Documento de Seguridad,

en materia de Protección de

Datos Personales del

Ayuntamiento de Calnali

2024 - 2027

Contenido

I. INTRODUCCION

En el Ayuntamiento de Calnali, la información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la organización. De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la organización afronta.

El presente Documento de Seguridad para Sistemas de Datos Personales se apega a las disposiciones jurídicas vigentes, siendo estas la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Hidalgo, la Ley de Transparencia y Acceso a la Información Pública del Estado de Hidalgo, para la mejor protección de los sistemas con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que estos contienen.

El documento brinda al Ayuntamiento de Calnali, homogeneidad en la organización, procesos y sistemas, en el que el Comité de Transparencia, conjuntamente con la Unidad de Transparencia y los responsables de los sistemas de datos personales, definen las medidas de seguridad administrativa y física implementadas para la protección de los sistemas de datos personales custodiados.

Así mismo, este documento tiene como propósito controlar internamente los sistemas de datos personales que posee el Ayuntamiento de Calnali, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

II. GLOSARIO

Área: Unidad administrativa, instancia u órgano del sujeto obligado que, en ejercicio de las funciones, atribuciones y/u obligaciones que le fueron asignadas para cumplir con sus fines y objetivos genere, posee y/o administre la información.

Auditabilidad: Característica que permite la revisión y análisis de eventos y análisis para su control posterior.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Autentificar: Acción de comprobar que la persona es quien dice ser. Ello mediante el cotejo de uno o más datos en dicha identificación oficial contra los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo).

Autorizar: Se considera como el acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que se le conceda el responsable de autorizar los accesos.

Bloqueo: La identificación y conservación de los datos personales, una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual correspondiente.

Clasificación: Acto por el cual se determina que la información que posee el Ayuntamiento de Calnali es reservada o confidencial.

Comité de Transparencia: El comité de Transparencia del Ayuntamiento de Calnali.

Confidencialidad: Propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, y que garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma, es decir, asegurar que la misma no sea divulgada o accedida a personas o procesos no autorizados.

Control de acceso: Medida de seguridad que permite el acceso únicamente a quien está autorizado para ello y una vez que se ha cumplido con el procedimiento de identificación.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima del titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este.

Destinatario: cualquier persona física o moral pública o privada que recibe datos personales.

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deban acceder a ella, ya sean personas, procesos o aplicaciones,

garantizando el acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorándums, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.

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.

Identificar: consiste aportar las pruebas necesarias para corrobar que una persona es quien dice ser, lo cual puede realizarse, por ejemplo, con una identificación que tenga validez oficial y en un ambiente electrónico con el nombre de usuario que se introduce al momento de ingresar al sistema (login).

Información: El conjunto organizado de datos contenido en los documentos (en cualquier forma: textual, numérica, grafica, cartográfica, narrativa o audiovisual, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro) que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título.

Instituto: Instituto de Transparencia y Acceso a la Información Pública del Estado de Hidalgo.

Integridad: Es garantizar la exactitud, totalidad y la confiabilidad de la información y los sistemas o métodos de procesamiento de manera que estos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

Ley: Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Hidalgo.

Lineamientos: Los actos administrativos de carácter general expedidos por el pleno del Instituto y de observancia obligatoria.

N/A: No aplica.

Protección a la duplicación: Consiste en asegurar que una transacción solo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grave una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Publicación: La reproducción en medios electrónicos o impresos de información contenida en documentos.

Recomendaciones: Las opiniones, propuestas, sugerencias, comentarios, y otros actos que emite el Instituto.

Recursos públicos: Los recursos humanos, financieros y materiales con que cuenta el Ayuntamiento de Calnali y que utiliza para alcanzar sus objetivos y producir los bienes o prestar los servicios que son de su competencia.

Respaldo incremental: Una operación de respaldo incremental solo copia los datos que han variado desde la última operación de respaldo de cualquier tipo. Se utiliza la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último respaldo. Se puede adquirir una aplicación de respaldo que identifica y registra la fecha y hora de realización de las operaciones de respaldo para identificar los archivos modificados desde esas operaciones.

Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

Servidores públicos habilitados: Los servidores públicos que pueden recibir y dar trámite a las solicitudes.

Sistemas de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Soportes físicos: Son los medios de almacenamiento identificables a simple vista, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

Tecnología de la Información: Se refiere al Hardware y software operado por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

Transmisión de datos personales: La entrega total o parcial de sistemas de datos personales a cualquier persona distinta del titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión.

Tratamiento: De manera enunciativa mas no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados 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: Área o Dirección que tengan la información de conformidad con las facultades que les correspondan.

Usuario: Servidor Público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

III. OBJETIVO

Describir el proceso de la administración de seguridad física y las normas comprendidas en la materia, a cargo del Ayuntamiento de Calnali, con el objetivo primordial de dar cumplimiento a los señalado en el artículo 53 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Hidalgo, con referencia a la guía para la elaboración de un documento de seguridad y la elaboración de especificaciones, guías, procedimientos generales, instrucciones de trabajo y registros de control.

