CORTV
CORPORACIÓN OAXAQUEÑA DE RADIO Y TELEVISIÓN

DOCUMENTO DE SEGURIDAD 2024-2025

PRESENTACION:

El presente documento trata de aclarar ciertos puntos con la finalidad de que la Corporación Oaxaqueña de Radio y Televisión sea más clara y así permitir a la ciudadanía en general conocer el actuar y tratamiento de la información tratándose de datos personales.

La definición básica de datos personales dice que es la información concerniente a una persona física, con la cual puede ser identificada o identificable. Dentro de estos existe una categoría que se denomina "datos personales sensibles", los cuales requieren especial protección, ya que refieren a información cuya utilización indebida puede afectar a una persona; estos datos pueden ser información genética, el estado de salud presente y futuro, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, origen racial o étnico y preferencia sexual de dicha persona.

La protección de esta información está regulada por la Constitución Política de los Estados Unidos Mexicanos, en su artículo 16 segundo párrafo que a la letra dice: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

Es por el motivo antes mencionado y en apego al 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y el 27 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca, que la Corporación Oaxaqueña de Radio y Televisión, como Sujeto Obligado presenta este Documento de Seguridad.

CONTENIDO

1. **Inventario de datos personales y de los sistemas de tratamiento.**
2. **Funciones y obligaciones de las personas que tratan los datos personales.**
3. **Ciclo de vida de los datos personales.**
4. **Análisis de riesgos.**
5. **Análisis de brecha.**
6. **Plan de trabajo.**
7. **Mecanismos de monitoreo y revisión de las medidas de seguridad.**
8. **Programa de general de capacitación.**

1. INVENTARIO DE LOS DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

FORMAS DE OBTENCIÓN DE LOS DATOS PERSONALES.

ÁREA	MEDIO DE RECOLECCIÓN
Dirección General	• Formatos físicos • Formatos electrónicos
Peritos y Unidad de Transparencia	• Formatos físicos • Formatos electrónicos
Departamento Administrativo	• Formatos físicos • Carpetas electrónicas
Departamento de Informática	• Formatos físicos • Formatos electrónicos
Dirección de Noticias	• Formatos físicos • Formatos electrónicos

Dirección de Radio	• Formatos físicos • Formatos electrónicos
Dirección de Televisión	• Formatos físicos • Carpetas electrónicas

FINALIDADES DE CADA TRATAMIENTO DE DATOS PERSONALES.

ÁREA	FINALIDADES DEL TRATAMIENTO
Dirección General	• Recabar datos de las y los participantes de las diferentes actividades que realiza la Corporación a través de internet. • Recabar datos de las y los asistentes a las reuniones de trabajo con el Titular de la Corporación. • Recabar información de los acuerdos tomados de las sesiones del equipo de trabajo que conforma la Corporación.
Unidad de Transparencia	• Referencias para respuestas a solicitudes de información.
Dirección de Administración y Finanzas	• Integración del expediente personal. • Generación de contratos y nombramientos. • Administrar asistencia y puntualidad del personal que labora en la Dirección. • Administrar nómina y prestaciones. • Registro y alta ante el Instituto Mexicano del Seguro Social. • Elaboración de contratos y comprobantes fiscales por concepto de pagos a proveedores y servicios contratados.
Dirección de Noticias	• Datos Personales de invitados a los noticieros.
Dirección de Radio	• Datos Personales de invitados a los programas de radio.
Dirección de Televisión	• Datos Personales de invitados a los programas de televisión.

TIPOS DE DATOS PERSONALES QUE SE TRATAN Y SI SON SENSIBLES.

ÁREA	TIPOS DE DATOS PERSONALES	SENSIBLES
Dirección General	• Nombre • Correo electrónico • Número de Teléfono.	• NO
Unidad de Transparencia	• Nombre • Correo electrónico • Número de Teléfono.	• NO
Dirección de Administración y Finanzas	• Nombre • Estado civil • Registro Federal de Contribuyentes (RFC) • Clave Única de Registro de Población (CURP) • Lugar de nacimiento • Fecha de nacimiento • Nacionalidad • Domicilio • Teléfono particular • Teléfono celular • Correo electrónico • Firma autógrafa • Edad • Fotografía • Referencias personales • Estatura • Peso • Tipo de sangre • Puesto o cargo que desempeña • Domicilio de trabajo • Correo electrónico institucional • Teléfono institucional • Referencias laborales	• PARCIAL
Dirección de Noticias	• Nombre • Correo electrónico • Número de Teléfono.	• NO

Dirección de Radio	• Nombre • Correo electrónico • Número de Teléfono.	• NO
Dirección de Televisión	• Nombre • Correo electrónico • Número de Teléfono.	• NO

NUEVAS MEDIDAS DE SEGURIDAD.

