B) Acciones	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No.
A) Consecuencias	N/A
B) Acciones	N/A
C) Potencial/probabilidad:	N/A

Denominación de la Unidad Administrativa:	**Departamento de Asuntos Jurídicos**
Nombre del sistema o inventario de Datos:	**XXIV.2 Carpetas de estudios e informes/incobrables**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No aplica
A) Consecuencias	N/A
B) Acciones	N/A
C) Potencial/probabilidad:	N/A

Eliminado: 27 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería	[redacted]
A) Consecuencias	
B) Acciones	
C) Potencial/probabilidad:	
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No.
A) Consecuencias	No aplica.
B) Acciones	No aplica.
C) Potencial/probabilidad:	No aplica.

Denominación de la Unidad Administrativa:	**Departamento de Asuntos Jurídicos**
Nombre del sistema o inventario de Datos:	**XXIV.3 Carpetas de Juicios de la Entidad**
Tipo de soporte:	Físico
Amenazas y vulnerabilidades: Considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
1.- Vulnerabilidad física o ambiental: Describir vulnerabilidades respecto a desastres naturales, ubicación, capacidad técnica, materiales.	[redacted]
A) Consecuencias: Describir las consecuencias o repercusiones en caso de continuar con la vulnerabilidad.	
B) Acciones: Describir las acciones que se están tomando para aminorar o erradicar la vulnerabilidad.	
C) Potencial/probabilidad: Establecer el grado de impacto si dicha vulnerabilidad ocurre y especificar la razón de su valoración.	
2.- Vulnerabilidad económica: Describir vulnerabilidades respecto a escasez y mal manejo de recursos.	No
A) Consecuencias	N/A
B) Acciones	N/A
C) Potencial/probabilidad:	N/A
3.- Vulnerabilidad social: Describir vulnerabilidades respecto a relaciones, comportamientos, métodos, conductas, ingeniería	[redacted]
A) Consecuencias	
B) Acciones	

Eliminado: 3 renglones correspondientes a información relativa al Análisis de Riesgo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

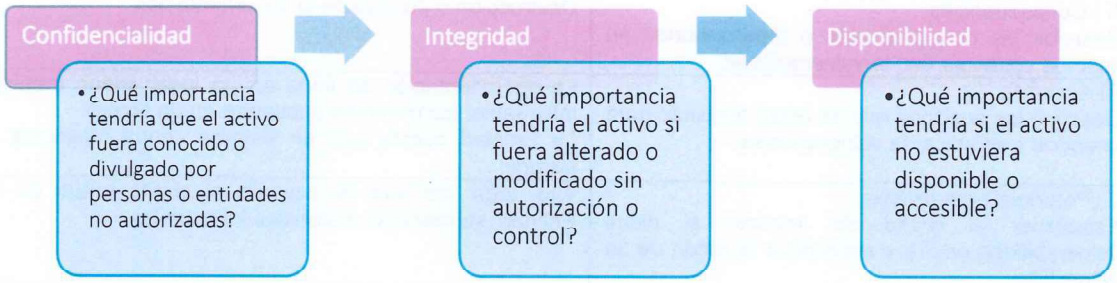
C) Potencial/probabilidad:	[redacted]
4.- Vulnerabilidad institucional o política: Describir vulnerabilidades respecto a procesos, organización, burocracia, corrupción, autonomía	No.
A) Consecuencias	No aplica.
B) Acciones	No aplica.
C) Potencial/probabilidad:	No aplica.

De conformidad con lo reportado por las Unidades Administrativas de la Entidad, y teniendo en cuenta las diferentes dimensiones de la seguridad, se realiza la siguiente tabla de valoración de los activos, asignándole un valor cuantitativo y cualitativo en una escala ***de 1 a 3, donde 1 es bajo, 2 es medio y 3 alto***, con base en el valor del activo en función de los tres principios fundamentales de la seguridad:

*Si la información tiene datos sensibles se colocara el mayor "3"

a) Confidencialidad (C)
b) Integridad (I)
c) Disponibilidad (D)

Tomando como base lo siguiente:



Valor Cualitativo	Valor Cuantitativo
Bajo	1-3
Medio	4-6

*metodología MAGERIT

Eliminado: Principios de seguridad y Valor del activo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

		Principios de la seguridad			Valor del activo	
No.	Nombre de activo	C	I	D	Valor total cuantitativo	Valor total cualitativo
1	II.1	[redacted]				
2	III.1					
3	IV.1					
4	IV.2					
5	IV.3					
6	VI.1					
7	VI.2					
8	VII.1					
9	VII.2					
10	VIII.1					
11	X.1					

12	XII.1	[redacted]
13	XIII.1	
14	XIV.1	
15	XV.1	
16	XVIII.1	
17	XX.1	
18	XXI.1	
19	XXII.1	
20	XXIII.1	
21	XXIII.2	
22	XXIV.1	
23	XXIV.2	

Eliminado: Principios de seguridad y Valor del activo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

24	XXIV.3	[redacted]

- * Para la obtención del valor total cuantitativo se sumaron los tres valores obtenidos de los principios y con ello se obtiene el valor cualitativo conforme a la tabla arriba citada.