IV. MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos
- Ley General de Transparencia y Acceso a la Información Publica
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos
- Reglamento de la Ley Federal de transparencia y Acceso a la Información Pública Gubernamental
- Constitución Política del Estado de Hidalgo
- Ley de Transparencia y Acceso a la Información Pública del Estado de Hidalgo
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Hidalgo
- Lineamientos Generales de Protección de Datos Personales para el Sector Público

V. TIPOS DE MEDIDAS DE SEGURIDAD

1) **MEDIDAS DE SEGURIDAD ADMINISTRATIVA:** 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. Deben implementarse para la consecución de los objetivos contemplados en los siguientes propósitos:

- **Política de seguridad:** Definición de directrices estratégicos en materia de seguridad de activos, alineados a las atribuciones del Ayuntamiento de Calnali. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios.
- **Cumplimiento de la normatividad:** Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal.
- **Organización de la seguridad de la información:** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de los datos personales. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.
- **Clasificación y control de activos:** Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.
- **Seguridad relacionada a los recursos humanos:** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.
- **Administración de incidentes:** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.
- **Continuidad de las operaciones:** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

2) **Medidas de seguridad física**

Seguridad física y ambiental: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa mas no limitativa, se debe considerar las siguientes actividades:

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización.
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

3) **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 recursos involucrados en su tratamiento. De manera enunciativa mas no limitativa, se deben considerar las siguientes actividades:

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del hardware y software.
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

VI. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

Medidas de Seguridad Físicas:

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Entorno Institucional	• Resguardo de documentos e información en archivos físicos de trámite y concentración. • Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información. • Limitar el número de personas con acceso a archivos físicos. • Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales. • Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales. • Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales. • Resguardo de llaves en oficinas de acceso restringido.
Entorno de los datos	• No se sitúan equipos en sitios altos para evitar caídas • No se colocan elementos móviles sobre los equipos para evitar que caigan sobre ellos. • El Ayuntamiento esta provisto de equipo para la extinción de incendios.

Controles de Identificación y Autenticación de Usuarios

Parte de tener control efectivo al trato de los datos personales es contar con un sistema que garantice la autenticación de usuarios, esto es por medio de administración de cuentas creadas específicamente para cada servidor público.

La administración de cuentas de usuario es una parte esencial de los sistemas que se desarrollan en el departamento de software. La razón principal de las cuentas de usuario es verificar la identidad de cada funcionario también permite la utilización personalizada de acceso a la información y generación de la misma.

Esta medida es tomada para los correos electrónicos institucionales y para cualquier sistema o plataforma tecnológica que cree este sujeto obligado.

El estándar para la creación de las cuentas es:

Usuario: Generalmente es el correo electrónico institucional.

Contraseña: Frase de confirmación de identidad que se encuentra encriptada para mayor seguridad.

Procedimientos de respaldo y recuperación de datos personales

Respaldo	Se realiza una digitalización completa de la información que ingresa a través de la oficialía de partes y se almacena en discos duros. A partir de la aprobación del presente documento deberá realizarse un respaldo incremental almacenado en discos duros. Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental del Sujeto Obligado, atendiendo a la establecido en la Ley de Transparencia y Acceso a la Información Pública del Estado de Hidalgo y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Hidalgo
Recuperación	Los respaldos incrementales contienen fecha y hora, tanto inicial como final. La recuperación se realiza cruzando la fecha del incidente y el ultimo respaldo.

Controles y mecanismos de seguridad para las transferencias

Transmisiones mediante el traslado de soportes físicos	1. Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información; así como para la Elaboración de Versiones Publicas. 2. La información solo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial. 3. Toda entrega de información requiere acuse de recibido. 4. A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.
Transmisiones mediante el traslado físico de soportes electrónicos	1. Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información; así como para la Elaboración de Versiones Publicas. 2. La información solo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial. 3. Toda entrega de información requiere acuse de recibido. 4. A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área. 5. A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar cifrados.
Transmisiones mediante el traslado sobre redes electrónicas	1. A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán ser sometidos a un proceso a través del cual la información puede ser codificada para no ser accedida por otros, a menos que tengan la clave del cifrado.

Transferencias	⊗ Interinstitucionales ○ Internacionales ⊗ Con entes privados
Tipo de traslado	⊗ De soportes físicos ○ Físico de soportes electrónicos ⊗ Sobre redes electrónicas

Bitácoras de acceso, Operación cotidiana y Vulneraciones a la Seguridad de los Datos Personales

Bitácoras de acceso	1) Las bitácoras de acceso a los datos personales se utilizan en los soportes y contienen la siguiente información: • Nombre y cargo de quien accede • Identificación del expediente • Fojas del Expediente • Propósito del Acceso • Fecha de Acceso • Hora de Acceso • Fecha de Devolución • Hora de Devolución

Vulneraciones a la Seguridad de los Datos Personales	La bitácora de vulneraciones contiene la siguiente información: 1) Nombre de quien reporta el incidente 2) Cargo 3) La fecha en la que ocurrió 4) El motivo de la vulneración de seguridad 5) Las acciones correctivas implementadas de forma inmediata y definitiva

Técnicas de Supresión y Borrado Seguro de Datos Personales

Métodos Físicos

1) Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados partículas, lo cual hace prácticamente imposible que se puedan unir.
2) Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o perdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Métodos Lógicos

Sobre-escritura: consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

Análisis de riesgos

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, se han identificado los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Origen de la amenaza	Causa	Posibles consecuencias
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del municipio.	Adquirir información o datos personales.	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas. Robo de información.
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales del municipio.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Extorsiones. Ataques a personas. Robo de información. Vulneración a la seguridad física y mental de los ciudadanos. Robo de información.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales.

		Robo de información. Extorsión. Modificaciones no autorizadas. Robo de información.
Daño físico.	Agua. Fuego. Accidentes. Corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.
Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios. Falta de actualización de antivirus.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales.	Daño y/o pérdida de los datos personales.

	La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	Modificaciones no autorizadas.

