Asunto	Disposiciones y medidas generales para la implementación de **las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara.** Revisión de la clasificación de la información como reservada relativa a la información contenida en los **capítulos V, IX y X** de las **Políticas Internas para la Gestión y Tratamiento de Datos Personales**, así como de las secciones denominadas: Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, remitida por la Coordinación de Transparencia y Archivo General de la Universidad de Guadalajara.
Fundamentación	De la determinación de disposiciones y medidas generales para la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara: Artículos 32, párrafo 1, fracción I, 33, 35, 36 y 87, párrafo 1, fracción X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. De la clasificación de la información reservada: Artículo 17, párrafo 1, fracción I, incisos a) y d) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Lineamiento Trigésimo Primero, fracción I, inciso b) y Trigésimo Cuarto de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los sujetos obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

Siendo las 12:00 horas del día 19 de marzo de 2019, en la Secretaría General de la Universidad de Guadalajara, se reunieron los integrantes del Comité de Transparencia de la Universidad de Guadalajara (en adelante Comité), como lo establece el artículo 29, párrafo 1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios (en adelante LTAIPEJM), a convocatoria de su Presidente, con el objeto de celebrar sesión extraordinaria, bajo el siguiente:

Orden del Día:

I. Cómputo de asistencia y en su caso, declaratoria de instalación;
II. Lectura y en su caso aprobación del orden del día;
III. Determinación de disposiciones y medidas generales para la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara, a solicitud de la Coordinación de Transparencia y Archivo General de la Universidad de Guadalajara (en adelante CTAG);
IV. Análisis, estudio, revisión y en su caso **confirmación de la clasificación como información reservada** relativa a la información contenida en los capítulos V, IX y X de las **Políticas Internas para la Gestión y Tratamiento de Datos Personales**, así como de las secciones denominadas: Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, remitida por la CTAG; y

Comite de Transparencia

V. Asuntos varios.

Asuntos y Acuerdos:

I. En el **punto I** del orden del día, el Presidente del Comité, Mtro. José Alfredo Peña Ramos, Secretario General de la Universidad de Guadalajara, hizo constar que se encuentran presentes todos los integrantes del Comité y en consecuencia existe el quórum legal que requiere el artículo 29, párrafo 2 de la LTAIPEJM, por lo que se declara debidamente instalada la sesión; por tanto, los acuerdos que de la misma se formalicen serán legales y válidos.

II. En relación al **punto II** del orden del día, el Presidente puso a consideración de los presentes la propuesta de orden del día, sometiéndose a votación económica y aprobándose por unanimidad de votos de los integrantes del Comité.

III. Luego de ello, con relación al **punto III** en el orden del día, la Mtra. Natalia Mendoza Servín, titular de la CTAG y Secretaria del Comité, solicitó que con fundamento en la atribución establecida en el artículo 87, párrafo 1, fracción X de la LPDPPSOEJM, determine las disposiciones y medidas generales para la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara.

IV. Derivado de lo anterior, con relación al **punto IV** en el orden del día, la Mtra. Natalia Mendoza Servín, titular de la CTAG y Secretaria del Comité, solicitó que con fundamento en la atribución establecida en el artículo 30, párrafo 1, fracción II de la LTAIPEJM, se confirme, modifique o revoque la clasificación de la información remitida por la CTAG.

La revisión de los **puntos III y IV** del orden del día, se realiza en términos de los siguientes:

ANTECEDENTES

PRIMERO. Que el día veintiséis de julio de dos mil diecisiete, se publicó en el Periódico Oficial "El Estado de Jalisco" la LPDPPSOEJM, reglamentaria de los artículos 6° base A y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, así como del artículo 9°, de la Constitución Política del Estado de Jalisco.

Comite de Transparencia

SEGUNDO. Que con fundamento en el Transitorio Primero de la LPDPPSOEJM, dicho ordenamiento legal entró en vigor el mismo día de su publicación en el Periódico Oficial "El Estado de Jalisco".

TERCERO. Los artículos 32, párrafo 1, fracción I y 33 de la LPDPPSOEJM, establecen que los responsables deberán **crear políticas internas para la gestión y tratamiento de los datos personales** y su contenido.

