Documento De Seguridad

Unidad de Transparencia

H. Ayuntamiento Constitucional de Manzanillo, Colima

Introducción:

En cumplimiento de las obligaciones de seguridad, el [Fecha de aprobación] el Comité de Transparencia del H. Ayuntamiento de Manzanillo aprobó la actualización al Documento de Seguridad, conforme al artículo 38 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima (LPDPPSOEC). Este documento comprende los siguientes apartados y anexos:

Para el municipio de Manzanillo, Colima, así como para su Unidad de Transparencia, la información representa un activo fundamental que debe ser protegido mediante un conjunto de procesos y sistemas administrados, ejecutados y preservados por la propia unidad de transparencia, así como por las distintas áreas del gobierno y los organismos públicos descentralizados que los generan. En todo momento se debe asegurar la confidencialidad de la información, buscando mejorar continuamente los procesos y sistemas relacionados con la reserva, integridad y disponibilidad de la información, mientras se mitigan los riesgos asociados con su tratamiento.

Este Documento de Seguridad para Sistemas de Datos Personales, en formatos físicos y electrónicos, se elabora en cumplimiento de las disposiciones jurídicas vigentes con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de la información personal que contienen dichos sistemas.

El documento pretende ser una herramienta que brinde homogeneidad en la organización, procesos y sistemas a la Unidad de Transparencia, donde el Comité de Transparencia, en colaboración con las áreas del sujeto obligado y sus organismos públicos descentralizados, establecen las medidas de seguridad física a implementarse para proteger los sistemas de datos personales custodiados.
Asimismo, este documento tiene como propósito asegurar el control de los sistemas de datos personales en posesión de la unidad, especificando el tipo de datos personales que almacenan, los responsables, encargados y usuarios de cada sistema, así como las medidas de seguridad concretas implementadas.

Objetivo:

El propósito primordial de este Documento de Seguridad es establecer un marco integral para la protección de los datos personales administrados por el H. Ayuntamiento de Manzanillo y su Unidad de Transparencia. Este marco tiene como objetivo principal salvaguardar la integridad, confidencialidad y disponibilidad de la información personal almacenada en sistemas físicos y electrónicos.

En virtud de las obligaciones legales y éticas del ayuntamiento y su unidad de transparencia, este documento busca proporcionar una guía detallada y coherente para la gestión de la seguridad de la información. Su finalidad es promover una cultura de seguridad sólida dentro de la organización, donde todos los empleados, responsables y usuarios comprendan la importancia de proteger la privacidad y los derechos de las personas cuyos datos son procesados.
Entre los objetivos específicos que este documento persigue, se incluyen:
Definir y documentar claramente las políticas, procedimientos y controles de seguridad necesarios para proteger los datos personales bajo la custodia del ayuntamiento y su unidad de transparencia.

Establecer roles y responsabilidades claros para la implementación, mantenimiento y supervisión de las medidas de seguridad contempladas en este documento.
Proporcionar orientación y capacitación adecuadas a todo el personal involucrado en el manejo de datos personales, con el fin de fomentar buenas prácticas de seguridad y conciencia sobre los riesgos asociados con el tratamiento de la información.
Garantizar el cumplimiento continuo de las leyes y regulaciones aplicables en materia de protección de datos personales, en particular la LPDPPSOEC, así como cualquier otro marco normativo relevante.
Establecer mecanismos efectivos de monitoreo, evaluación y mejora continua de las medidas de seguridad implementadas, con el fin de adaptarse a los cambios en el entorno operativo y a las nuevas amenazas y vulnerabilidades que puedan surgir.
este Documento de Seguridad tiene como objetivo fundamental asegurar que los datos personales manejados por el H. Ayuntamiento de Manzanillo y su Unidad de Transparencia sean tratados de manera responsable y segura, en cumplimiento con los más altos estándares de protección de la privacidad y la seguridad de la información.

I Inventario de Datos Personales y de Sistemas de Tratamiento

El Artículo 38 fracción I de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición del inventario de datos personales y de los sistemas de tratamiento de datos personales

1. Datos Personales Custodiados

El H. Ayuntamiento de Manzanillo y su Unidad de Transparencia gestionan una variedad de datos personales, los cuales se detallan a continuación:

I) *Datos de Identificación:* Incluyen nombres, apellidos, números de identificación oficial (como el CURP o la credencial de elector), fechas de nacimiento, género, estado civil, entre otros.