Identificación de Medidas de Seguridad

	Control	Parámetro
Medidas de Seguridad Administrativas	Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada, publicada y comunicada a todos los integrantes de la administración municipal.	En cuanto al presente documento de seguridad sea terminado, será expuesto para su revisión y aprobación y su posterior difusión.
	Avisos de privacidad: Los requisitos para los avisos de privacidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Los avisos de privacidad serán publicados y actualizados anualmente en caso de ser necesario a la par del documento de seguridad.
	Atender las necesidades de seguridad cuando se trata con ciudadanos: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los ciudadanos, a los activos o información de la organización.	Se realizarán la versión publica de los documentos para poder cumplir con los requerimientos de Trasparencia de los ciudadanos.
	Inventarios de Activos: Todos los activos deben ser claramente identificados y se debe elaborar y mantener un inventario de los activos más importantes.	Se realizará un inventario de activos y se actualizará anualmente.
	Roles y Responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de	Se dará a conocer a los involucrados sus roles y responsabilidades sobre la seguridad de datos personales.

	seguridad de la información de la organización.	
	Términos y Condiciones del Empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarias de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Cada vez que sea contratado algún empleado nuevo, contratista o usuario de tercero se anexara a su contrato sus responsabilidades sobre los términos y condiciones respecto a la seguridad de información.
	Administración de Medios Removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Cuando implementen se los Medios Removibles, se hará un manual sobre el uso de los mismos.
	Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Se implementará la bitácora de Intercambio de Información además de las medidas de seguridad ya citadas en este documento.
	Uso Sistema de Monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Las bitácoras de cada área serán implementadas para un control en el uso de la información y los sistemas.
	Registro de Usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicio de información.	Las Bitácoras de cada área ayudara con la administración de usuarios externos al área misma, además el encargado de cada área será el responsable de la administración de acceso a los sistemas de información, así sea físicos o digitales (contraseñas, usuarios, llaves de archiveros).
	Procedimiento de Control de Cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	En caso del cambio de algún administrador de área, el nuevo encargado de la misma deberá de asegurarse de que su antecesor le entregué todas las etapas de seguridad como usuarios, contraseñas y llaves de archiveros, además de informar al encargado de la Unidad de

		Trasparencia con un Oficio el cumplimiento de lo anterior.
	Procedimientos y Responsabilidades de Respuesta a Incidentes de Seguridad de la Información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	En este documento de seguridad se explican los procedimientos en caso de algún incidente de Seguridad de Información, que serán explicados a los encargados de cada área, además serán capacitados para aplicar correctamente los procedimientos y dar a conocer cada uno sus responsabilidades sobre seguridad.
	Verificación del Cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	En cada inventario se revisará el estado de los equipos y se actualizarán o instalarán los protocolos de seguridad adecuados.
	Distribución de las Responsabilidades de Seguridad de la Información: Todas las responsabilidades de seguridad deben estar claramente definidas.	En las capacitaciones se tratará la distribución de responsabilidades de tal manera que entren claramente definidas.
	Retorno de Activos: Todos los empleados, contratistas y usuarios de terceras partes, deben regresar a la organización todos los activos que tengan en posesión una vez termine el trabajo, contrato o acuerdo.	Todos los activos serán retornados y se llevarán a cabo las medidas de eliminación y formateo necesarios para su reutilización.
Medidas de Seguridad Avanzadas para Accesos desde intranet	Eliminación o Reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o formateo apropiado de cualquier información sensible y software de autor antes de su eliminación	Antes de cualquier procedimiento de Eliminación o Reutilización se llevará a cabo un formateo apropiado del equipo.
	Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos malicioso. Se deberán	Se cotizarán y se asignara un presupuesto para la instalación de un antivirus para evitar problemas con los equipos informáticos.

	implementar procedimientos de concienciación adecuados.	
	Registro de Auditoria: Se deberán producir y almacenar registros de auditoria relacionados a las actividades de los usuarios, las excepciones y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Se realizarán auditorias aleatorias entre áreas para mejorar las medidas de seguridad y monitorear los controles de acceso.
	Administración de Privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	Solamente el Titular de la Unidad de Transparencia tendrá la capacidad de asignar privilegios.
	Uso de Contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Cada equipo tendrá una contraseña segura que únicamente será conocida por el usuario de ese equipo, se seguirán las recomendaciones de contraseñas que se explican en este documento.
	Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	De momento se utiliza cualquier documento oficial que pueda autentificar su identidad (INE, Credencial de alguna institución pública)
	Control de Vulnerabilidades Técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	La bitácora de vulnerabilidades que se llevara a cabo y cuyos formatos están incluidos en este documento servirá para obtener oportunamente las vulnerabilidades técnicas y poder generar acciones para corregirlas.
Medidas de Seguridad Físicas	Política sobre el uso de Controles Criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Se darán a conocer a través de manuales sobre como encriptar documentos de Word y Excel.
	Respaldos de Información: Deberán realizarse copias de respaldo de la información y	A través de distintos métodos de respaldo: USB, Disco Duro y la Implementación de la nube y se

	aplicaciones. Se deberán probar los respaldos de acuerdos a una política establecida.	realizaran respaldos periódicos para evitar la pérdida de información.
	Eliminación de los Derechos de Acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Actualmente solo los responsables de cada área tienen derecho de acceso a la información de la misma, y en caso de la contratación de nuevo personal tendrán definidos sus derechos de acceso.
	Perímetro de Seguridad Física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	Se está trabajando en la construcción de una pared divisoria para mejorar la protección de la oficina más vulnerable, además todos los archivos están resguardados dentro de cada área.
Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad	Eliminación y Entrega de los Medios de Almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando se desocupen los medios almacenamiento se utilizarán los protocolos de formateo necesarios para que ser reutilizados y de destrucción apropiados antes de su eliminación.
	Medios Físicos de Almacenamiento en Transito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Cuando se tenga el medio físico de almacenamiento en cada área, será resguardado bajo llave que solo posea el encargado de la misma.
	Políticas y Procedimientos de Intercambio de Información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo instalaciones de comunicaciones.	Se implementará la bitácora de transferencia de tal manera que el intercambio información estará controlado, además de utilizar protocolos adecuados para el intercambio información.
	Política de Uso de los Servicios de Red: Los usuarios solo deben contar con acceso a los servicios para los que han sido autorizados.	Para llevar esto acabo se utilizarán las contraseñas en los equipos de cada área de tal manera que solo el encargado de esa área pueda acceder a ellos.

