IEQROO
INSTITUTO ELECTORAL DE QUINTANA ROO

2003 IEQR 2023
Democracia para todas y todos

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DEL INSTITUTO ELECTORAL DE QUINTANA ROO

María Beatriz Robles Martínez

Eriberto Gabriel Coot Chay

GUÍA DE CONTENIDO

DATOS DE ELABORACIÓN

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES
FECHA DE ELABORACIÓN 15 de agosto 2023
ÁREA ENCARGADA DE LA ELABORACIÓN DEL DOCUMENTO Unidad de Transparencia y Archivo Electoral
APROBACIÓN DEL DOCUMENTO Comité de Transparencia

I. INTRODUCCIÓN

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la ley.

El artículo 34 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO) establece las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados.

Entendiendo por sistema de gestión es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en (LGPDPPSO) y las demás disposiciones que le resulten aplicables en la materia.

De ahí que el presente Documento de Seguridad tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior del Instituto Electoral de Quintana Roo por las diversas unidades administrativas que conforman su estructura orgánica, para mantener vigente y promover la mejora continua en la protección de los mismos, en términos de lo previsto en los artículos 35 y 36 de la LGPDPPSO, además de desarrollar buenas prácticas en la materia.

II. MARCO JURÍDICO

Constitución Política de los Estados Unidos Mexicanos. (CPEUM).

Ley General de Transparencia y Acceso a la Información Pública. (LGTAIP).

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (LGPDPPSO).

Ley de Instituciones y Procedimientos Electorales para el estado de Quintana Roo. (LIPEQROO)

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el estado de Quintana Roo.

Ley de Transparencia y Acceso a la Información Pública para el estado de Quintana Roo.

Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. ÁMBITO DE APLICACIÓN

El presente documento de seguridad constituye el instrumento que describe y da cuenta sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Instituto Electoral de Quintana Roo (IEQROO) para garantizar el cumplimiento de los principios y deberes establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Asimismo, dicho documento será de observancia obligatoria para todos los servidores electorales que intervienen en el tratamiento de datos personales que se encuentren en posesión de este Instituto, así como para toda aquella persona física o moral, pública o privada, que debido a la prestación de un servicio tenga acceso a los datos personales de conformidad con lo establecido en la LGPDPPSO.

En este sentido, la Unidad de Transparencia y Archivo integra el presente documento de seguridad con base en la información generada por las citadas unidades administrativas acorde al ámbito de sus funciones y, de conformidad con las disposiciones aplicables.

IV. INVENTARIO DE DATOS PERSONALES EN LAS ÁREAS DEL INSTITUTO ELECTORAL DE QUINTANA ROO

El tratamiento de los datos personales que lleva a cabo el IEQROO a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismos, se realiza estableciendo políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Transparencia y Acceso a la Información Pública.

En este sentido el IEQROO inició su proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman el instituto, se involucran el tratamiento de datos personales.

Para esto, dispuso de un formato denominado Identificación de datos personales y tratamiento que permitió que las diversas unidades que integran el IEQROO informaran los nombres de las personas funcionarias que tratan datos personales (nombre y función), así como la identificación de datos personales (identificativos, patrimoniales y/o sensibles), considerando los elementos mínimos que establece el artículo 33, fracción II de la Ley General y el diverso 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Posterior a esto se llevó a cabo el levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

Lo anterior para considerar el ciclo de vida de los datos personales, para que los servidores públicos que intervienen en el tratamiento sepan que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que tiene relevancia en el proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior del IEQROO.

ÁREAS QUE CONFORMAN AL INSTITUTO ELELCTORAL DE QUINTANA ROO

1. Presidencia, consejeros y consejeras electorales
2. Secretaria Ejecutiva
3. Dirección de Administración
4. Dirección Jurídica
5. Dirección de Organización
6. Dirección de partidos políticos
7. Dirección de capacitación electoral
8. Unidad técnica de comunicación social
9. Unidad técnica de informática y estadística
10. Unidad técnica de transparencia y archivo Electoral

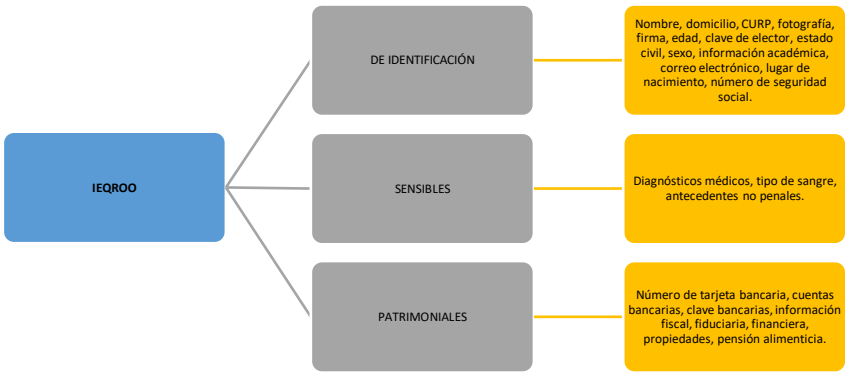
De las diez áreas que conforman el IEQROO **7** de ellas reportan **26** inventarios reportados de la siguiente forma:

En este sentido, fue posible identificar que, en el ejercicio de sus atribuciones, 26 procesos en cuyo cauce se actualiza algún tratamiento de datos personales, por lo que, mediante un ejercicio de sistematización, se pudo deducir que dichas actividades pueden ser categorizadas en los siguientes rubros:

TRATAMIENTOS DENTRO DE LAS UNIDADES ADMINISTRATIVAS DEL IEQROO EN LOS QUE SE TRATAN DATOS PERSONALES

- Atención a solicitudes de información.
- Atención a Usuarios en biblioteca.
- Coordinar los procedimientos para designación de las y los consejeros y vocales de los consejos municipales del IEQROO.
- Coordinar los procedimientos para designación de las y los consejeros y vocales de los consejos distritales del IEQROO.
- Proceso de selección de candidaturas independientes.
- Registro de candidaturas.
- Denuncias en materia de responsabilidades administrativas.
- Afiliaciones del ISSSTE.
- Expedientes de personal permanente.
- Contratos de servicio profesional del IEQROO.
- Adjudicación directa.
- Licitación pública nacional.
- Etapa de entrevistas de concurso público del SPEN.
- Promover la educación cívica para la construcción de la ciudadanía del estado de Quintana Roo.
- Difundir la cultura política democrática.
- Acciones en materia de grupos en situación de vulnerabilidad.
- Acciones para el empoderamiento de la mujer.
- Constitución y registro de partidos políticos estatales.
- Declaraciones patrimoniales.
- Procedimientos sancionadores.
- Nóminas.
- Estados de cuenta bancarios.
- Comprobante electrónico de pago.
- Invitación a cuando menos tres proveedores.
- Padrón de proveedores y contratistas.
- Expedientes de personal eventua

De igual forma con la aplicación de inventarios se pudo observar que los datos personales que se manejan en las áreas de IEQROO corresponden a las siguientes categorías:



Tal y como se muestra, la dirección de Administración posee el mayor número de tratamientos, dada la naturaleza de sus funciones, toda vez que entre las áreas que la integran se encuentran aquellas con atribuciones para administrar los recursos humanos, materiales y financieros del

Instituto Electoral de Quintana Roo, por lo que las áreas de atención, oportunidad y verificación en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades de esta unidad administrativa.

El Inventario de Datos Personales del Instituto Electoral de Quintana Roo, constituye un elemento del Sistema de Gestión de Datos Personales, que junto con las medidas de seguridad representa un instrumento de evidencia para la implementación de las directrices de la política en materia de protección de datos personales. Asimismo, traza las rutas para una capacitación focalizada en materia protección de datos en aras de fortalecer la estructura de los operadores en cada uno de los procesos en que se tratan datos, buscando con ello sensibilizar y preparar a los responsables y encargados de los mismos para que su tratamiento se lleve a cabo de conformidad con los estándares en la materia.

V. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVENGAN EN EL TRATAMIENTO DATOS PERSONALES

Todos los servidores electorales que tengan acceso a los datos personales, están obligados a conocer y aplicar las medidas de seguridad propias que sean de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, o en su caso, se deberá de garantizar la confidencialidad, integridad y disponibilidad. Funciones genéricas en cualquier nivel de tratamiento:

- Tener a la vista el Aviso de Privacidad.
- Tratar los datos personales con responsabilidad y las medidas de seguridad que se haya establecido para tal fin.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.
- Estar capacitado en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.
- Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
- Recabar los datos personales para la finalidad para la cual estos fueron solicitados según el trámite o el sistema de tratamiento que corresponda.

El incumplimiento a lo establecido en este Documento de Seguridad, así como lo establecido por la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Quintana Roo, será causa de aplicación de medidas de apremio y/o sanción de acuerdo a lo dispuesto en el artículo 171 de del mismo ordenamiento.

Una vez que se contó con la integración de los inventarios de datos, se llevó a cabo la elaboración del análisis de riesgo y brecha, atendiendo a lo previsto en el artículo 33, fracción IV y V de la Ley General de la materia, las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de dichos datos.

VI. ANÁLISIS DE RIESGO

El análisis de riesgo, además de ayudar a visualizar las medidas de seguridad administrativas, de gestión, soporte y revisión de la seguridad de la información; físicas, como lo son las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados.

Para analizar los riegos de los datos personales que son objeto de tratamiento, se elaboró un instrumento que, a partir de considerar su objeto y atribuciones constitucionales, clasifica los datos en tres tipos:

1. **De identificación o contacto**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.