II) *Datos de Contacto:* Direcciones físicas, direcciones de correo electrónico, números de teléfono, entre otros

III) *Datos Laborales:* Información relacionada con el empleo, como cargos, salarios, historiales laborales, entre otros.

IV) *Datos Sensibles:* Se incluyen aquellos datos que requieren un tratamiento especial, como información sobre la salud, orientación sexual, creencias religiosas, entre otros.

2. Sistemas de Tratamiento de Datos Personales

A continuación, se presenta un listado de los sistemas y aplicaciones utilizados para el tratamiento de datos personales dentro del H. Ayuntamiento de Manzanillo y su Unidad de Transparencia:

Sistema de Gestión de Recursos Humanos: Se utiliza para almacenar y gestionar información relacionada con el personal municipal, incluyendo datos de nómina, contratación y desempeño laboral.

Plataforma de Atención Ciudadana: Utilizada para gestionar consultas, quejas y solicitudes de los ciudadanos, contiene datos personales de contacto y detalles sobre las interacciones.

Sistema de Transparencia y Acceso a la Información: Se utiliza para gestionar solicitudes de acceso a la información pública, que incluyen datos personales de los solicitantes.

Sistema de Videovigilancia: Este sistema de videovigilancia incluye cámaras de seguridad conectadas a un NVR (Grabador de Video en Red) para almacenamiento de videos. Los detalles específicos sobre el acceso y tratamiento de los datos de videovigilancia se detallan a continuación.

3. Sistemas de Videovigilancia
El sistema de videovigilancia consiste en cámaras de seguridad distribuidas en áreas estratégicas del municipio. Cada una de estas cámaras está conectada a un NVR, el cual se encarga de almacenar todos los videos capturados por las cámaras. Los videos se conservan en el NVR hasta que se llena todo su espacio de disco duro. Una vez alcanzada la capacidad máxima, el NVR comienza a sobrescribir los videos más antiguos con los más recientes, asegurando así la disponibilidad de espacio para nuevas grabaciones.

4. Acceso Restringido
El acceso a los datos almacenados en los NVR está estrictamente controlado y restringido. Solo el personal autorizado de las Jefaturas de Redes y TI, el director de área de Redes y TI, el Director General de Sistemas y el personal de C2 en Seguridad Pública tienen acceso a los videos grabados por las cámaras de videovigilancia.

5. Aviso de Privacidad
Se ha elaborado y difundido un Aviso de Privacidad que informa a los ciudadanos sobre el uso de las cámaras de videovigilancia, así como sobre el tratamiento de los datos personales que puedan ser captados por estas.

6. Control de Acceso a las Cámaras
Cada cámara de videovigilancia cuenta con un usuario y una contraseña de acceso. Estas credenciales son exclusivas y están en posesión del personal autorizado mencionado anteriormente, garantizando así que solo personas debidamente autorizadas puedan acceder a las imágenes grabadas.

7. Resguardo de Equipos y Seguridad de Sistemas
Los equipos relacionados con la videovigilancia, como las cámaras y los NVR, son resguardados por la Dirección de Patrimonio. Por otro lado, la seguridad de los sistemas informáticos asociados a la videovigilancia es responsabilidad de la Dirección General de Sistemas, la cual implementa medidas de seguridad adecuadas para proteger la integridad y confidencialidad de los datos.

II Las Funciones Y Obligaciones De Las Personas Que Traten Datos Personales

> El Artículo 38 fracción II de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales

El tratamiento de datos personales es una responsabilidad compartida que recae en diversos participantes dentro del H. Ayuntamiento de Manzanillo y su Unidad de Transparencia. A continuación, se detallan las funciones y obligaciones del personal involucrado en el manejo de datos personales:

1. Responsabilidades Generales

Cumplimiento Legal: Todo el personal encargado del tratamiento de datos personales debe cumplir estrictamente con las disposiciones legales y normativas aplicables, incluyendo la LPDPPSOEC y otras regulaciones pertinentes.
Confidencialidad: Se espera que el personal trate la información personal con la debida confidencialidad y que solo la divulgue o comparta según sea necesario en el ejercicio de sus funciones.
Capacitación: El personal debe participar en programas de capacitación y concienciación en materia de protección de datos personales, con el fin de mantenerse al tanto de las mejores prácticas y políticas de seguridad de la información.