ANÁLISIS DE BRECHA

Proceso de evaluación de las medidas de seguridad que ya existen contra las que sería conveniente tener, que resultan necesarias para la protección de Datos Personales.

Denominación de la Unidad Administrativa:	Unidad de Transparencia /Gerencia de Operación Administración y Finanzas
Nombre del sistema o inventario de Datos:	**II.1 Plataforma Nacional de Transparencia/ Solicitudes de Acceso a la Información y de ejercicios de Derechos ARCO**
Tipo de soporte	Físico y electrónico
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías.	[redacted]

Eliminado: 49 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Eliminado: Principios de seguridad y Valor del activo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Eliminado: 23 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.		
Denominación de la Unidad Administrativa:	Gerencia de Operación, Administración y Finanzas	
Nombre del sistema o inventario de Datos:	**III.1 CONTPAQI**	
Tipo de soporte:	Físico y electrónico	
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]	
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)		
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	No aplica	No aplica
Denominación de la Unidad Administrativa:	Departamento de Recursos Humanos	
Nombre del sistema o inventario de Datos:	**IV.1 Expediente de Personal**	
Tipo de soporte:	Físico	
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control a saber:	[redacted]	

Eliminado: 25 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos. .	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	No aplica
Denominación de la Unidad Administrativa:	Departamento de Recursos Humanos
Nombre del sistema o inventario de Datos:	**IV.2 Software Biostar**
Tipo de soporte	**Electrónico**
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos. .	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	

Eliminado: 25 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	No aplica	No aplica
Denominación de la Unidad Administrativa:	Departamento de Recursos Humanos	
Nombre del sistema o inventario de Datos:	**IV.3 Software Fortia**	
Tipo de soporte	**Físico y Electrónico**	
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos..	[redacted]	
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)		
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	No aplica	No aplica
Denominación de la Unidad Administrativa:	Subgerencia de Adquisiciones y Contratación de Servicios	
Nombre del sistema o inventario de Datos:	**VI.1 Contratos**	
Tipo de soporte	**Físico**	
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar.	[redacted]	

Eliminado: 24 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Denominación de la Unidad Administrativa:	Subgerencia de Adquisiciones y Contratación de Servicios
Nombre del sistema o inventario de Datos:	**VI.2 Sistema de Compras- IEPSA**
Tipo de soporte	**Electrónico y Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]

Eliminado: 38 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Denominación de la Unidad Administrativa:	Departamento de Compras
Nombre del sistema o inventario de Datos:	**VII.1 Pedidos, Órdenes de Maquila y Solicitudes de Servicio**
Tipo de soporte:	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías.	

Eliminado: 25 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Denominación de la Unidad Administrativa:	Departamento de Compras
Nombre del sistema o inventario de Datos:	**VII.2 Expediente de Proveedor**
Tipo de soporte	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]
Denominación de la Unidad Administrativa:	Departamento de Almacén e Inventarios
Nombre del sistema o inventario de Datos:	**VIII.1 Reporte de Entradas al Almacén**
Soporte	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos.	[redacted]

Eliminado: 37 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Denominación de la Unidad Administrativa:	Cobranza y Organización Documental
Nombre del sistema o inventario de Datos:	**X.1 Sistema de cuentas por cobrar**
Soporte:	**Electrónico**
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber:	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	

Eliminado: 41 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Denominación de la Unidad Administrativa:	Gerencia Comercial	
Nombre del sistema o inventario de Datos:	**XII.1 Expedientes de contratos**	
Tipo de soporte:	**Físico**	
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías) Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]	
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]	
Denominación de la Unidad Administrativa:	Subgerencia Comercial	
Nombre del sistema o inventario de Datos:	**XIII.1 Seguimiento y Atención a clientes**	
Tipo de soporte:	**Físico**	
Definir la forma y medidas de seguridad para el tratamiento de los riesgos. Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. Se debe especificar con qué medidas de seguridad se cuenta y que tipo de control es, a saber: Disuasivo. Cualquier medio físico de custodia. (Ej. Cámaras o policías)	[redacted]	