Análisis de brecha

- 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.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.
- Cada oficina cuenta con puertas que separa el área al momento de terminar labores.
- 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 (electrónica, física, en plataformas, o cualquiera generada) y guardada está en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados 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, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área. Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas del sujeto obligado El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

VII. GESTIÓN DE VULNERABILIDADES

Plan de respuesta

1) Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
2) En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
3) Llenado de Formato A (anexo 1), por parte de la persona que detecto la vulneración.
4) Llenado de Formato B (anexo 2), por parte de la Unidad de Transparencia.
5) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
6) Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia.
7) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.
8) Llenado de la bitácora de vulneraciones conforme al artículo 56 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Mecanismos de monitoreo y revisión de las medidas de seguridad

Informe anual

Primer monitoreo y evaluación de los sistemas de seguridad durante el mes diciembre y presentación de informe al pleno durante los primeros días de enero.

Plan de trabajo

Documento de Seguridad para la Protección de Datos Personales del Ayuntamiento de Calnali.

Duración tres años

Se ha planteado implementar la totalidad de las medidas de seguridad faltantes en un periodo de tres años a partir de la aprobación del presente documento de seguridad.

En este sentido, las medidas de seguridad físicas y técnicas que requieran la erogación de recursos como la compra de muebles incombustibles, y cestos metálicos para papeles y sustitución de los materiales plásticos e inflamables, se realizaran conforme a los tiempos administrativos de la institución y el presupuesto lo permita.

Año 1:

Control	Parámetro
Fuga de información: se deben prevenir las oportunidades de fuga de información.	Ninguno.
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Ninguno.
Política sobre el uso de controles criptográficos: una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.

Año 2

Actividad	Áreas involucradas
Términos y condiciones de empleo: Como parte su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Jurídico Oficialía Mayor Unidad de Transparencia
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Unidad de Transparencia
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Jurídico Unidad de Transparencia
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Unidad de Transparencia
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Unidad de Transparencia
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas	Unidad de Transparencia

Control	Parámetro
Eliminación de los derechos de acceso: los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, la información e instalaciones de procedimiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Jurídico Unidad de Transparencia Síndico Procurador
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales	Ninguno.
Eliminación del Plan de Contingencia	Todas las áreas.

Programa General de Capacitación

La capacitación del personal del Sujeto Obligado es anual y está dividido en ocho áreas de responsabilidad con las mismas temáticas:

Niveles de responsabilidad	Temáticas
Asamblea Municipal	Generalidades de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados. Principios y deberes. Sistema de Gestión, Medidas de seguridad y acciones preventivas.
Síndico Procurador Municipal	
Órgano Interno de Control	
Secretaria General Municipal	
Tesorería Municipal	
Unidad de Transparencia y Soporte Técnico	
Encargados de las áreas administrativas	
Delegados Auxiliares Municipales	

VIII. ÁMBITO DE APLICACIÓN

El presente documento de seguridad es aplicable y de observancia obligatoria para todas las unidades administrativas del Ayuntamiento de Calnali, en cumplimiento a las funciones que le son inherentes, por todos los individuos que pertenezcan a este y sea cual fuere su nivel jerárquico y su situación en la institución; así como para las personas externas que, debido a la presentación de un servicio, tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

NIVELES DE PROTECCIÓN DE LOS DATOS PERSONALES

Las medidas de seguridad que son aplicables a cada uno de los sistemas a cargo del Ayuntamiento de Calnali, deberán considerar el tipo de datos personales que contiene, lo cual determina el nivel de protección requerido, siendo básico, medio o alto, como a continuación se establece:

Nivel de protección básico:

a) Datos de identificación: Nombre, domicilio, estado civil, firma, RFC, CURP, lugar de nacimiento, fecha de nacimiento.

b) Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Nivel de protección medio:

a) Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

b) Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, el Ayuntamiento de Calnali, debe asegurar de acuerdo con la naturaleza de los datos contenidos en los sistemas de datos personales que custodia, los niveles de protección conforme a su grado de confidencialidad, disponibilidad e integridad.

TIPO DE TRANSMISIONES DE DATOS PERSONALES Y MODALIDADES PARA LA TRANSMISIÓN

Se deberán considerar tres tipos de transmisiones que se pueden llevar a cabo dependiendo de quién sea el destinatario:

a) Interinstitucionales: Transmisiones de datos a dependencias y entidades de la Administración Pública Federal, de los órganos Poder Judicial de la Federación, de los poderes Legislativo, Ejecutivo y Judicial locales de las entidades federativas, en el ejercicio de sus facultades.
b) Internacionales: Transmisiones a gobiernos de otro Estado reconocido por la comunidad Internacional y/u órganos internacionales y sus organismos, cuya competencia que motive el requerimiento haya sido reconocida por el Estado Mexicano.
c) Con entes privados u organizaciones civiles.