1.1. Secretaria Particular del Despacho

1.1.1. Departamento de Atención Ciudadana.

1.2. Asistente Operativa

1.3. Dirección General de Participación Ciudadana y Desarrollo Comunitario

1.3.1. Dirección de Participación Ciudadana

1.3.2. Dirección de Formación y Educación Comunitaria

1.3.3. Coordinación General

1.3.4. Supervisor de Cuadrilla

1.3.5. Coordinación PAPSC

1.4. Dirección de Asesoría Municipal

1.5. Dirección de Comunicación Social

1.5.1. Subdirección de Comunicación Social

1.5.2. Departamento de Información.

1.5.3. Departamento de Redes Sociales

1.5.4. Departamento de Fotografía y Video

1.5.5. Departamento de Planeación y Medios Alternativos

1.5.6. Departamento de Diseño

1.6. Unidad de Transparencia

1.6.1. Departamento de Información Pública Gubernamental

1.6.2. Departamento de Protección de Datos Personales

1.6.3. Coordinación de Transparencia

1.7. Juzgado Cívico Municipal

1.7.1. Jueces Cívicos Municipales

1.7.2. Secretario de Juzgado Cívico Municipal

1.7.3. Unidad de Mediación Ciudadana

1.7.4. Unidad de Evaluación Médica

1.7.5. Unidad de Evaluación Psicológica

1.7.6. Unidad de Resguardo Ciudadano

1.8. Coordinación del Sistema Municipal de Justicia Cívica

1.8.1. Departamento de Vinculación Social

1.8.2. Departamento de Lengua de Señas Mexicana

1.9. Dirección General de Inspección y Vigilancia

1.10. Procuraduría Municipal de Protección de Niñas, Niños y Adolescentes

1.11. Secretaría Técnica de Infraestructura y Planeación

2. SECRETARÍA DEL AYUNTAMIENTO

2.2. Dirección de Archivo Histórico

2.3. Dirección de Protección Civil y Bomberos

2.4. Dirección de Asuntos Internos

2.6. Junta Municipal de Reclutamiento

3.4. Dirección de Ingresos y Zona Federal

3.5.1. Departamento de Padrón y Licencias Comerciales

4.5 Dirección de Recursos Humanos

4.6. Dirección de Adquisiciones

5. CONTRALORÍA MUNICIPAL

6. DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS

7. DIRECCIÓN GENERAL DE DESARROLLO SOCIAL

8. DIRECCIÓN GENERAL DE DESARROLLO HUMANO

8.1. Dirección de Educación y Juventud

9. DIRECCIÓN GENERAL DE DESARROLLO ECONÓMICO Y TURÍSTICO

9.7. Dirección de Ferias, Eventos y Exposiciones

10. DIRECCIÓN GENERAL DE MEDIO AMBIENTE

11. DIRECCIÓN GENERAL DE DESARROLLO URBANO

12. DIRECCIÓN GENERAL DE OBRAS PÚBLICAS

13. DIRECCIÓN GENERAL DE SERVICIOS PÚBLICOS

14. DIRECCIÓN GENERAL DE SEGURIDAD PÚBLICA Y POLICÍA VIAL

14.1 Subdirección General de Seguridad Pública y Policía Vial

15. DIRECCIÓN GENERAL DE SISTEMAS COMPUTACIONALES

16. DIRECCIÓN GENERAL DE DESARROLLO RURAL Y PESCA

17. DIRECCIÓN GENERAL DE CATASTRO

2. Personal de la Unidad de Transparencia

Gestión de Solicitudes: El personal de la Unidad de Transparencia es responsable de gestionar las solicitudes de acceso a la información pública, asegurándose de que se manejen los datos personales de acuerdo con los procedimientos establecidos y en cumplimiento de la ley.
Elaboración y Divulgación de Avisos de Privacidad: Es responsabilidad de este personal elaborar y difundir los avisos de privacidad pertinentes, informando a los ciudadanos sobre el tratamiento de sus datos personales.