Eliminado: 64 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Preventivo. Anticipan la ocurrencia de fallas y reduce el impacto de una vulneración. Correctivo. Reduce el efecto de una vulneración de seguridad ocurrida. Detectivo. Descubren la causa de fallas o vulneraciones y disparan controles preventivos o correctivos.	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Denominación de la Unidad Administrativa:	Departamento de Cotizaciones
Nombre del sistema o inventario de Datos:	**XIV.1 Elaboración de cotizaciones órdenes de trabajo y carta aceptación**
Soporte:	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos	[redacted]
2) Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
1) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes.	

Eliminado: 60 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]
Denominación de la Unidad Administrativa:	Departamento de Facturación y Embarques
Nombre del sistema o inventario de Datos:	**XV.1 Sistema de Facturación**
Soporte:	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos.	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Denominación de la Unidad Administrativa:	Coordinación de líneas de Apoyo
Nombre del sistema o inventario de Datos:	**XVIII.1 Expedientes de Órdenes de trabajo**
Soporte:	**Físico**
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar. .	[redacted]

Eliminado: 66 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]
Denominación de la Unidad Administrativa:	Departamento de Mantenimiento
Nombre del sistema o inventario de Datos:	**XX.1 Cotizaciones de Proveedores de Refacciones**
Soporte:	**Físico**
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar.	[redacted]

Eliminado: 36 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]
Denominación de la Unidad Administrativa:	Coordinación de Informática
Nombre del sistema o inventario de Datos:	**XXI.1 Entradas y salidas de Bienes Informáticos**
Soporte:	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos	[redacted]
2) Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]

Eliminado: 76 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Denominación de la Unidad Administrativa:	Departamento de Soporte Técnico
Nombre del sistema o inventario de Datos:	**XXII.1 DVR/Videograbación**
Soporte:	**Electrónico**
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar.	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]

Eliminado: 43 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	[redacted]
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]
Denominación de la Unidad Administrativa:	Coordinación de Innovación y Calidad
Nombre del sistema o inventario de Datos:	**XXIII.1 Expediente para actualizar Licencia Ambiental**
Soporte:	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos	[redacted]
2) Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]

Eliminado: 49 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Denominación de la Unidad Administrativa:	Coordinación de Innovación y Calidad
Nombre del sistema o inventario de Datos:	**XXIII.2 Expediente para actualizar la Cédula de Operación Anual/Sistema COA Web**
Soporte:	**Físico**
Definir la forma y medidas de seguridad para el tratamiento de los riesgos	[redacted]
2) Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	
Denominación de la Unidad Administrativa:	Departamento de Asuntos Jurídicos
Nombre del sistema o inventario de Datos:	**XXIV.1 Escrituras Públicas de Impresora y Encuadernadora Progreso, S.A. de C.V.**
Soporte:	**Físico**
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar.	[redacted]
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar.	

Eliminado: 57 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.	[redacted]
Denominación de la Unidad Administrativa:	Departamento de Asuntos Jurídicos
Nombre del sistema o inventario de Datos:	**XXIV.2 Carpetas de estudios dictámenes e informes/incobrables.**
Soporte	**Físico**
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar.	[redacted]
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)	[redacted]
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías.	[redacted]

Eliminado: 35 renglones correspondientes a información relativa al Análisis de Brecha.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.		
Denominación de la Unidad Administrativa:	Departamento de Asuntos Jurídicos	
Nombre del sistema o inventario de Datos:	**XXIV.3 Carpetas de Juicios de la Entidad.**	
Soporte	**Físico**	
Definir las opciones para el tratamiento del riesgo, mitigar, eliminar, transferir o aceptar.	[redacted]	
Identificar las medidas de seguridad actualmente implementadas. a) Funcionamiento actual b) Nivel de madurez (en caso de que se estén implementando)		
3) Seleccionar las medidas de seguridad faltantes. a) Reforzar las medidas de seguridad existentes. b) Definir nuevas medidas de seguridad. c) Usar mejores prácticas estándares, guías. Dichas medidas pueden reemplazar los controles de seguridad implementados actualmente.		

Tabla de Grado de Probabilidad

La probabilidad es la posibilidad de que el riesgo se materialice en un periodo de tiempo; por lo que se establece una escala cuantitativa y cualitativa considerando los escenarios previstos, y los registros, bitácoras o datos históricos conforme a la siguiente tabla:

BAJA 1
- Si ha ocurrido 1 antecedente registrado en un periodo de 5 años o y/o que, por el entorno, la posibilidad de que suceda sea mínima.