Para implementar las medidas de seguridad aplicables a las transmisiones citadas, la Unidad Administrativa responsable, debe considerar la modalidad por la cual se envían los datos personales a los destinatarios, pudiendo hacerse mediante el traslado de soportes físicos, mediante el traslado físico de soportes electrónicos o el traslado sobre redes electrónicas. Cada una de estas modalidades se deberá ceñir a lo siguiente:

a) Traslado de soportes físicos: En esta modalidad los datos personales se trasladan en medios de almacenamiento inteligibles a simple vista que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo del traslado de soportes

físicos es cuando una dependencia envía por correspondencia oficios o formularios impresos.
b) Traslado físico de soportes electrónicos: En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo de ello es cuando una dependencia entrega a otra por mensajería oficial un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

c) Traslado sobre redes electrónicas: En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet.

Catálogo de sistemas de datos personales. Versión publica

Unidad Administrativa: Unidad de Transparencia	
Nombre del sistema:	Expedientes ARCO
Responsable:	
Nombre:	TSU. Pedro Pablo Octaviano
Cargo:	Titular de la Unidad de Transparencia
Adscripción:	Presidencia Municipal
Correo electrónico:	u.de.transparencia.calnali.2024@gmail.com
Teléfono:	7713295347
Funciones:	Recibir y dar trámite a las solicitudes de derechos ARCO.
Obligaciones:	Supervisar el correcto resguardo de los datos personales
Datos personales contenidos en el sistema:	Datos personales: Nombre, Apellido Paterno, Apellido Materno, Domicilio, Teléfono, Correo Electrónico, Firma, Huella, Edad, Estado Civil
Folio del registro en el Sistema personal	

Estructura y descripción de los sistemas de datos personales. Versión pública.

Formulario que llenan las áreas generadoras versión pública.

Unidad Administrativa: (Nombre de la unidad administrativa)	
Nombre del sistema:	(El fin por el cual se recabaron los datos) *Es un formato para cada tramite o programa. Ejemplo: Solicitud de Derechos ARCO
Responsable:	
Nombre:	(Nombre completo del Responsable) Ejemplo: TSU. Pedro Pablo Octaviano
Cargo:	(Cargo que desempeña el Responsable): Ejemplo: Titular de la Unidad de Transparencia
Adscripción:	(Área de adscripción de la Unidad Administrativa) Ejemplo: Presidencia Municipal
Correo electrónico:	(Correo electrónico institucional de la unidad Administrativa) Ejemplo: u.de.transparencia.calnali.2024@gmail.com
Teléfono:	(Teléfono institucional de la Unidad Administrativa) Ejemplo: 7713295347
Funciones:	(La que señala el Manual Organizacional del Ayuntamiento de Calnali) Ejemplo: Recibir y dar trámite a las solicitudes de derechos ARCO.
Obligaciones:	(La que señala el Manual Organizacional del Ayuntamiento de Calnali) Ejemplo: Supervisar el correcto resguardo de los datos personales.
Encargado:	
Nombre:	(Nombre completo del personal que tenga acceso a los datos personales recabados) *Si es más de uno, es necesario repetir este recuadro “Encargado” Ejemplo: Lic. “N”
Cargo:	Ejemplo: Auxiliar, Secretaria
Adscripción:	Ejemplo: Presidencia Municipal
Correo electrónico:	Ejemplo: u.de.transparencia.calnali.2024@gmail.com
Teléfono:	(Teléfono institucional de la Unidad Administrativa) Ejemplo: 7713295347
Funciones:	Ejemplo: Recibir y dar trámite a las solicitudes de derechos ARCO.
Obligaciones:	Ejemplo: Supervisar el correcto resguardo de los datos personales.
Datos personales contenidos en el sistema:	Datos personales: Se refiere a los datos recabados, por ejemplo, para dar trámite a una solicitud de derechos ARCO se requiere: Nombre, Apellido Paterno, Apellido Materno, Domicilio, Teléfono, Correo Electrónico, Firma, Huella, Edad, Estado Civil
Folio del registro en el Sistema personal	Dejar en blanco

Estructura y descripción de los sistemas de datos personales. Versión pública.

Formulario que llenan las áreas generadoras versión pública.

Unidad Administrativa: Unidad de Transparencia	
Nombre del sistema:	Expedientes ARCO
Tipo de Soporte	
Tipo de Soporte:	Se refiere al lugar donde se guardan los documentos que pertenecen a este sistema Ejemplo: Físico y digital
Descripción:	Físico: Expedientes de cada una de las solicitudes de derechos ARCO, las cuales se archivan en un folder tamaño oficio en color beige organizados con número de expediente en forma consecutiva y el año en que fue abierto. Digital: Los expedientes son escaneados en formato PDF, los cuales son identificados con el mismo número que se le asigno al expediente físico. * Hay que adecuarlo a su dirección
Características del lugar donde se resguardan los soportes:	
Físico: Oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación adecuada de los documentos. El mobiliario que contiene los expedientes se encuentra en el área física del área de la Unidad de Transparencia del Ayuntamiento de Calnali. Los expedientes se encuentran alojados en los archiveros los cuales están localizados junto a la puerta que da al exterior, la cual cuenta con protecciones metálicas, en esta área no existe consumo de alimentos, con prevención de plagas para lo cual se coloca veneno y con una temperatura ambiental media. Las oficinas mencionadas permanecen cerradas en días y horas no hábiles. Digital: Se encuentran los expedientes completos en formato digital cargados en Servidor Hosting contratado, el acceso a los equipos de cómputo requiere de contraseña, las cuales solo las posee el personal adscrito a esta dependencia. La Oficina de la Unidad de Transparencia permanece bajo llave misma que permanece cerrada en días y horas no hábiles.	