3. Personal de TI y Redes

Mantenimiento de Sistemas: El personal de TI y redes debe garantizar la seguridad y el buen funcionamiento de los sistemas informáticos y de comunicaciones utilizados para el tratamiento de datos personales.
Control de Acceso: Son responsables de administrar los controles de acceso a los sistemas que contienen datos personales, asegurando que solo el personal autorizado tenga acceso a la información.

4. Personal de Seguridad Pública

Acceso a Videovigilancia: El personal de seguridad pública autorizado tiene acceso a los videos grabados por las cámaras de videovigilancia, y deben utilizar esta información de manera responsable y conforme a los procedimientos establecidos.

5. Personal de Patrimonio

Resguardo de Equipos: Este personal es responsable del resguardo y mantenimiento de los equipos relacionados con la videovigilancia, como las cámaras y los NVR, garantizando su integridad y disponibilidad.

6. Monitoreo y Supervisión

Supervisión Continua: Se designará personal responsable de monitorear y supervisar el cumplimiento de las políticas y procedimientos establecidos en este Documento de Seguridad, así como de informar sobre cualquier incidente o violación de seguridad.

III Análisis de Riesgos

El Artículo 38 fracción III de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la Realización de análisis de riesgo del tratamiento de datos personales

El análisis de riesgos es un componente fundamental en la gestión de la seguridad de la información dentro del H. Ayuntamiento de Manzanillo y su Unidad de Transparencia. Este proceso permite identificar y evaluar los riesgos potenciales asociados con el tratamiento de datos personales, así como determinar las medidas de seguridad adecuadas para mitigarlos. A continuación, se describen los pasos para realizar un análisis de riesgos efectivo:

Identificación de Activos: Se identifican todos los activos de información relevantes para el ayuntamiento y su unidad de transparencia, incluyendo sistemas, bases de datos, documentos y otros recursos que contengan datos personales.

Identificación de Amenazas: Se identifican las posibles amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de los datos personales, como ataques cibernéticos, errores humanos, desastres naturales, entre otros.

Evaluación de Vulnerabilidades: Se evalúan las vulnerabilidades existentes en los sistemas y procesos de tratamiento de datos, que podrían ser explotadas por las amenazas identificadas.

Determinación del Impacto: Se determina el impacto potencial que tendría la materialización de cada amenaza en los activos de información, en términos de pérdida financiera, daño a la reputación, violación de la privacidad, entre otros.

Evaluación de Riesgos: Se calcula el nivel de riesgo asociado con cada amenaza, multiplicando la probabilidad de ocurrencia por el impacto potencial.

Priorización de Riesgos: Se priorizan los riesgos identificados en función de su nivel de gravedad, para enfocar los recursos en la mitigación de aquellos con mayor impacto y probabilidad de ocurrencia.

Selección de Medidas de Seguridad: Se seleccionan y se implementan las medidas de seguridad adecuadas para mitigar los riesgos identificados, tales como controles de acceso, encriptación de datos, políticas de respaldo, entre otros.

Monitoreo y Revisión Continua: Se establece un proceso de monitoreo y revisión continua para asegurar que las medidas de seguridad sean efectivas y se ajusten según sea necesario ante cambios en el entorno operativo o nuevas amenazas.

IV Análisis de brecha

El Artículo 38 fracción IV de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la Realización de análisis de brecha acorde al tratamiento de datos personales

Dentro del marco operativo del H. Ayuntamiento de Manzanillo y su Unidad de Transparencia, En el contexto del H. Ayuntamiento de Manzanillo y su Unidad de Transparencia, donde la protección de datos personales y la seguridad de la información son aspectos fundamentales, surge la necesidad de realizar un análisis de brechas. Este análisis se presenta como una herramienta estratégica para evaluar la disparidad entre el estado actual de las prácticas de seguridad y el estado deseado. A través de este proceso, se busca identificar las áreas de mejora y las deficiencias en políticas, procedimientos y sistemas, especialmente en aspectos clave como el tratamiento de datos personales, la gestión de la videovigilancia y el cumplimiento normativo. Al abordar estas brechas de manera proactiva, la organización puede fortalecer su postura de seguridad, mitigar riesgos y avanzar hacia el cumplimiento de los más altos estándares en protección de datos y seguridad de la información.