MEDIA 2
- Si se han registrado 2 antecedentes en un periodo anual y/o esporádicamente en un intervalo de 3 años.

ALTA 3
- Si han ocurrido más de dos eventos al término de un año, o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda

Derivado de lo anterior y según lo reportado por las Unidades Administrativas el Grado de Probabilidad de los inventarios de ***datos reportados es baja 1.***

Valoración del Riesgo Inherente Impacto

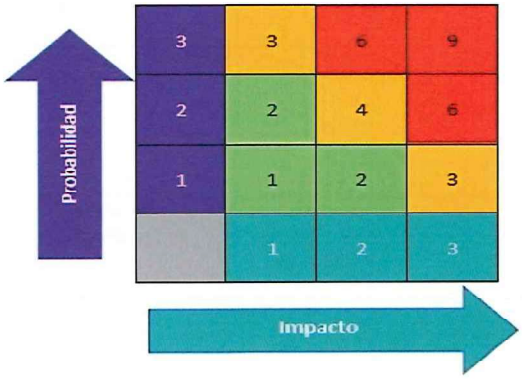
Impacto en los titulares Análisis de Impacto en los Titulares, este valore se obtuvo de **multiplicar la probabilidad por el impacto** con ello se obtendrá el riesgo inherente tomando como base la siguiente matriz de riesgo:

El nivel de riesgo también debe ser representado en una escala cuantitativa y cualitativa, en este caso una escala de 3 niveles, en orden creciente y su equivalencia cuantitativa (1, 2 y 3) respectivamente, **donde 1 será riesgo bajo; 2, medio y 3, alto.**

1-2 =BAJO

3-5 =MEDIO

6-9= ALTO



No.	Nombre de activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente
1	II.1	[redacted]			
	II.1				

Eliminado: Amenazas, Probabilidad, Impacto y Riesgo Inherente.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Eliminado: Amenazas, Probabilidad, Impacto y Riesgo Inherente.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

		[redacted]
2	III.1	
	III.1	
3	IV.1	
4	IV.2	
5	IV.3	
	IV.3	
6	VI.1	
7	VI.2	

Eliminado: Amenazas, Probabilidad, Impacto y Riesgo Inherente.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

		[redacted]
8	VII.1	
9	VII.2	
10	VIII.1	
11	X.1	
12	XII.1	
13	XIII.1	

Eliminado: Amenazas, Probabilidad, Impacto y Riesgo Inherente.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

		[redacted]
14	XIV.1	[redacted]
15	XV.1	[redacted]
16	XVIII.1	[redacted]
17	XX.1	[redacted]

Eliminado: Amenazas, Probabilidad, Impacto y Riesgo Inherente.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

		[redacted]
18	XXI.1	
19	XXII.1	
20	XXIII.1	
21	XXIII.2	
22	XXIV.1	

Eliminado: Amenazas, Probabilidad, Impacto y Riesgo Inherente.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

		[redacted]
23	XXIV.2	[redacted]
24	XXIV.3	[redacted]

PLAN DE TRABAJO

De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de

acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, derivado de lo anterior se presenta el Plan de Trabajo emitido por las diversas Unidades Administrativas de la Entidad toma en consideración el análisis de riesgo y brecha:

Plan de Trabajo						
Gerencia de Operación Administración y Finanzas /Titular de la Unidad de Transparencia.						
Sistema o Inventario de Datos:	**Medida de seguridad a implementar**	**Responsable**	**Descripción**	**Fecha de inicio**	**Fecha final**	**Evidencia Entregable**
[redacted]						
Subgerencia de Adquisiciones y Contratación de Servicios						
[redacted]						
Departamento de Compras						
[redacted]						
Departamento de Compras						
[redacted]						

Eliminado: Plan de trabajo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Eliminado: Plan de trabajo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

[redacted]

Gerencia Comercial

[redacted]

Subgerencia Comercial /Atención Institucional

[redacted]

Departamento de Cotizaciones

[redacted]

Eliminado: Plan de trabajo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Departamento de Facturación y Embarques

[redacted]

Coordinación de Informática

[redacted]

Departamento de Soporte Técnico

[redacted]

Eliminado: Plan de trabajo.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Coordinación de Innovación y Calidad
[redacted]
Departamento de Asuntos Jurídicos
[redacted]
Departamento de Asuntos Jurídicos
[redacted]
Departamento de Asuntos Jurídicos
[redacted]