CUARTO. De igual forma, los artículos 35 y 36 de la LPDPPSOEJM, establecen que los responsables **deberán elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo para el tratamiento de los datos personales** y su contenido, y

CONSIDERANDO

A) Respecto a las disposiciones y medidas generales para la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara, es importante hacer énfasis en lo siguiente:

1. Que conforme a lo establecido en los artículos 32, párrafo1, fracción I, 33, 35, 36 y 87, párrafo 1, fracción X, LPDPPSOEJM, el Comité tiene la atribución de determinar las disposiciones y medidas generales para la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara.

2. Que el artículo 32, fracción 1 de la LPDPPSOEJM dispone:

> ***Artículo 32.*** *Deberes – Acciones para el establecimiento y mantenimiento de medidas de seguridad.*
> *1. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes acciones interrelacionadas:*
> *I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*
> *(...).*

3. Que el artículo 33 de la LPDPPSOEJM señala que:

> ***Artículo 33.*** *Deberes – Contenido de las políticas internas de gestión y tratamiento de los datos.*
> *1. Con relación a la fracción I del artículo anterior de la presente Ley, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y tratamiento de los datos personales, al menos, lo siguiente:*
> *I. Los controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales;*

Comite de Transparencia

II. Las acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;
III. Las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales;
IV. El proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;
V. Los controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento, y
VI. Las medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones de esta Ley y demás aplicables.

4. Que el artículo 35 de la LPDPPSOEJM establece que:

Artículo 35. *Deberes – Documento de seguridad.*
1. El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a esta Ley y demás disposiciones aplicables.
2. El documento de seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales.

5. Que el artículo 36 de la LPDPPSOEJM indica que:

Artículo 36. *Deberes – Contenido del documento de seguridad.*
1. El documento de seguridad deberá contener, al menos, lo siguiente:
I. El nombre de los sistemas de tratamiento o base de datos personales;
II. El nombre, cargo y adscripción del administrador de cada sistema de tratamiento y/o base de datos personales;
III. Las funciones y obligaciones de las personas que traten datos personales;
IV. El inventario de los datos personales tratados en cada sistema de tratamiento y/o base de datos personales;
V. La estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan;
VI. Los controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen;
VII. El resguardo de los soportes físicos y/o electrónicos de los datos personales;
VIII. Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales;
IX. El análisis de riesgos;
X. El análisis de brecha;
XI. La gestión de vulneraciones;
XII. Las medidas de seguridad físicas aplicadas a las instalaciones;
XIII. Los controles de identificación y autenticación de usuarios;
XIV. Los procedimientos de respaldo y recuperación de datos personales;
XV. El plan de contingencia;
XVI. Las técnicas utilizadas para la supresión y borrado seguro de los datos personales.
XVII. El plan de trabajo;
XVIII. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y XIX. El programa general de capacitación.

6. Que el artículo 87, párrafo 1, fracción X de la LPDPPSOEJM dispone:

Artículo 87. *Comité de Transparencia – Atribuciones. 1. El Comité de Transparencia tendrá las siguientes atribuciones:*
(…)
X. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones aplicables; y
(…)

Comite de Transparencia

B) Respecto a la clasificación de la información como RESERVADA, es importante hacer énfasis en lo siguiente:

1. Que conforme a lo establecido en artículo 30, párrafo 1, fracción II de la LTAIPEJM, el Comité tiene la atribución de confirmar, modificar o revocar la clasificación de la información pública que realicen los titulares de las áreas del sujeto obligado.

2. Que la CTAG remitió a este Comité la **clasificación como reservada** de la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones denominadas: Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, en el marco de la determinación de disposiciones y medidas generales para la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara.

3. Que en relación con lo anterior, es importante hacer énfasis en que la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones denominadas: Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, debe considerarse como reservada, tomando en consideración lo siguiente:

Comite de Transparencia

El hecho de proporcionar la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones denominadas: Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, tomando en consideración que la estrategia de seguridad de datos personales de la Universidad de Guadalajara está determinada, entre otras cuestiones, por los factores de riesgo y vulnerabilidad de los datos personales en posesión de este sujeto obligado, que de darse a conocer pondrían en riesgo la información confidencial bajo resguardo de esta Casa de Estudios, por lo que dicha información debe clasificarse como información reservada.