Evaluar el Estado Actual:
Revisión de políticas y procedimientos de seguridad de la información existentes en el ayuntamiento y la unidad de transparencia.
Evaluación de los controles de seguridad implementados, como firewalls, antivirus, sistemas de detección de intrusiones, etc.
Análisis de la capacitación del personal en materia de seguridad de la información.
Revisión de medidas de protección de datos implementadas, como cifrado, etc.

Identificar Requisitos de Seguridad:
Análisis detallado de los requisitos de seguridad establecidos en el Documento de Seguridad y la LPDPPSOEC.
Identificación de los principales estándares y regulaciones relacionados con la protección de datos personales y la transparencia.

Comparar con el Estado Deseado:
Identificación de las brechas entre el estado actual de la seguridad de la información y los requisitos establecidos en el Documento de Seguridad y otras normativas aplicables.
Ejemplos de brechas pueden incluir la falta de controles adecuados para proteger datos personales, deficiencias en la capacitación del personal en seguridad de la información, etc.

Priorizar Brechas:
Clasificación de las brechas identificadas según su impacto potencial en la seguridad de la información y la probabilidad de ocurrencia.
Priorización de las brechas más críticas que representen un mayor riesgo para la protección de datos personales y la transparencia.

Desarrollar un Plan de Acción:
Creación de un plan de acción detallado para abordar cada una de las brechas identificadas.
El plan de acción debe incluir la implementación de nuevos controles de seguridad, actualización de políticas y procedimientos, capacitación del personal, entre otros.

Implementar Medidas Correctivas:
Ejecución del plan de acción desarrollado para cerrar las brechas identificadas.
Asignación de recursos adecuados y colaboración entre diferentes áreas para garantizar la efectividad de las medidas correctivas.

Monitorear y Revisar Regularmente:
Monitoreo continuo de la seguridad de la información y revisión periódica del estado de las brechas identificadas.
Actualización del plan de acción según sea necesario para garantizar el cumplimiento continuo de los requisitos de seguridad.

V Plan de trabajo

En el contexto actual de avances tecnológicos y crecientes desafíos en materia de seguridad y protección de datos, el H. Ayuntamiento de Manzanillo reconoce la importancia fundamental de garantizar la integridad, confidencialidad y disponibilidad de la información, así como la salvaguarda de los datos personales de sus ciudadanos. Con el objetivo de fortalecer la seguridad y protección de datos en todas sus operaciones y servicios, se ha desarrollado el presente plan de trabajo.

El principal objetivo de este plan es implementar medidas efectivas que mejoren la seguridad de la información y protejan los datos personales dentro del H. Ayuntamiento de Manzanillo y su Unidad de Transparencia. A través de una evaluación exhaustiva, identificaremos las áreas de riesgo y vulnerabilidad, desarrollaremos estrategias para mitigar dichos riesgos y fortaleceremos la infraestructura de seguridad, incluyendo los sistemas de vigilancia, para garantizar un entorno seguro y confiable para nuestros ciudadanos y colaboradores.

> El Artículo 38 fracción V de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la Realización de plan de trajo para mejorar el tratamiento de datos personales.

Evaluación Integral de Seguridad: Iniciar con una evaluación exhaustiva de la seguridad de la información y de las instalaciones del H. Ayuntamiento de Manzanillo, incluyendo la revisión de políticas, procedimientos y controles de seguridad existentes. Esta evaluación abarcará también la infraestructura de las cámaras de vigilancia para asegurar su adecuada configuración y funcionamiento.

Análisis de Brecha de Seguridad y Protección de Datos: Realizar un análisis detallado de brechas para identificar áreas de mejora en la seguridad y protección de datos personales, tomando en cuenta los resultados obtenidos de la evaluación previa. Este análisis incluirá aspectos como la capacitación del personal, la actualización de políticas y procedimientos, así como la implementación de controles adicionales en función de las necesidades identificadas.