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

La implementación de medidas de seguridad es un proceso que se debe hacer paulatina y secuencialmente, a fin de elegir controles útiles para mitigar el riesgo, optimizar tiempo y dinero y reforzar la seguridad de los datos personales cada vez más, por lo anterior en cumplimiento a lo establecido en siguientes artículos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados:

Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

(…)

VIII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, (…)

Artículo 35. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

(…)

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, (…)

Artículo 30. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de

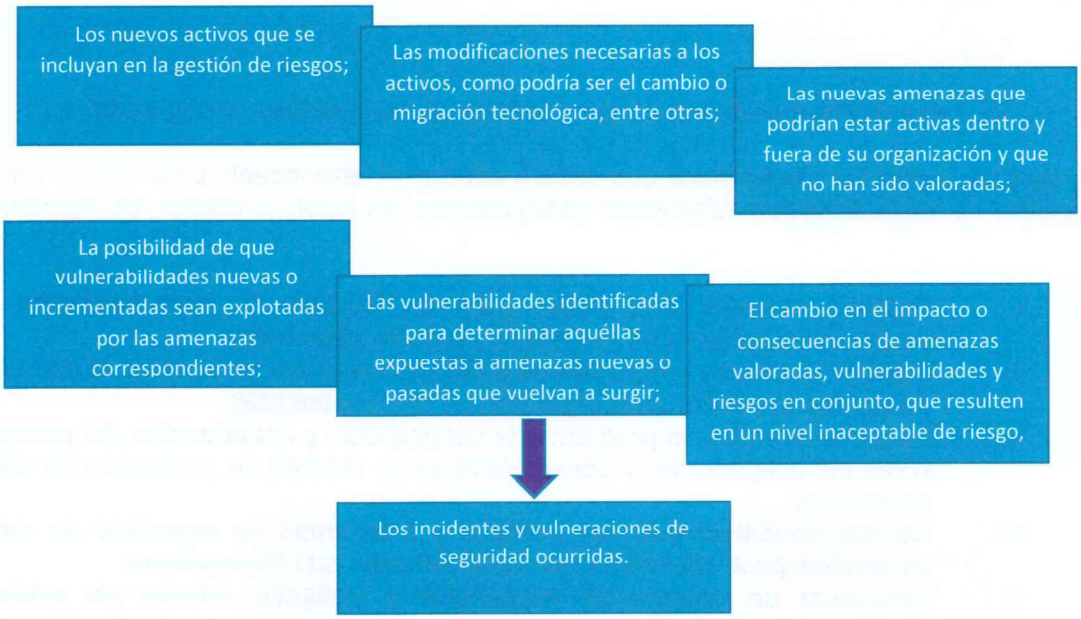
conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

Art. 63 de los Lineamentos Generales para la Protección de Datos Personales para el Sector Público.

Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:



De conformidad con lo establecido en la metodología MAGERIT se presenta la siguiente escala de madurez de las medidas de seguridad y las medidas a implementar:

factor	nivel	significado
0%	**L0**	inexistente

	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

En este apartado se detallan las acciones para el mantenimiento de las medidas de seguridad contempladas en la LGPDPPSO, así como a las obtenidas del resultado del cuestionario que realizó la Unidad de Transparencia a las Unidades Administrativas de la Entidad, en las cuales de manera general y con la finalidad de mantener un monitoreo y revisión se llevarán a cabo de manera permanente.

Medida de Seguridad	Tipo de Medida	Nivel	Significado	Observaciones	seguimiento
[redacted]					

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

[redacted]

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

[redacted]

* En el Anexo 1 se presentan las respuestas del cuestionario que se emitió a las Unidades Administrativas.

Finalmente se presentan de manera general las acciones y medidas de seguridad que se llevarán a cabo:

1- Se deberá informar al Comité de Transparencia los avances, al Plan de Trabajo junto con la evidencia correspondiente de manera semestral.
2- Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.
3- Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, ello se realizara a través del cuestionario que emitirá la Unidad de Transparencia para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo ello se verificara en reuniones semestrales que se llevaran a cabo a través del Comité de Transparencia
4- Vulneraciones a la seguridad de los datos personales. En caso de identificar un incidente de seguridad que involucre datos personales, la unidad administrativa, en su caso el área de Informática y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente
5- Actualización tecnológica. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.
6- Se implementara un acuerdo de confidencialidad que se dará a conocer a las Unidades Administrativas de la Entidad que intervienen en el manejo de datos personales y que no cuentan con este documento. (Anexo 2)

7- Se realizara un Registro de Incidentes o de vulneraciones(Anexo 3)
8- Respaldo o en su caso escaneo de la documentación.

Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:

a) personal de vigilancia en los accesos a la empresa.
b) control de acceso del personal.
c) control de asistencia a través de huella digital
d) circuito cerrado de cámaras de vigilancia.

Se presenta el cuestionario que se implementará cada semestre a las unidades administrativas para el monitoreo de las medidas de seguridad, el cual podrá modificarse de conformidad a los cambios o necesidades de las áreas o sistemas.

CUESTIONARIOS PARA LAS UNIDADES ADMINISTRATIVAS

De las siguientes medidas de seguridad administrativas, físicas y técnicas deberá colocar SI o NO de acuerdo a lo solicitado en cada pregunta, para el caso de las respuestas que se señalen "SI", especificar de qué manera es implementada en el caso de "NO" deberán describir la acción a implementar.

Medidas de Seguridad Administrativas

	Denominación de la Unidad Administrativa:				
	Sistema o Inventario de Datos:				
	Nivel de protección que requieren lo datos personales: *ver los tipos de niveles.				
		SI	NO	Medida de seguridad a implementar	Observaciones
1	**Declaración de confidencialidad**: Se cuenta con alguna declaración de confidencialidad que se pone a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.				
2	**Listado de personal**: Se cuenta con un documento que contenga la relación del personal que interviene en el tratamiento de datos personales, en donde se incluya nombre, cargo, funciones en el tratamiento y obligaciones en materia de datos personales, por cada tratamiento.				
3	**Clasificación de los archivos físicos**: Se identifican y clasifican los documentos conforme a lo				

	establecido en el Catálogo de Disposición Documental.				
4	**Clasificación de los archivos electrónicos:** Se cuenta con un procedimiento para la baja de documentos electrónicos que contienen datos personales.				
5	**Capacitación:** El personal involucrado en el tratamiento de los datos personales asiste a cursos de capacitación implementados por el Comité de Transparencia en el Programa Anual de Capacitación.				
6	**Bitácora de vulneraciones:** Se cuenta con un documento y control informativo en donde se reporten los tipos de vulneraciones. (Registro de incidentes).				
7	**Depuración y borrado seguro del archivo físico:** Se transfieren y depurar los archivos físicos de manera periódica, conforme a los plazos de conservación y parámetros dispuestos en la normativa en materia.				
8	**Depuración y borrado seguro del archivo electrónico:** Se borra de manera segura y permanente, las bases de datos o parte de ellas que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación.				
9	**Bitácora de consulta**: Se cuenta con una bitácora como control para registrar el nombre, cargo, fecha y hora de consulta de la base de datos que contienen datos personales.				
10	Se cuenta con algún responsable de seguridad: para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.				

11	**Transferencias:** Se realizan transferencias con las medidas de confidencialidad necesarias, se envía la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.				
12	**Transmisión de datos personales**: El remitente registra la o las transmisiones que realiza.				
13	Se revisa y, en su caso, actualizan los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales.				
14	Se dan a conocer los avisos de privacidad a los titulares de los datos personales en el momento que corresponde.				

Medidas de Seguridad Fisicas

	Denominación de la Unidad Administrativa:				
	Sistema o Inventario de Datos:				
	Nivel de protección que requieren lo datos personales: *ver los tipos de niveles				
		SI	**NO**	**Medida de seguridad a implementar**	**Observaciones**
1	Cuidado de los bienes informáticos: Se verifica que se mantenga en buen estado los bienes informáticos.				
2	Prevenir accesos no autorizados: Se cuenta con una base de datos o registros del personal que accede a los sistemas o bases de datos				

	por cada unidad administrativa.				
3	No instalar equipos ajenos: Se cuenta con un procedimiento para la instalación de equipos de cómputo que no sean propiedad de la Entidad. Los usuarios que requieran hacer uso de la red interna utilizan solamente las direcciones IP asignadas por la Unidad Administrativa correspondiente.				
4	En caso de requerir conectar un dispositivo de almacenamiento de información (p. ej. USB, disco duro portátil, etcétera) al equipo del usuario, se verifica que previamente se aplique el antivirus.				
5	Archivero con candado: Se resguardan las bases de datos en archivo físico en un archivero con candado o con llave de seguridad.				
6	Candados de seguridad para equipos de cómputo: Se cuenta con candados de seguridad en los equipos de cómputo.				
7	Zona de confidencialidad: Se cuenta con una zona de confidencialidad en donde se resguardan los archivos físicos o equipos de cómputo que contengan las bases de datos, cuya finalidad sea limitar el acceso al personal no autorizado, equipos o aparatos de copiado.				
8	Se cuenta con personal de vigilancia en los accesos a la empresa.				
9	Se cuenta con cámaras de seguridad de circuito cerrado dentro de la Entidad.				
10	Cuando se integran nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizan actualización del análisis de				

	riesgo, análisis de brecha y plan de trabajo.				
11	Se implementan medidas de seguridad para asegurar el acceso a los espacios donde se almacenan los soportes físicos o electrónicos que tienen datos personales.				