ÁREA	MEDIDAS DE SEGURIDAD A IMPLEMENTAR	TIPO DE MEDIDA DE SEGURIDAD
Dirección General	Tener bajo llave la información en formato físico y guardar los archivos digitales bajo contraseña.	• Física y digital
Unidad de Transparencia	Tener bajo llave la información en formato físico y guardar los archivos digitales bajo contraseña.	• Física y digital
Dirección de Administración y Finanzas	Tener bajo llave la información en formato físico y guardar los archivos digitales bajo contraseña.	• Física y digital
Dirección de Noticias	Tener bajo llave la información en formato físico y guardar los archivos digitales bajo contraseña.	• Física y digital
Dirección de Radio	Tener bajo llave la información en formato físico y guardar los archivos digitales bajo contraseña.	• Física y digital
Dirección de Televisión	Tener bajo llave la información en formato físico y guardar los archivos digitales bajo contraseña.	• Física y digital

2.-FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN LOS DATOS PERSONALES.

Cada una de las áreas que se encarga de resguardar y generar información, cuenta con encargados de información, quienes a su vez clasifican dicha información como datos generales, datos personales, y datos personales sensibles, apegándose a el artículo 3 fracción X de la Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados, a continuación se presenta la lista de los encargados de cada área:

ÁREA	NOMBRE DEL ENCARGADO	FUNCION
Dirección General	Ing. David García Luis	Encargado de catalogar y solicitar la clasificación de la información perteneciente a la Dirección.

Unidad de Transparencia	Lic. Carlos Felgueres Salazar	Vínculo entre las áreas y el Comité de Transparencia, solicita y acredita la clasificación de la información pública perteneciente a las direcciones de la CORTV.
Dirección de Administración y Finanzas	Lic. Olivia Santaella Pinelo	Encargada de catalogar y solicitar la clasificación de la información perteneciente a su Dirección.
Dirección de Noticias	Lic. Maribel Mendoza Ramírez	Encargada de catalogar y solicitar la clasificación de la información perteneciente a su Dirección.
Dirección de Radio	Lic. Gabriel Reyes Vásquez	Encargada de catalogar y solicitar la clasificación de la información perteneciente a su Dirección.
Dirección de Televisión	Lic. Diana Isis Molina Domínguez	Encargada de catalogar y solicitar la clasificación de la información perteneciente a su Dirección.

3.- CICLO DE VIDA DE LOS DATOS PERSONALES

Las actividades consideradas dentro del ciclo de vida de los datos personales son:

Obtención: La obtención de datos personales comprende todas las tareas en donde los datos personales son creados de manera directa por fuentes autorizadas o en forma indirecta a través de transferencias o generados mediante procedimientos de deducción.

Almacenamiento: Es el proceso por medio del cual se guardan los datos personales en forma electrónica, impresa o cualquier otro medio.

Uso: El uso de los datos personales implica el acceso, manejo y procesamiento para el propósito que fueron creados.

Divulgación: La divulgación consiste en las remisiones y transferencias de los datos personales hacia otras instancias que requieren y tienen autorización para el tratamiento de los datos personales.

Bloqueo: El bloqueo se realiza cuando los datos personales ya no son de utilidad, pero por alguna disposición regulatoria interna o externa deben retenerse.

Cancelación: La cancelación o destrucción de los datos personales implica la eliminación de la información cuando deja de ser útil para el propósito que fue creada.

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal o cualquier otro recurso humano o material que resulte pertinente considerar.

Para esto, la Corporación cuenta con el Catálogo de Disposición Documental, por sus siglas CADIDO, el cual fue aprobado por el Archivo General del Estado de Oaxaca quienes, revisaron, evaluaron y aprobaron las disposiciones de las cuales la CORTV se dio a la tarea de solicitar a cada una de sus direcciones solicitando la información con la temporalidad útil de los archivos que poseen, misma que se detalla en dicho Catalogo, al cual puede acceder mediante el siguiente link: https://drive.google.com/file/d/1Vl4VeV37puuOJOYGHfxGOES9an2Vy6aO/view?usp=sharing

4.- ANÁLISIS DE RIESGO

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

Esta metodología en particular, contempla tres factores que en conjunto determinan el riesgo latente de los datos personales:

- **Beneficio**, factor que deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.
- **Accesibilidad**, factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.
- **Anonimidad**, factor que determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos.

Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles.

En este sentido, tanto la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 33, fracción IV como la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca en su artículo 26, fracción IV, establecen que se debe contar con un análisis de riesgos de datos personales para identificar peligros y estimar los riesgos considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento como pueden ser, de manera enunciativa mas no limitativa: hardware, software, personal del responsable, entre otros.

El responsable de esta actividad deberá considerar los requerimientos regulatorios, códigos de conducta de la CORTV o mejores prácticas de un sector específico, el valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida, el valor y exposición de los activos involucrados en el tratamiento de los datos personales y las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

Los beneficios de contar con un análisis de riesgos son grandes y algunos de ellos son: soporte a decisiones estratégicas, apoyo en la definición y asignación efectiva de recursos, justificar

esfuerzos en tiempo, recurso humano y financieros, promover la mejora continua y transmitir confianza a empleados.

Para determinar las medidas de seguridad a implementar se analizaron los siguientes puntos:

- **Beneficio para el atacante:** Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados. (Beneficio económico por venderlos o usarlos).
- **Accesibilidad para el atacante**: Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados. (Miles de personas pueden acceder a la vez una base de datos a través de un sitio web).
- **Anonimidad del atacante**: Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados. (Internet es un medio más anónimo que presentarse físicamente a las instalaciones de la Institución).

Por lo cual la Corporación Oaxaqueña de Radio y Televisión, cuenta con la siguiente tabla:

ÁREA	NUMERO DE TITULARES
Dirección General	5
Unidad de Transparencia	2
Dirección de Administración y Finanzas	21
Dirección de Noticias	24
Dirección de Radio	5
Dirección de Televisión	14
TOTAL	71

IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS DATOS PERSONALES

- **Datos con riesgo inherente bajo:** Se considera información general concerniente a una persona física identificada o identificable, como: datos de identificación, información académica o laboral.
- **Datos con riesgo inherente medio:** Se contemplan datos que permitan conocer la ubicación física de la persona, como: dirección física, información relativa al tránsito de las personas dentro y fuera del país, así como, número de dependientes, beneficiarios, familiares, referencias laborales y referencias personales.

- **Datos con riesgo inherente alto**: Se contemplan los datos personales sensibles, aquellos 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.
- **Datos con riesgo inherente reforzado**: Son aquellos como: información adicional de tarjeta bancaria (número de tarjeta de crédito y/o débito combinado con cualquier otro contenido de la misma como fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (NIP).

IDENTIFICACIÓN DE TIPO DE DATOS Y DE NIVEL DE RIESGO INHERENTE

TIPO DE DATO	NIVEL DE RIESGO INHERENTE
Ubicación en conjunto con patrimoniales	REFORZADO
Información adicional de tarjeta bancaria	REFORZADO
Titulares de alto riesgo	REFORZADO
Salud	ALTO
Origen, creencias e ideológicos	ALTO
Ubicación	MEDIO
Patrimoniales	MEDIO
Autenticación	MEDIO
Jurídicos	MEDIO
Tarjeta bancaria	MEDIO
Personales de identificación	BAJO

Considerando lo anterior, el número de titulares es de 71 de los cuales no recabamos datos sensibles que pudieran afectar a la esfera más íntima de una persona o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave, el nivel de riesgo inherente de los datos personales tratados por las distintas áreas que los recaban es:

NIVEL DE RIESGO INHERENTE MEDIO

5.- ANÁLISIS DE BRECHA

En cumplimiento al artículo 33 fracción V de la Ley General, que establece realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.
El análisis de brecha consiste en determinar la diferencia entre las medidas de seguridad existentes y las que faltan para reducir el riesgo hasta un nivel por abajo del establecido por la organización como nivel aceptable.

ÁREA	NUMERO DE TITULARES
Dirección General	La información se encuentra resguardada por un responsable, quien además de contar con su propia oficina con llave, cuenta con una cámara de vigilancia.

Unidad de Transparencia	La información se encuentra resguardada por un responsable quien cuenta con archiveros y un cajón con llave.
Dirección de Administración y Finanzas	La información se encuentra resguardada por un responsable, quien registra entrada y salida de documentación con una bitácora de quien y con que razón solicita dicha información, además cuenta con archiveros y un cajón con llave.
Dirección de Noticias	La información se encuentra resguardada por un responsable quien cuenta con archiveros y un cajón con llave.
Dirección de Radio	La información se encuentra resguardada por un responsable quien cuenta con archiveros y un cajón con llave.
Dirección de Televisión	La información se encuentra resguardada por un responsable quien cuenta con archiveros y un cajón con llave.