Implementación de Medidas Correctivas y Preventivas: Desarrollar e implementar un plan de acción para abordar las brechas identificadas, priorizando aquellas áreas que representen un mayor riesgo para la seguridad de la información y la protección de datos personales. Esto incluirá la actualización de políticas y procedimientos, la realización de capacitaciones específicas para el personal, así como la mejora y ampliación de los controles de seguridad, incluyendo los relacionados con las cámaras de vigilancia.

Mejora Continua y Monitoreo: Establecer mecanismos de monitoreo continuo para supervisar la efectividad de las medidas implementadas y detectar cualquier cambio en el entorno de seguridad. Esto incluirá la revisión periódica de los controles de seguridad, la realización de pruebas de vulnerabilidad y la actualización regular de las políticas y procedimientos en función de las lecciones aprendidas y las nuevas amenazas identificadas.

Capacitación y Concientización: Impartir programas de capacitación y concientización sobre seguridad de la información y protección de datos personales dirigidos al personal del H. Ayuntamiento de Manzanillo, con el objetivo de fomentar una cultura de seguridad y privacidad en toda la organización. Esto

incluirá la formación sobre el manejo adecuado de la información, el reconocimiento de amenazas y la respuesta ante incidentes de seguridad.

Fortalecimiento de la Infraestructura de Seguridad: Realizar mejoras en la infraestructura de seguridad, incluyendo la optimización de las cámaras de vigilancia y su integración con sistemas de monitoreo centralizado, para garantizar una cobertura efectiva de las áreas críticas y una respuesta rápida ante incidentes.

Auditorías y Certificaciones: Realizar auditorías internas y externas de seguridad de manera periódica para verificar el cumplimiento de las políticas y estándares de seguridad establecidos, así como para obtener certificaciones relevantes que demuestren el compromiso del H. Ayuntamiento de Manzanillo con la protección de datos personales y la seguridad de la información.

VI Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

El compromiso con la seguridad de la información y la protección de datos personales, el H. Ayuntamiento de Manzanillo ha establecido la implementación de mecanismos de monitoreo y revisión. Estos mecanismos buscan asegurar la eficacia de las medidas de seguridad ya implementadas, a través de un monitoreo continuo, garantizar que las medidas de seguridad en el tratamiento de datos personales sean efectivas y estén actualizadas. Esto permitirá al H. Ayuntamiento de Manzanillo identificar y abordar rápidamente cualquier vulnerabilidad o riesgo potencial, protegiendo así la privacidad y la confidencialidad de la información manejada

El Artículo 38 fracción VI de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad, así como las amenazas y vulneraciones que están sujetas a los datos personales y mejorar el tratamiento de los mismos

Monitoreo Continuo de Actividades: Implementaremos un sistema de monitoreo continuo para supervisar las actividades relacionadas con la seguridad de la información y la protección de datos personales en el H. Ayuntamiento de Manzanillo y su Unidad de Transparencia. Este sistema utilizará herramientas especializadas para rastrear el acceso a los sistemas, la actividad del usuario y posibles anomalías que puedan indicar una violación de seguridad.

Revisiones Periódicas de Políticas y Procedimientos: Realizaremos revisiones periódicas de las políticas y procedimientos de seguridad de la información para garantizar su relevancia y efectividad en un entorno operativo cambiante. Estas revisiones serán llevadas a cabo por un equipo designado de expertos en seguridad, quienes actualizarán las políticas según sea necesario para abordar nuevas amenazas y vulnerabilidades.

Auditorías Internas y Externas: Se llevarán a cabo auditorías internas y externas de seguridad de manera regular para evaluar el cumplimiento de las políticas y estándares de seguridad establecidos. Estas auditorías serán realizadas por equipos especializados en seguridad de la información, quienes identificarán posibles áreas de mejora y recomendarán acciones correctivas según sea necesario.

Evaluación de Incidentes de Seguridad: Estableceremos un proceso formal para la evaluación de incidentes de seguridad, que incluirá la investigación de cualquier incidente reportado o detectado, la determinación de su causa raíz y la implementación de medidas correctivas para prevenir futuros incidentes similares. Este proceso garantizará una respuesta rápida y efectiva ante cualquier amenaza o violación de seguridad.