Anexo 1

Formato A

Formato A

Vulneraciones a los Sistemas de Información y Bases de Datos

Contenido de la bitácora:	Complete el contenido de la bitácora
Fecha del incidente:	
Nombre:	
Cargo:	
Área:	
Responsable del área:	
Causa de la vulneración:	
Sistema de información o base de datos vulnerado	
Cantidad de titulares	
Soporte de la información vulnerada	☐ Físico ☐ Electrónico ☐ Mixto
Seleccione el tipo de vulneración	☐ Perdida o destruccion no autorizada ☐ Robo, extravio o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, alteracion o modificacion no autorizada
Tipo de datos personales comprometidos	☐ Identificativos ☐ Laborales ☐ Transito y Movimientos Migratorios ☐ Academicos ☐ Procedimientos Administrativos o Judiciales ☐ Patrimoniales ☐ Salud ☐ Idelogicos ☐ De origen ☐ Caracteristicas Personales ☐ Vida Sexual

Nombre y firma de quien reporta	Nombre y firma del administrador del sistema	Nombre y firma del titular del area

Anexo 2

Formato B

Formato B

Vulneraciones a los Sistemas de Información y Bases de Datos

Contenido de la bitácora:	Complete el contenido de la bitácora
Fecha del incidente:	
Nombre del responsable de la investigación:	
Cargo:	
Área:	
Numero de investigación:	
La información vulnerada está registrada en el documento de seguridad	☐ Si ☐ No
En caso de que la información no estuviera vulnerada, solicite al responsable del área un informe al respecto con el objeto de responder el contenido del apartado A.	
Apartado A	
Fecha en que se creó el sistema de información o base de datos vulnerada	
Fundamento legal para obtención de los datos personales	
Resguardo de los soportes	
Usuarios	
Medidas de Seguridad físicas técnicas y administrativas aplicadas	
Las causas enunciadas en el formato A	
Lo que el titular del área considere pertinente	
Apartado B	
Administrador del sistema de información o base de datos vulnerados	
Usuarios del sistema de información o base de datos vulnerados	
Los hechos de modo tiempo y lugar enunciados en formato A	
Resguardante soporte físico o electrónico vulnerado	

Anexo 3

Bitácora de Transferencias

Bitácora de Transferencias.

Fecha	Medio	Datos Personales Transferidos	Receptor	Persona que recibe	Autorización

Anexo 4

Plan de contingencia

Plan de contingencia para la protección de la información del Ayuntamiento de Calnali

Clasificación de la contingencia:

Según sea el tipo de la contingencia se le puede asignar un grado de afectación:

Grado 1: Son las más bajas que van desde fallas eléctricas, fallas con la conexión de internet y que pueden ser resueltas por el mismo personal del Sujeto Obligado.

Grado 2: Requiere tanto el apoyo del personal del Sujeto Obligado, así como de personal externo (Por ejemplo, en un incendio apoyo de Bomberos y Protección Civil).

Grado 3: Son contingencias que por su alcance puedan afectar severamente la operatividad del Sujeto Obligado y se requiere además del apoyo externo.

Consideraciones Principales

- Se debe realizar una evaluación de los riesgos
- Dentro de la implementación del plan de contingencia se debe contar con un responsable general quien guiara la implementación del mismo, así como la toma de decisiones.
- Se designe a un encargado de cada área para que apoye en cualquier desastre que ocurra y genere la contingencia, capacitándolos para el manejo de las mismas, como el uso de extintores, planes de evacuación, etc.
- Es necesario hacer las pruebas previas del plan de contingencia para garantizar su funcionalidad en caso de siniestro (las pruebas generalmente se hacen en tiempo real y lo más aproximados a la realidad).
- Reunión con las comisiones o brigadas de las áreas de la Municipalidad (capacitación y evaluaciones)
- Revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.
- Difusión del documento del plan de contingencia una vez aprobado.

Lugar alternativo del trabajo.

En caso de algún desastre mayor (terremoto o incendio) que implique perdidas estructurales se plantea en algunos casos la posibilidad de contar con algún lugar alternativo de trabajo los sitios alternos de trabajo pueden ser: propios de la organización, de una entidad con la que hay acuerdo o reciprocidad, instalaciones alquiladas (se debe contar con presupuesto).

En caso de contar con un ambiente alterno debe contar con los siguientes recursos:

- Mesas para monitores y teclados de los servidores principales
- Sillas
- Switches
- Router para la conexión a internet
- UPS

- Teléfono
- Extinguidor
- Útiles de oficina

Medidas preventivas ante siniestros

Medidas de prevención y conservación de archivos:

- El archivo general debe situarse en el primer piso del edificio (no sótanos).
- Espacios con luz natural y sin humedad.
- Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad.
- Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
- Los estantes de los archivos deben estar entre 10 y 15cmdel suelo (facilitan la limpieza y evitan su vez la acumulación de humedad y proliferación de plagas).
- Todos los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

Medidas preventivas en caso de Incendios.

- Se recomienda tener un conocimiento básico de primeros auxilios.
- Para la pronta detección de un incendio se puede contar con detectores de humo.
- En caso de incendio no abrir puertas y ventanas, el aire es factor para propagación del fuego.
- Si se tienen almacenadas sustancias inflamables como gasolina, acetona, aguarrás, alcohol o tiner, se sugiere colocarlos en lugares ventilados y lejos de las flamas, fuentes de calor y aparatos eléctricos (si no los necesita, deséchelos preferentemente).
- Si el incendio es pequeño, se procurará apagarlo mediante un extintor. Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua.
- No sobrecargar los contactos eléctricos, desconectando los que no se utilicen.

Sobre el resguardo de la información en caso de incendio:

- Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es lugares cercanos a los extintores (sugerencias para realizar el almacenamiento de la información: CD, Disco duro, bases de datos, la nube únicamente si es segura).
- Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de los mismos con resguardo en la nube).