4. Que para analizar la procedencia de la clasificación de la información como reservada y en atención a lo previsto por el párrafo 1 del artículo 18 de la LTAIPEJM, el lineamiento Décimo Cuarto de los Lineamientos Generales en Materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios (en adelante Lineamientos de Clasificación) y el Lineamiento Décimo Tercero de los Lineamientos Generales para la Protección de la Información Confidencial y Reservada, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios (en adelante Lineamientos de Protección), este Comité procederá a analizar la prueba de daño que remiten la dependencia, en los términos siguientes:

   - **La información solicitada se encuentra prevista en alguna de las hipótesis de reserva que establece la ley.** La información clasificada se encuentra prevista en el Artículo 17, párrafo 1, fracción I, incisos a) y d) de la LTAIPEJM, en relación con el Lineamiento Trigésimo Primero, fracción I, inciso b) y Trigésimo Cuarto de los Lineamientos de Clasificación.

Comite de Transparencia

- **La divulgación de dicha información atente efectivamente el interés público protegido por la ley, representando un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad estatal.** El hecho de proporcionar la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones denominadas Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan, Resguardo de los soportes físicos y/o electrónicos de los datos personales, Análisis de riesgos, Análisis de brecha, Medidas de seguridad físicas aplicadas a las instalaciones, Controles de identificación y autenticación de usuarios, Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, podría servir de base para que cualquier persona pueda hacer un mal uso de dicha información con fines contrarios a la ley, lo que vulneraría la seguridad de los datos personales en posesión de la Institución, ya que al conocer dicha información, es posible que ésta se utilice para realizar actos delictivos en contra de los titulares de los datos personales. Aunado a ello, de revelarse los planes, procesos, mecanismos, controles, medidas y acciones de seguridad implementados por esta Casa de Estudios para la protección de datos personales, se pudieran diseñar estrategias para evadirlos, ocasionándose una afectación sustancial a la seguridad de los datos personales bajo resguardo de la Universidad de Guadalajara, lo que representaría un perjuicio significativo al interés público.

  Si bien es cierto uno de los aspectos del interés público tutelado por la LTAIPEJM es garantizar el acceso a la información pública a toda persona, también lo es que al revelar o difundir la información susceptible de ser clasificada como reservada, se estaría atentando contra otro de los aspectos de interés público previstos por la LTAIPEJM, por lo que para el caso concreto un aspecto del interés público tutelado por la LTAIPEJM (clasificación de información reservada), funge como límite temporal de otro de los aspectos del interés público tutelados (acceso a la información).

- **El daño o el riesgo de perjuicio que se produciría con la revelación de la información supera el interés público general de conocer la información de referencia.** La revelación de la información pondría en peligro las estrategias legales para la protección de datos personales, toda vez que, el uso que se haga de la misma, puede generar conductas que deriven en actos ilícitos en contra de los titulares de los datos personales y de la propia Universidad. En este contexto es que el derecho de acceso a la información del solicitante, no puede estar por encima de los planes, procesos, mecanismos, controles, medidas y acciones de seguridad implementados por esta Casa de Estudios para la protección de datos personales.

- **La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.** Se considera que reservar la información es proporcional y representa el medio menos restrictivo disponible para evitar un perjuicio, pues como ya se ha señalado, de darse a conocer la información, se pondrían en riesgo los datos personales en posesión de la Universidad al menoscabarse las estrategias legales de seguridad implementadas para su protección.

  Si bien es cierto, se restringe el derecho de acceso a la información del solicitante, al clasificar la información como reservada, es importante reiterar que dicho mecanismo además de estar reconocido en la Constitución Política de los Estados Unidos Mexicanos, se realiza para que no se causen agravios a los titulares de los datos personales, así como a la propia Institución, esto es, la decisión tomada representa el medio menos restrictivo, que el perjuicio que podría causar en caso de divulgarse la información.

  Adicionalmente, conviene señalar que, si bien es cierto, se restringe el derecho de acceso a la información del solicitante, al clasificar la información solicitada como reservada, dicha restricción no es absoluta, tomando en consideración que el solicitante puede realizar cualquier otra solicitud de acceso a la información distinta a la información pública protegida, con independencia de que la clasificación realizada es temporal en términos de la propia LTAIPEJM.