Capacitación y Concientización Continuas: Continuaremos ofreciendo programas de capacitación y concientización sobre seguridad de la información y protección de datos personales para todo el personal del H. Ayuntamiento de Manzanillo. Estos programas se actualizarán regularmente para abordar nuevas amenazas y garantizar que todos los empleados estén al tanto de las mejores prácticas de seguridad.

Evaluación de Desempeño de Sistemas de Videovigilancia: Implementaremos un sistema de evaluación de desempeño para los sistemas de videovigilancia, que incluirá la revisión regular de la calidad de las imágenes capturadas, la funcionalidad de las cámaras y la integridad de los datos almacenados. Cualquier anomalía o problema detectado será abordado de manera oportuna para garantizar la efectividad continua de la vigilancia

Mecanismos	Medidas
Monitoreo y revisión	Cada una de las cámaras está agregada a un NVR, es cual almacena todos los videos de todas las cámaras que tenga asignadas hasta que se llena todo su espacio de disco duro, a partir de allí comienza a sobrescribir los videos más viejos con los videos más nuevos que se vayan generando.
Monitoreo	Tienen acceso Solo el personal de las Jefaturas de Redes y TI, el director de área de Redes y TI, el Director General de Sistemas y el personal de C2 en Seguridad Pública.
Monitoreo y revisión	Cada cámara tiene un usuario y una contraseña de acceso, las que solo tienen el personal de las Jefaturas de Redes y TI, el director de área de Redes y TI, el Director General de Sistemas
Revisión	La Dirección de Patrimonio tiene los resguardos, y la seguridad de los sistemas los maneja la Dirección General de Sistemas.
Revisión	Se realizan mantenimientos preventivos a todos los equipos de cómputo, impresoras, enlaces inalámbricos, servicios gratuitos de internet y cámaras de seguridad. Licencias de programas Se han estado llevando a cabo procesos de licenciamientos, con el cual ya la mayoría de las computadoras tienen sus licencias de Windows Resguardo de Servidores Se tienen resguardados todos los servidores bajo llave Control de resguardo El control de los resguardos los tiene la Dirección de Patrimonio

VII El programa general de capacitación

El Artículo 38 fracción VII de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, El programa general de capacitación para mejorar el tratamiento de datos personales

El presente Plan General de Capacitación ha sido desarrollado por el Departamento de Seguridad Informática y Protección de Datos del H. Ayuntamiento de Manzanillo, con el fin de fortalecer las competencias y conocimientos del personal en materia de seguridad de la información y protección de datos personales. Reconociendo la importancia estratégica de

estos temas para el adecuado funcionamiento y la reputación de la institución, se establece este plan como un instrumento fundamental para garantizar el cumplimiento normativo y promover una cultura organizacional orientada a la seguridad y privacidad de la información.
Objetivos:
Dotar al personal del H. Ayuntamiento de Manzanillo con los conocimientos necesarios para comprender, implementar y mantener medidas efectivas de seguridad de la información y protección de datos personales.
Promover una cultura de responsabilidad y compromiso en el tratamiento y manejo adecuado de la información confidencial.
Garantizar el cumplimiento de la normativa vigente en materia de protección de datos personales y seguridad de la información.

Contenido del Plan:

1. Fundamentos de Seguridad de la Información:
Conceptos básicos de seguridad de la información.
Importancia de la protección de datos personales.
Principios fundamentales de privacidad y confidencialidad.
2. Marco Legal y Normativo:
Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Colima (LPDPPSOEC).
Otras regulaciones y normativas relevantes.
Responsabilidades legales del personal en el tratamiento de datos personales.
3. Gestión de Riesgos y Brechas:
Identificación y evaluación de riesgos en el tratamiento de datos personales.
Análisis de brechas de seguridad y medidas correctivas.
Planificación y ejecución de acciones para mitigar riesgos.
4. Seguridad de Sistemas y Tecnologías:
Buenas prácticas en seguridad informática.
Protección de sistemas y redes.
Uso seguro de herramientas y aplicaciones tecnológicas.
5. Procesos y Procedimientos:
Políticas y procedimientos internos de seguridad.
Manejo seguro de la información.
Protocolos de respuesta ante incidentes de seguridad.
6. Concientización y Cultura de Seguridad:
Sensibilización sobre la importancia de la seguridad de la información.
Promoción de una cultura organizacional orientada a la seguridad.
Responsabilidad individual en la protección de datos personales.