Durante un incendio:

- Ubicar los extintores cerciórese de saber usarlos y que estos sean utilizables.
- Si detecta un incendio procure mantener la calma y repórtelo inmediatamente o presione alguna señal de alarma.
- No abra puertas ni ventanas el fuego se extiende con el aire.
- Si es un incendio que no puede controlar usted mismo llame a los bomberos.
- No pierda tiempo buscando objetos personales y salga del inmueble lo antes posible.
- Si hay gas o humo humedezca un trapo y cubra su nariz y boca.
- Si existe una puerta que deba atravesar toque con precaución la perilla; si esta caliente, no la abra.
- Si su ropa se enciende; tírese al piso y ruede lentamente.

Después del Incendio

Un técnico debe de revisar las instalaciones de gas y electricidad antes de utilizarlas nuevamente.

Terremoto.

El daño ocasionado por un terremoto puede dañar principalmente la estructura del edificio, sin embargo, si los datos almacenados se encuentran en discos duros, cd, USB, al contar con un respaldo de información incluso en la nube se tiene un respaldo inmediato, que permitiría recuperar la información si los otros respaldos físicos se dañaran, para inmediatamente apenas se tenga una conexión a internet y una computadora tener acceso a dichos respaldos.

Medidas preventivas en caso de sismo

- No colocar muebles, equipos o cajas que bloqueen las rutas y salidas de emergencia del archivo.
- Contar con un teléfono celular de emergencia en caso de falla de líneas telefónicas fijas.
- Contar con un plan de evacuación y realizar simulacros de manera cotidiana.
- Tener a la mano una radio de baterías, linterna y los principales documentos personales.
- Contar con un botiquín de primeros auxilios.
- Si se tienen anaqueles, los objetos pesados se colocan al final.
- Localizar los lugares seguros en cada cuarto; bajo mesas sólidas y escritorios resistentes.
- Ubicar los lugares peligrosos: como ventanas donde los vidrios pueden estrellarse, libreros o muebles que podrían caerse en caso de sismo.

Durante un sismo

- Mantener la calma y ubicar en una zona segura.

- Parase bajo un marco de puerta con trabe o de espaldas a un muro de carga.
- Adoptar posición fetal de cara al suelo, abrazándose usted mismo en un rincón, de ser posible protegerse la cabeza.
- Alejarse de ventanas, espejos y objetos de vidrio, así como de objetos colgantes.
- Retirarse de objetos calientes, libreros, gabinetes o muebles pesados.
- Si se está en un edificio evitar el uso de elevadores, si se esta en la calle evitar los postes, arboles, ramas y balcones
- Si es posible cerrar llaves del gas, desconecte la alimentación eléctrica y no encender fuego.

Después del sismo:

- Si usted quedo atrapado, conserve la calma y trate de comunicarse al exterior golpeando un objeto.
- Evite pisar cables que hubieran quedado caídos o sueltos.
- Encienda la radio para mantenerse informado (posibles replicas).
- En caso de visible daño estructural del edificio debe ser evaluado por protección civil para evitar cualquier riesgo secundario.
- Se deben revisar las instalaciones eléctricas y de gas principalmente para evitar un desastre secundario.

Inundaciones por lluvia.

Medidas preventivas en caso de inundación.

- Es importante realizar la revisión y reparación de la hermeticidad de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporada de lluvias esto para evitar goteras.
- Evitar en lo posible colocar expedientes y/o documentos directamente sobre el piso.
- Respetar, al menos, una altura de 10 a 15cm de los archiveros.
- Colocar barreras para el agua (cubrir los documentos con plásticos, cubetas o recipientes para las goteras) en la parte superior de los estantes dentro del local de archivo.
- Evacuar los documentos afectados hacia áreas ventiladas.
- Inmediatamente colocar papel secante en cada hoja de los expedientes.
- Si en un documento se moja en su totalidad se puede realizar la congelación del mismo para su recuperación, debe realizar preferentemente un especialista (restauración).

Durante una inundación:

- Desconectar servicios de luz, gas y agua.
- Mantenerse alejados de árboles y poses de luz.
- Evitar tocar o pisar cables eléctricos
- Cubrir con bolsas de plástico aparatos u objetos que puedan dañarse con el agua.

Después de la inundación:

- Se puede expulsar el agua con una bomba de achique con motor de combustión o eléctrico, si hay suministro eléctrico garantizando en caso emergencia, y si no hubiere, mediante esponjas, baldes, recogedores, etc.
- Cerciorarse de que los aparatos electrónicos estén secos antes de utilizarlos nuevamente
- Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Ventilar las áreas afectadas después de la inundación.

Si los documentos han sufrido daños y se encuentran mojados, se debe seguir el procedimiento de congelación para recuperarlos. A continuación, se describe este procedimiento para recuperar los archivos humedecidos:

1) Se introduce la obra en una bolsa de polietileno con cierre de cremallera o termosellable. Es muy importante envolver el libro en plástico y reducir el volumen de aire para evitar la formación de condensación. Para que la congelación se realice de forma correcta, se debe dejar un amplio espacio entre los libros.
2) La cámara de congelación debe alcanzar una temperatura de -20ºC. En un proceso acelerado de descenso de la temperatura el tratamiento será mas efectivo. La temperatura debe ser constante y el congelador no ha de formar hielo ya que se puede acumular humedad. Se recomienda que en el momento de Aplicación combinada de los tratamientos de congelación y vacío para la desinfección de documentos. Se debe depositar la obra en la cámara de congelación hasta que esta haya alcanzado dicha temperatura, para evitar la aclimatación de los organismos.
3) El tratamiento debe durar como mínimo 72 horas, dependiendo del grosor de la obra y la temperatura del congelador. No obstante, si es necesario, se puede alargar hasta un periodo de tres semanas.
4) La obra se ha de descongelar de forma paulatina sin ser extraída del envoltorio, hasta alcanzar el equilibrio con la temperatura ambiente. Una vez descongelada y alcanzado el equilibrio, el envoltorio se puede retirar.