Medidas de Seguridad Técnicas

	Denominación de la Unidad Administrativa:				
	Sistema o Inventario de Datos:				
	Nivel de protección que requieren lo datos personales: *ver los tipos de niveles				
		SI	**NO**	**Medida de seguridad a implementar**	**Observaciones**
1	Cuidado de la contraseña personal: Se cuenta con un listado del personal que maneja contraseñas, se le comunica que debe abstenerse de compartir contraseñas personales de la red institucional, las contraseñas, tokens, identificadores o cualquier mecanismo utilizado para la autenticación en un recurso informático.				
2	Actualización de contraseñas: En caso de olvido o sospecha de divulgación de una contraseña o mecanismo de autenticación, se cambian las contraseñas a efecto de evitar robo de identidad.				
3	Se reportan las fallas: al área correspondiente cualquier fallo, error, sospecha, violación a la				

	seguridad de la información.				
4	Se tiene con accesos restringíos para la instalación de softwares: descargas en el equipo de cómputo institucional software y aplicaciones de lugares no seguros o dudosa procedencia.				
5	Respaldo de información: Se realizan respaldos de la información que residen en el equipo de cómputo asignado con ayuda de Informática considerando las necesidades propias del área.				
6	Se cuenta con un sistema operativo de red instalada en los equipos.				
7	En caso de que la respuesta sea afirmativa, proporciona dicho sistema operativo un manejo riguroso de perfiles de usuarios y contraseñas.				

PROGRAMA GENERAL DE CAPACITACIÓN.

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la Ley General señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

Artículo 64. Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

Derivado de lo anterior la Unidad de Transparencia remite cada año oficio a los titulares de las Unidades Administrativas la Cedula de Detección de Necesidades de Capacitación en materia de Transparencia, Acceso a la Información, Protección de datos personales y temas relacionados, con la finalidad de que señalen los temas de su interés así como del personal a su cargo, para que posteriormente se realice el **Programa de Capacitación debidamente integrado al INAI, mismo que se tomara en consideración para dar**

cumplimiento a este apartado y se publicara en la sección correspondiente de Transparencia de la página web de la Entidad.

No obstante, lo anterior se tiene contemplado el siguiente tomar en consideración para el programa de capacitación los siguientes temas, para todo el personal de mando y personal operativo que maneje datos personales, con la finalidad de que todo el personal de mando cuente con el curso de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y posteriormente se quiere capacitar al personal operativo en temas especializados en materia de Datos Personales:

	Nivel	Temática
Capacitación básica	**Inicial**	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Capacitación especializada	**Intermedio**	*Tratamiento de Datos Biométricos y Manejo de Incidentes de Seguridad de Datos Personales *Sistema de Gestión de Seguridad de Datos Personales Sector Público
	Avanzado	Temas especializados en materia de protección de Datos Personales y gestión y administración de archivos electrónicos en el sector púbico Auditorías voluntarias

Actualización del documento de seguridad.

El artículo 36 de la Ley General establece la obligación de la actualización del 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.

En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citado, para, en su caso, actualizar el presente documento de seguridad.

Elaboró:

Lcda. Nancy García Márquez
Titular de la Jefatura del Departamento de Asuntos Jurídicos y Servidor Público
Habilitado en la Unidad de Transparencia

Aprobó:

Integrantes del Comité de Transparencia

Mtra. Laura Jessica Cortazar Morán
Titular del Área de Especialidad en Control Interno en el Ramo Educación Pública y Suplente de la Titular del Órgano Especializado en Control Interno en la Secretaría de la Función Pública

L.C. Noemí Gámez Hernández
Titular de la Jefatura del Departamento de Cobranza y Organización Documental y Coordinadora de Archivos

C.P. María del Socorro Laguna Brindis
Titular de la Gerencia de Operación Administración y Finanzas y Titular de la Unidad de Transparencia

1.- Aprobado en la Segunda Sesión Ordinaria del Comité de Transparencia de fecha 14 de febrero de 2023.
2.- Actualización aprobada en la Séptima Sesión Ordinaria del Comité de Transparencia, de fecha 16 de julio de 2024.