Metodología de Capacitación: El plan se desarrollará a través de una combinación de modalidades presenciales y virtuales, incluyendo sesiones teóricas, talleres prácticos, estudios de casos y evaluaciones periódicas. Se asignará un equipo de instructores especializados para guiar y supervisar el proceso de aprendizaje, asegurando la comprensión y aplicación efectiva de los conceptos impartidos.

Evaluación y Seguimiento: Se llevarán a cabo evaluaciones periódicas para medir el nivel de conocimiento y competencia del personal en materia de seguridad de la información y protección de datos personales. Con base en los resultados obtenidos, se realizarán ajustes y mejoras al plan de capacitación para garantizar su eficacia y relevancia continua.

VIII Mecanismos de Restauración y Recuperación de Datos Personales

> El Artículo 38 fracción VIII de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, Los Mecanismos de Restauración y Recuperación de Datos Personales para mejorar el tratamiento de datos personales

En caso de destrucción o pérdida de datos personales, es fundamental contar con mecanismos efectivos de restauración y recuperación que permitan recuperar la información de manera oportuna y garantizar la continuidad de las operaciones. A continuación, se detallan los pasos y procedimientos para implementar estos mecanismos:

1. Plan de Respuesta a Incidentes:

Desarrollar un plan detallado de respuesta a incidentes que incluya procedimientos específicos para la restauración y recuperación de datos personales en caso de destrucción o pérdida.
Designar un equipo de respuesta a incidentes con roles y responsabilidades claramente definidos, incluyendo a personas encargadas de coordinar la restauración y recuperación de datos.

2. Copias de Seguridad:
Implementar un sistema de copias de seguridad periódicas de todos los datos personales almacenados en los sistemas de información.
Establecer políticas de retención de copias de seguridad que permitan mantener versiones históricas de los datos durante un periodo adecuado de tiempo.

3. Almacenamiento Seguro de Copias de Seguridad:
Almacenar las copias de seguridad en ubicaciones físicas y/o en la nube que sean seguras y accesibles únicamente para personal autorizado.
Utilizar técnicas de encriptación para proteger la integridad y confidencialidad de las copias de seguridad durante su almacenamiento y transmisión.

4. Procedimientos de Recuperación:
Establecer procedimientos detallados para la recuperación de datos a partir de las copias de seguridad en caso de destrucción o pérdida de la información.
Documentar los pasos necesarios para restaurar los datos en los sistemas de producción de manera segura y eficiente.

5. Pruebas de Recuperación:
Realizar pruebas periódicas de los procedimientos de recuperación para verificar su efectividad y corregir posibles fallos o deficiencias.
Registrar y evaluar los resultados de las pruebas de recuperación para identificar áreas de mejora y optimización.

6. Capacitación y Concientización:
Capacitar al personal involucrado en la restauración y recuperación de datos sobre los procedimientos y protocolos establecidos.
Promover una cultura de concientización sobre la importancia de la restauración y recuperación de datos personales en caso de incidentes de seguridad.

7. Revisión y Actualización Continua:
Revisar y actualizar periódicamente los mecanismos de restauración y recuperación de datos para garantizar su relevancia y eficacia ante nuevos riesgos y amenazas.
Incorporar lecciones aprendidas de incidentes previos para mejorar los procesos y procedimientos de restauración y recuperación.

El artículo 38 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima da la actualización del documento de seguridad cuando ocurran los siguientes eventos:

I. Inventarios de datos personales y de los sistemas de tratamiento.
II. Funciones y obligaciones del personal que trate datos personales.
III. Análisis de riesgo.
IV. Análisis de brecha.
V. El plan de trabajo
VI. Los mecanismos de monitoreo y la revisión de las medidas de seguridad.
VII. Programa general de capacitación.
VIII. Los mecanismos de restauración y/o recuperación de los datos personales en caso de destrucción o perdida

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.