Comité de Transparencia

Cabe señalar que la limitación de otorgar la información solicitada es estrictamente proporcional al riesgo que existe de que la misma sea entregada, toda vez que la medida no impide el ejercicio del derecho de acceso a la información en su totalidad, sino que únicamente respecto de la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones denominadas Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan, Resguardo de los soportes físicos y/o electrónicos de los datos personales, Análisis de riesgos, Análisis de brecha, Medidas de seguridad físicas aplicadas a las instalaciones, Controles de identificación y autenticación de usuarios, Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara.

Con ello, la divulgación de la información reservada generaría:

- **Un daño presente.** Al poner al descubierto la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, afectaría las estrategias legales de seguridad de datos personales adoptadas por la Universidad para prevención de conductas delictivas. Adicionalmente, conforme a lo señalado en la fracción V del párrafo 1 del artículo 26 de la LTAIPEJM, la Universidad de Guadalajara tiene prohibido difundir, distribuir, transferir, publicar o comercializar información reservada, o permitir el acceso de personas no autorizadas, y el incumplimiento de dicha disposición es considerada como infracción administrativa del titular del sujeto obligado en la fracción XII del párrafo 1 del artículo 119 de la LTAIPEJM;

Comité de Transparencia

- **Un daño probable.** El hecho de entregar la información solicitada, podría perjudicar de forma grave, menoscabar y limitar las medidas de seguridad de datos personales implementadas por la Universidad, ya que la información solicitada puede servir para que cualquier persona que pretenda cometer algún acto ilícito, conozca con certeza cuáles son los planes, procesos, mecanismos, controles, medidas y acciones de seguridad de esta Casa de Estudios para evitar la materialización de incidentes que pongan en riesgo los datos personales bajo su resguardo; y;

- **Un daño específico**. El daño específico que se causaría con la entrega de la información, es en detrimento de los titulares de los datos personales en posesión de la Universidad de Guadalajara, así como de las estrategias legales de seguridad de datos personales de la propia Institución.

5. Asimismo, la Primera Sala de la Suprema Corte de Justicia de la Nación en su Tesis Aislada (Constitucional) 1a. VIII/2012 (10a.) publicada en el Semanario Judicial de la Federación y su Gaceta, Libro V, Febrero de 2012, Tomo 1, página 656 establece que el derecho de acceso a la información puede verse limitado en virtud del interés público mediante la clasificación de la información como reservada, derivándose un catálogo genérico y específico de tal tipo de información pública protegida en el que encontramos aquella que expresamente se clasifique como confidencial, reservada, comercial reservada o gubernamental reservada:

Comité de Transparencia

INFORMACIÓN RESERVADA. LÍMITE AL DERECHO DE ACCESO A LA INFORMACIÓN (LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL). *Las fracciones I y II del segundo párrafo del artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, establecen que el derecho de acceso a la información puede limitarse en virtud del interés público y de la vida privada y los datos personales. Dichas fracciones sólo enuncian los fines constitucionalmente válidos o legítimos para establecer limitaciones al citado derecho, sin embargo, ambas remiten a la legislación secundaria para el desarrollo de los supuestos específicos en que procedan las excepciones que busquen proteger los bienes constitucionales enunciados como límites al derecho de acceso a la información. Así, en cumplimiento al mandato constitucional, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental establece dos criterios bajo los cuales la información podrá clasificarse y, con ello, limitar el acceso de los particulares a la misma: el de información confidencial y el de información reservada. En lo que respecta al límite previsto en la Constitución, referente a la protección del interés público, los artículos 13 y 14 de la ley establecieron como criterio de clasificación el de información reservada. El primero de los artículos citados establece un catálogo genérico de lineamientos bajo los cuales deberá reservarse la información, lo cual procederá cuando la difusión de la información pueda: 1) comprometer la seguridad nacional, la seguridad pública o la defensa nacional; 2) menoscabar negociaciones o relaciones internacionales; 3) dañar la estabilidad financiera, económica o monetaria del país; 4) poner en riesgo la vida, seguridad o salud de alguna persona; o 5)* ***causar perjuicio al cumplimiento de las leyes****, prevención o verificación de delitos, impartición de justicia, recaudación de contribuciones, control migratorio o a las estrategias procesales en procedimientos jurisdiccionales, mientras las resoluciones no causen estado. Por otro lado, con un enfoque más preciso que descriptivo, el artículo 14 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental contiene un catálogo ya no genérico, sino específico, de supuestos en los cuales la información también se considerará reservada: 1) la que expresamente se clasifique como confidencial, reservada, comercial reservada o gubernamental reservada; 2) secretos comercial, industrial, fiscal, bancario, fiduciario u otros; 3) averiguaciones previas; 4) expedientes jurisdiccionales que no hayan causado estado; 5) procedimientos de responsabilidad administrativa sin resolución definitiva; o 6) la que contenga opiniones, recomendaciones o puntos de vista de servidores públicos y que formen parte de un proceso deliberativo en el cual aún no se hubiese adoptado una decisión definitiva. Como evidencia el listado anterior, la ley enunció en su artículo 14 supuestos que, si bien pueden clasificarse dentro de los lineamientos genéricos establecidos en el artículo 13, el legislador quiso destacar de modo que no se presentasen dudas respecto a la necesidad de considerarlos como información reservada.*