Robo.

Robo común de equipos:

En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias.

Huelga o manifestaciones:

Si el archivo tiene cerradura, asegúrese que quede bajo llave.

Amenazas informáticas

Medidas preventivas para amenazas informáticas.

Es necesario contar con un inventario actualizado de los equipos de cómputo, impresoras, escáner, fotocopiadoras y tener contacto con proveedores de software, hardware y medios de soporte.

- Prevención de falla de los equipos: se debe procurar dar mantenimiento preventivo por lo menos dos veces al año, y contar con proveedores en caso de que se requiera algún reemplazo inmediato.
- Los equipos pueden quedar dañados por fallas eléctricas, se requiere contar con estabilizadores/reguladores, en cada uno de los equipos principalmente en aquellos que su afectación implique la perdida de información importante.

Hackeo informático:

Ante un evento de hackeo informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:

- Cambiar contraseñas.
- Debe tener al menos ocho caracteres.
- No debe contener información personal como nombre real, nombre de usuario o incluso el nombre del Sujeto Obligado.
- Debe ser muy distinta a tus contraseñas previas.
- No debe contener palabras completas.
- Debe contener caracteres de las cuatro categorías primarias: mayúsculas, minúsculas, números y caracteres especiales.

Mientras se está conectado a Internet el Hacker tendrá acceso a los archivos e información guardados en la computadora hackeada. Por lo que se debe desconectar el cable de la red lo antes posible.

Posteriormente:

- Contactar al personal de soporte para que retire del aire la página.
- Evalué los daños causados: El experto debe evaluar qué información se perdió y cuál es la que se mantiene para restaurar el sitio lo antes posible.

Mantener la misma dirección web.

Cuando la página fue atacada la dirección usualmente no se ve afectada. Lo que generalmente se pierde es la información (textos, videos, fotos, audios) que contenía. Se sugiere restaurar el sitio con la misma dirección, para que los usuarios no se confundan.

Anexo 5

Manual para cifrar documentos

Manual para cifrar documentos.

Como cifrar documentos en Word o Excel.

Contraseña para archivo de Word.

En el caso de Word, tenemos que hacer los siguientes pasos:

- Lo primero es abrir el archivo que queramos proteger.
- Una vez abierto, vamos a Archivo que queramos proteger.
- Proteger documento, Cifrar contraseña.
- Acto seguido nos pide que pongamos una clave dos veces. En cuanto aceptemos, quedara registrada.

Si llegado el momento queremos revertir la situación, es muy sencillo. Para ello hay que seguir los pasos como antes. Una vez estemos en Cifrar contraseña, simplemente tendremos que borrarla y dar clic en aceptar. Nuestro archivo de Word quedara abierto nuevamente.

También podremos hacer que nuestro documento sea solo de lectura, restringir la edición u otorgar permisos solo a ciertos usuarios.

Contraseña para archivo Excel.

Para quienes quieran poner una contraseña a documentos de Excel, el proceso es muy similar:

- Tenemos que abrir el documento e ir a Archivo, Información.
- Una vez aquí dar clic en permisos, proteger libro y cifrar con contraseña.
- Lo mismo que con el documento Word, nos pedirá una clave por dos veces. A partir de aquí nuestro archivo estará cifrado con una contraseña.

Para revertir la situación debemos de realizar el mismo proceso. Borrar la clave que hemos puesto y pulsar en aceptar

Como cifrar un archivo.

El cifrado de archivos ayuda a proteger tus datos mediante su cifrado. Solo una persona que disponga de la clave de cifrado correcta (por ejemplo, una contraseña) puede descifrarlos. El cifrado de archivos no esta disponible en determinados sistemas operativos Windows de forma predeterminada. Quizá sea necesario habilitar el módulo de “disco cifrado”.

Sistemas Windows:

1) Haz clic con el botón derecho en un archivo o carpeta (o mantenlo presionado) y selecciona Propiedades.
2) Selecciona el botón Opciones avanzadas y selecciona la casilla de verificación. Cifrar contenido para proteger datos.

3) Selecciona Aceptar para cerrar la ventana Atributos avanzados, selecciona Aplicar y luego selecciona Aceptar.

Sistemas Linux:

Para cifrar/descifrar archivos individuales rápidamente, solo se ocupa una herramienta gratuita como AESCrypt, la cual viene con una interfaz grafica de modo que no necesitas ser un experto en Linux para utilizarla. Para instalar AESCrypt, se puede descargar el script de instalación o el código fuente de la pagina principal. Sin embargo, para los usuarios de Ubuntu, se recomienda el uso del repositorio PPA no oficial:

$ sudo add-apt-repository ppa: aasche/aescrypt

$ sudo apt-get update

$ sudo apt-get install aescrypt

Para cifrar un archivo, haz click derecho sobre este y selecciona “Abrir con AESCrypt”. Se te pedirá que introduzcas una contraseña. Esto será necesario para descifrar el archivo mas tarde, así que no lo olvides. Cifrar un archivo produce un archivo separado con la extensión AES, manteniendo al archivo original intacto. Siéntete libre de mantener o eliminar el original.

Para descifrar un archivo, haz click en el archivo AES y selecciona “Abrir con AESCrypt”. Introduce la contraseña que se utilizo para cifrar el archivo. Se va a producir una copia idéntica por separado.