2. **Patrimoniales**, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

3. **Sensibles**, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por

ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Para la determinación del riesgo sobre esa tipología de datos personales se valora la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con una diversidad de activos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza). Para facilitar el análisis, se establecieron cuatro tipos de amenazas:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

En general se tiene que el Instituto Electoral de Quintana Roo cuenta con **7** unidades administrativas, en las que se da tratamiento de datos personales mediante **27** procesos como se visualiza a continuación:

INSTITUTO ELECTORAL DE QUINTANA ROO RIESGOS DE PROCESOS POR UNIDAD ADMINISTRATIVA	
Atención a solicitudes de información.	1
Atención a usuarios en biblioteca.	1
Coordinar los procedimientos para la designación de las y los consejeros y vocales de los consejos municipales del Instituto Electoral de Quintana Roo.	2
Coordinar los procedimientos para la designación de las y los consejeros y vocales de los consejos distritales.	2
Difundir la Cultura Política y Democrática.	1
Acciones en materia de Grupos en Situación de Vulnerabilidad.	1.25
Acciones para el Empoderamiento y Liderazgo de la Mujer.	1
Promover la Educación Cívica para la Construcción de la Ciudadanía del estado de Quintana Roo.	1
Proceso de selección de candidaturas independientes.	2
Constitución y registro de partidos políticos estatales.	1
Registro de candidaturas.	2
Declaraciones patrimoniales.	3
Denuncias en materia de Responsabilidades.	2
Procedimientos sancionadores.	2
Nominas.	1.25
Afiliaciones del ISSSTE.	1
Expedientes de personal eventual.	1.25
Expedientes de personal permanente.	1.25
Estados de cuenta bancarios.	1
Contratos de servicio profesional del Instituto.	1.25
Comprobante electrónico de pago.	2
Adjudicación directa.	2
Invitación a cuando menos 3 proveedores.	2

INSTITUTO ELECTORAL DE QUINTANA ROO RIESGOS DE PROCESOS POR UNIDAD ADMINISTRATIVA	
Litación pública nacional.	2
Padrón de proveedores y contratistas.	1
Etapa de entrevistas del concurso público del SPEN.	1.15
Almacenamiento de datos en el servidor del IEQROO.	2

VI. ANÁLISIS DE BRECHA

Una vez identificados los posibles riesgos a los que este Instituto se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las medidas de seguridad reportadas por las diversas unidades administrativas, las cuales consisten en lo siguiente:

● Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.

● El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.

● Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.

● Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.

● Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.

● Una vez recabados los datos personales, ya realizada la carpeta o expediente electrónico, o físico, y guarda está en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.

● Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora.

● Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.

Ahora bien, a efecto de evitar la vulneración de los datos personales en posesión de este Instituto, se considera que además de las medidas existentes, se puede reforzar la seguridad de la información con la adopción de las siguientes prácticas:

1. **Control de acceso a la información,** consistente en mantener un control sobre las personas que recaban, administran, usas, almacenan o difunden datos personales.

Dicho control puede realizarse a través de una bitácora en la que se señale el nombre y cargo del servidor público responsable, el proceso de tratamiento de datos personales que realiza, así como las medidas de seguridad que adopta a efecto de resguardar la información.

2. **Activos del responsable**, la cual se refiere a la asignación de responsabilidades y a la clasificación de la información.

En ese sentido, se propone que las áreas realicen un estudio pormenorizado acerca de los procesos que se vinculen con tratamiento de información confidencial, los tramos de responsabilidad de cada encargado de la información y se documenten mediante una bitácora.

3. **Seguridad física**, en este apartado se sugiere tener archiveros en buen estado y con seguridad para el resguardo de la información

En cuanto hace a la información que se resguarda de manera electrónica, se recomienda la actualización de los sistemas y el mantenimiento de los equipos.

4. **Incidentes de seguridad de información**.

En relación con este punto y derivado del diagnóstico realizado, no se ha presentado ninguna eventualidad en la cual se hayan vulnerados los datos personales que trata el IEQROO, no obstante, se recomienda generar programas de capacitación respecto a las acciones a realizar ante una posible incidencia y de los mecanismos de mitigación del daño.

VIII. PLAN DE TRABAJO Y MEDIDAS DE SEGURIDAD

La existencia del documento de seguridad, busca enmarcar los deberes del IEQROO para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que el IEQROO realizará para la aplicación del presente documento de seguridad.

Lo anterior se realizará en base a las atribuciones establecidas en el la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Quintana Roo.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

1. Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.

2. Se comunicará a los enlaces sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.

3. Se buscará la participación del IDAIPQROO para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad:

1. Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.

2. Actualizar las medidas de Seguridad conforme al Sistema de Protección de

Datos Personales hecho para el IEQROO.

3. Actualizar el presente plan de trabajo.

4. Se emitirá un programa anual de capacitaciones y además se promoverá que el personal del IEQROO se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

IX. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúan siendo efectivas e idóneas para el IEQROO. Realizaremos el siguiente cuadro, donde se concentran los mecanismos de monitoreo y el objetivo de cada uno de ellos:

MECANISMOS DE MONITOREO	OBJETIVO DEL MONITOREO
• Visitas a 4 áreas cada 12 meses, de las cuales serán elegidas de forma aleatoria. • Solicitar reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	• Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas. • Monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

X. PROGRAMA GENERAL DE CAPACITACIÓN

Se manejarán las capacitaciones de conformidad con las necesidades del sujeto obligado en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado.

Las fechas exactas se les notificarán a los enlaces de Transparencia con al menos una semana de anticipación a las fechas estimadas con la intención de que éstos las difundan con los interesados en asistir a las capacitaciones.