Amparo en revisión 168/2011. Comisión Mexicana de Defensa y Protección de los Derechos Humanos, A.C. y otra. 30 de noviembre de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

Comite de Transparencia

Ahora bien, por lo que ve al párrafo 1, artículo 19 de la LTAIPEJM, este Comité considera que la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones denominadas: Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, debe conservarse con el carácter de información reservada, por un periodo de cinco años, contados a partir de la fecha de firma de la presente acta.

6. Que este Comité, procedió a revisar la clasificación, la cual se encuentra realizada conforme a los requisitos establecidos por la LTAIPEJM, y considera que se acreditan los supuestos establecidos por el artículo 17, párrafo 1, fracción I, incisos a) y d) de la LTAIPEJM, así como los Lineamientos Trigésimo Primero, fracción I, inciso b) y Trigésimo Cuarto de los Lineamientos de Clasificación, respecto al procedimiento de clasificación de información pública protegida, para lo cual se acuerda confirmar la clasificación.

En razón de lo antes expuesto y en virtud de que no existen más argumentos u opiniones al respecto, con la finalidad de determinar las disposiciones y medidas generales para la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y el Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara y de confirmar la clasificación de la información, el Comité emite los siguientes:

A C U E R D O S:

PRIMERO.- Se **implementan en la Universidad de Guadalajara las Políticas Internas para la Gestión y Tratamiento de Datos Personales**, mismas que se establecen en el documento que como Anexo I se acompaña a la presente acta.

Las Políticas tendrán por objeto establecer y regular los procedimientos internos para la gestión y tratamiento de datos personales en la Red Universitaria, atendiendo a la obligación de esta Casa de Estudio de garantizar la seguridad y el derecho a la protección de datos personales; así como reducir el número de probables vulneraciones a datos personales en posesión de este sujeto obligado.

Comité de Transparencia

SEGUNDO.- Se implementa, en la Universidad de Guadalajara, el Documento de Seguridad para el Tratamiento de Datos Personales, conforme a lo referido en el Anexo I de la presente acta.

El Documento de Seguridad tendrá como objeto establecer y regular las medidas de seguridad de carácter físico, técnico y administrativo, atendiendo a la obligación de esta Casa de Estudio de garantizar la seguridad y el derecho a la protección de datos personales conforme a la Ley y demás disposiciones aplicables.

TERCERO.- Se instruye a la CTAG para que realice las gestiones necesarias para llevar a cabo la implementación de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y del Documento de Seguridad para el Tratamiento de Datos Personales en todas las dependencias de la Red Universitaria, a partir de la firma de la presente acta.

CUARTO.- Para cualquier aclaración o duda respecto a las disposiciones anteriormente señaladas, la entidad responsable será la CTAG.

QUINTO.- Todas las dependencias de la Red Universitaria serán responsables de la correcta observancia de las Políticas Internas para la Gestión y Tratamiento de Datos Personales y del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, por lo que deberán vigilar y garantizar su cumplimiento.

SEXTO.- Se **CONFIRMA LA CLASIFICACIÓN DE LA INFORMACIÓN COMO RESERVADA** relativa a la información contenida en los capítulos V, IX y X de las Políticas Internas para la Gestión y Tratamiento de Datos Personales, así como de las secciones denominadas: Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan; Resguardo de los soportes físicos y/o electrónicos de los datos personales; Análisis de riesgos; Análisis de brecha; Medidas de seguridad físicas aplicadas a las instalaciones; Controles de identificación y autenticación de usuarios; Plan de contingencia y Plan de trabajo del Documento de Seguridad para el Tratamiento de Datos Personales, ambos de la Universidad de Guadalajara, por un periodo de cinco años, contados a partir de la fecha de firma de la presente acta.