MEDIDAS DE SEGURIDAD A IMPLEMENTAR

MEDIDAS DE SEGURIDAD A IMPLEMENTAR	TIPO DE MEDIDA
Roles y responsabilidades: Identificar y definir los roles y responsabilidades de las personas que tienen acceso a los datos personales, qué perfil y con qué nivel de privilegio según sus facultades.	Administrativa
Seguridad en la transferencia o remisión: En caso de contar con la figura de encargado, contar con el documento que avale la transferencia y que contenga una cláusula de confidencialidad de la información.	Administrativa
Inventario de activos: Identificar los activos y mantener actualizado el inventario de los mismos.	Física
Controles de seguridad: Cada activo deberá contar con llave y un administrador que garantice la seguridad de la información.	Física
Registro en bitácora de los solicitantes de la información.	Física
Sensibilización y capacitación: Fomentar la cultura de la seguridad de la información, para ello, todos los servidores públicos de la Dirección deberán recibir capacitación de	Administrativa

manera periódica respecto al tratamiento que realicen de los datos personales.	
Eliminación de los derechos de acceso: Los derechos de acceso de los servidores públicos responsables y encargados a las instalaciones o al tratamiento de la información, deben ser removidos en cuanto termine la relación laboral o de servicios, o en caso de realizar ajustes a las funciones del servidor público o encargado.	Administrativa
Establecer contraseñas: Implementar contraseñas para toda la información que se tiene resguardada en equipos de cómputo y medios de almacenamiento electrónico.	Técnica
Eliminación de forma segura de información: Establecer mecanismos para eliminar de manera segura información tanto en equipos de cómputo como elementos físicos, tomando precauciones con los procedimientos de reutilización.	Física

6.- PLAN DE TRABAJO

El plan de trabajo es parte medular del documento de seguridad y es donde se detallan las acciones tomadas para implementar las medidas de seguridad.

En cumplimiento a lo establecido en el artículo 33 fracción VI de la Ley General, ayudados del análisis de riesgos y el análisis de brecha, se seleccionaron las medidas de seguridad aplicables a la protección de datos personales. La implementación de cada uno de los mecanismos de seguridad se realizará de acuerdo al siguiente plan de trabajo:

MEDIDAS DE SEGURIDAD	PERIODO
Roles y responsabilidades.	Al iniciar actividades de personal
Inventario de activos.	Trimestralmente
Controles de seguridad.	Diario.
Registro en bitácora.	Diario.
Sensibilización y capacitación.	Trimestralmente
Eliminación de los derechos de acceso.	Con cambio de Personal
Establecer contraseñas.	Al iniciar actividades de personal
Eliminación de forma segura de información.	Al finalizar actividades de personal

7.- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

En términos de lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 33 fracción VII, el responsable deberá 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.

Con base en el Plan de Trabajo planteado se evaluarán de manera semestral en los meses de julio y diciembre, tanto las medidas administrativas, físicas y técnicas, así también se trabajará con los responsables de las unidades administrativas para revisar la efectividad de las medidas de seguridad implementadas, informando los avances en las sesiones del Comité de Transparencia.

8.- PROGRAMA GENERAL DE CAPACITACIÓN

La mejor medida de seguridad contra posibles vulneraciones es contar con servidores públicos conscientes de sus deberes respecto a la protección de datos personales, que identifiquen sus atribuciones, facultades y funciones para su adecuado tratamiento.

Los Lineamientos Generales de Protección de Datos Personales establecen que 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.

El presente Programa se sustenta en los temas y acciones de capacitación del Departamento de Formación y Capacitación, dependiente de la Dirección de Comunicación, Capacitación, Evaluación, Archivo y Datos Personales del Órgano Garante de Acceso a la Información Pública, Transparencia, Protección de Datos Personales y Buen Gobierno del Estado de Oaxaca para el ejercicio 2024, el cual se puede consultar mediante el siguiente link:
https://ogaipoaxaca.org.mx/site/descargas/PROGRAMA_GENERAL_ANUAL_DE_FORMACION_Y_CAPACITACION.pdf

De igual manera, para el ejercicio 2025, la Propuesta para capacitación es la siguiente:

Temas para Capacitación 2025	Primer trimestre	Segundo trimestre	Tercer trimestre	Cuarto trimestre
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.	X			X
Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como Para la Elaboración de Versiones Públicas.		X	X	
Medidas de Seguridad y Documento de Seguridad	X			