Fecha de elaboración	Fecha de la última Actualización
01/02/2023	16/07/2024

(Hoja de firmas del Documento de Seguridad en Materia de Protección de Datos Personales de Impresora y Encuadernadora Progreso, S.A. de C.V.)

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

ANEXOS

1

Resultado del cuestionario por Unidad Administrativa de las medidas a implementar

U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
SUBGERENCIA COMERCIAL XII.1 Seguimiento y Atención a clientes	[redacted]		
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
SUBGERENCIA COMERCIAL XV.1 Facturación	[redacted]		
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Gerencia Comercial	[redacted]	N/A	N/A

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

	[redacted]		
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Departamento de Cotizaciones	[redacted]	N/A	N/A
Compras/Pedidos Órdenes De Maquila	[redacted]		N/A
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Compras/Expediente de Proveedor	[redacted]		N/A
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimo tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Subgerencia de Adquisiciones Sistema de Compras	[redacted]		N/A
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Subgerencia de Adquisiciones Contratos	[redacted]		N/A
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Gerencia de Operación Administración y Finanzas/Unidad de Transparencia	[redacted]	N/A	N/A
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Departamento de Asuntos Jurídicos Escrituras Públicas	[redacted]	N/A	N/A
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Departamento de Asuntos Jurídicos Escrituras Públicas	[redacted]	N/A	N/A
U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
DEPARTAMENTO DE SOPORTE	[redacted]	N/A	N/A

TECNICO/ VIDEOGRABACION	[redacted]		

[redacted]

U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Departamento de Mantenimiento	[redacted]	N/A	N/A

U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Departamento de Mantenimiento	[redacted]	N/A	N/A

U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
DEPARTAMENTO DE ALMACEN E INVENTARIOS	[redacted]	N/A	N/A

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

Eliminado: Medidas de seguridad.
Fundamento: Artículo 113, fracciones I y V de la Ley General de Transparencia y Acceso a la Información Pública, 110 fracción I y V de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el primer párrafo del numeral Décimo Octavo y Vigésimotercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para las versiones públicas.
Motivo: Por tratarse de información que puede poner en riesgo la seguridad pública, así como la seguridad de las personas.

U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Coordinación de Innovación y Calidad COA	[redacted]	[redacted]	[redacted]

U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
Coordinación de Innovación y Calidad LAU	[redacted]	N/A	N/A

U.A.	MEDIDA ADMINISTRATIVA	MEDIDA FISICAS	MEDIDAS TECNICAS
	[redacted]	N/A	N/A

ANEXO 2

ACUERDO DE CONFIDENCIALIDAD

Por medio de la presente manifiesto que: Yo: _____,
Área de Adscripción _____,
Cargo: _____,

Derivado del ejercicio de mis funciones, de conformidad en los artículos 6 y 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, me ocupare en proteger los datos personales que se me confieran dentro de Impresora y Encuadernadora Progreso, S.A. de C.V. ; actuaré con reserva y discreción.

Por lo anterior me comprometo a: Mantener reserva y confidencialidad de dicha información, sin divulgarla ni proporcionarla a terceras personas en forma verbal; escrita; por medios electrónicos, magnéticos, o por cualquier otro; directa o indirectamente; por el contrario, me obligo a conservarla y no divulgarla.

No usar la información directa o indirectamente en beneficio propio o de terceros, mucho menos revelar el contenido de los datos personales que los titulares suscriben dentro de IEPSA.

En caso de incumplimiento de lo señalado en el artículo 49 de la Ley General de Responsabilidades Administrativas; así como del artículo 12 del Código de Ética de la Administración Pública Federal (D.O.F., 08 de febrero de 2022), la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás normatividad aplicable en la materia, me someto a las sanciones que establezca la autoridad competente.

Dejo expreso constancia que este Compromiso de Confidencialidad lo he suscrito a los _____ días de _____ del año 20___

Firma _____

ANEXO 3

REGISTRO DE INCIDENTES

Fecha:
Aprobado por:

Tipo de incidencia: _____
_____

El momento en que se produjo fecha lugar y hora:
_____
_____

Nombre y cargo de quién notifica la incidencia: _____
_____

Nombre y cargo de quién recibe la notificación:_____

Las acciones que se implementan a consecuencia de la incidencia:
_____
_____

Soportes físicos: (oficios, expedientes, archiveros, ficheros, computadoras, discos duros robados o dañados).
Soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos tanto dañados como recuperados.

Quién autorizó la recuperación de dato._____