SÉPTIMO.- Notifíquese lo acordado al Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.

Comité de Transparencia

V. El Presidente preguntó a los miembros del Comité si había algún asunto no registrado en el orden del día que propongan desahogar, sin embargo no se presentaron asuntos varios.

Luego de lo anteriormente referido, los integrantes del Comité firmaron la presente acta por cuadruplicado y la sesión se declaró concluida a las 14:00 horas del día de su fecha.

"Piensa y Trabaja"
Guadalajara, Jalisco, 19 de marzo de 2019
El Comité de Transparencia de la Universidad de Guadalajara

Mtro. José Alfredo Peña Ramos
Presidente del Comité

Mtra. Ma. Asunción Torres Mercado
Contralora General

Mtra. Natalia Mendoza Servín
Secretaria del Comité

POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE LA UNIVERSIDAD DE GUADALAJARA

Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx

Í N D I C E

Pág.

I. ANTECEDENTES

Primero.- Que el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos señala que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación, cancelación de los mismos, así como a manifestar su oposición al uso de su información personal, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos personales, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Segundo.- Que el veintiséis de enero de dos mil diecisiete, se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante Ley General de Protección de Datos), la cual entró en vigor al día siguiente de su publicación.

Tercero.- Que en términos del artículo 1 de la Ley General de Protección de Datos este ordenamiento tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión del sector público de los tres órganos de gobierno.

Cuarto.- Que el artículo citado en el punto anterior contempla como sujetos obligados a cumplir con la Ley General de Protección de Datos cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal, estatal y municipal.

Quinto.- Que el día veintiséis de julio de dos mil diecisiete se publicó en el Periódico Oficial “El Estado de Jalisco” la Ley de Protección de Datos

Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios (en adelante LPDPPSOEJM); reglamentaria de los artículos 6° base A y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, así como del artículo 9°, de la Constitución Política del Estado de Jalisco.

Sexto.- Que con fundamento en el Transitorio Primero de la LPDPPSOEJM, dicho ordenamiento legal entró en vigor el mismo día de su publicación en el Periódico Oficial “El Estado de Jalisco”.

En virtud de lo anterior y con base en los artículos 32, fracción I y 33, así como demás disposiciones del Título Segundo, Capitulo II de la LPDPPSOEJM, se emiten las políticas internas de la Universidad de Guadalajara para la gestión y tratamiento de datos personales.

II. OBJETIVO

Las presentes políticas tienen por objeto establecer y regular los procedimientos internos para la gestión y tratamiento de datos personales en la Red Universitaria, de conformidad con lo ordenando por los artículos 32, párrafo 1, fracción I y 33 de la LPDPPSOEJM, atendiendo a la obligación de esta Casa de Estudios de garantizar la seguridad y el derecho a la protección de datos personales; así como reducir el número de probables vulneraciones a datos personales en posesión de este sujeto obligado.

Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx

III. DEFINICIONES

Para los efectos de este documento, se tiene por reproducido el contenido del artículo 3° de la LPDPPSOEJM, y se entenderá por:

I. **CTAG:** la Coordinación de Transparencia y Archivo General de la UdeG.
II. **Centros Universitarios:** los Centros Universitarios Temáticos y Regionales.
III. **Dependencias:** los órganos administrativos que conforman la Administración Central, los Centros Universitarios, incluidas las Empresas Universitarias y los Sistemas de la UdeG.
IV. **Enlace:** la persona que haya sido designada por el titular de la dependencia, con el objeto de coadyuvar con la CTAG y cumplir con las obligaciones de transparencia, protección de datos personales y archivos de dicha dependencia.
V. **Políticas:** las políticas internas para la gestión y tratamiento de datos personales de la Universidad de Guadalajara.
VI. **SEMS:** el Sistema de Educación Media Superior.
VII. **SUV:** el Sistema de Universidad Virtual.
VIII. **UdeG:** la Universidad de Guadalajara.

IV. OBLIGACIONES GENERALES PARA LAS DEPENDENCIAS DE LA UDEG

1. **Seleccionar a una persona que se encargue de los aspectos de transparencia, protección de datos personales y archivos.**
   La persona designada, debe dedicarse a las tareas de transparencia, protección de datos personales y archivo.

La persona designada como Enlace, deberá estar en contacto constante con la CTAG, con el fin de atender a las solicitudes de acceso a la información pública, las solicitudes para el ejercicio de los derechos ARCO, así como coadyuvar con la CTAG para la publicación de información fundamental y la gestión documental.

Asimismo, es importante que dicha persona se capacite en la CTAG o a través de algún otro programa que ofrezca la UdeG, otras instituciones de educación o los órganos garantes en materia de transparencia y protección de datos personales.

Finalmente, otro de los factores importantes es seleccionar a una persona con habilidades y capacidades adecuadas, ya que el rol exige atención y conocimientos especializados.

2. **Crear una cultura consciente de la transparencia, así como de la seguridad y la protección de información.**

   Se deberá promover y asistir a las campañas de concientización y sensibilización, así como los foros, conferencias y programas educativos en la materia para lograr este objetivo. La CTAG será la encargada de desarrollar el programa general de capacitación de la UdeG.

3. **Buscar recursos disponibles.**

   La persona que sea designada como Enlace, comenzará a identificar algunos de los recursos tangibles disponibles, tales como presupuesto o personal administrativo a su cargo. Además, otros de los recursos importantes a considerar es identificar las áreas o unidades administrativas de la dependencia que puedan ayudar al Enlace, como las áreas de tecnologías de la información, recursos humanos, de finanzas, de servicios generales, el área jurídica, entre otros.

   También, el Enlace deberá conocer la organización y los procesos internos del flujo de trabajo; así como identificar las tecnologías

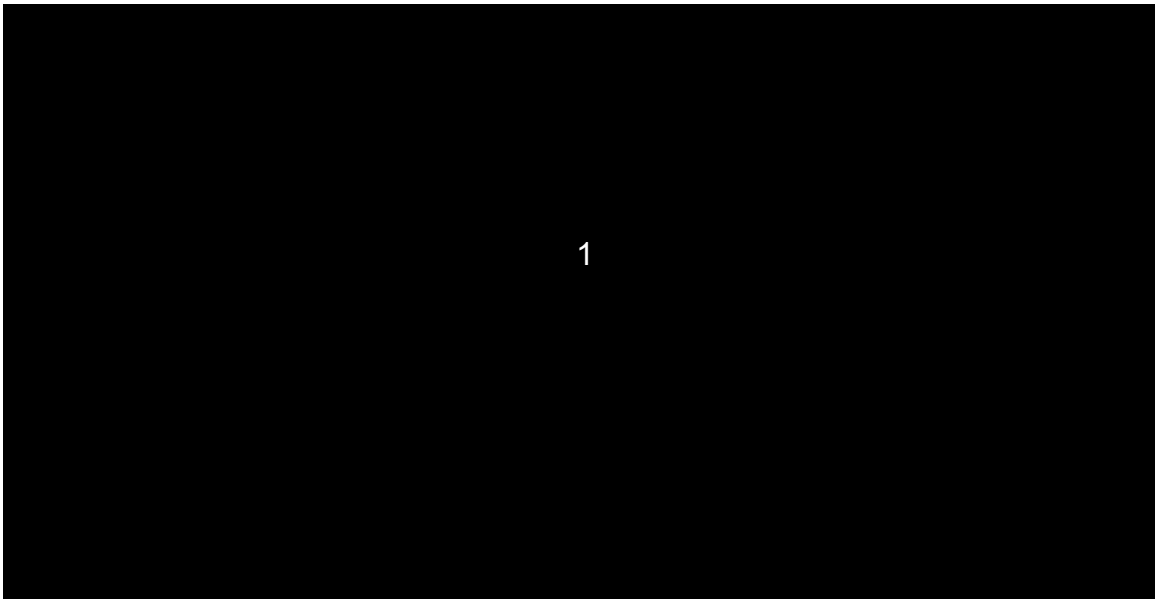
disponibles en la dependencia, las cuales pueden ser plataformas institucionales para compartir archivos, antivirus, y en su caso, plataformas de educación en línea.

4. **Cumplir con las presentes políticas y las normas oficiales en materia de transparencia, de seguridad y protección de información, así como de archivos.**

   El Enlace recabará la documentación legal disponible, tales como las presentes políticas, leyes, reglamentos, lineamientos y demás normatividad aplicable para su estudio.

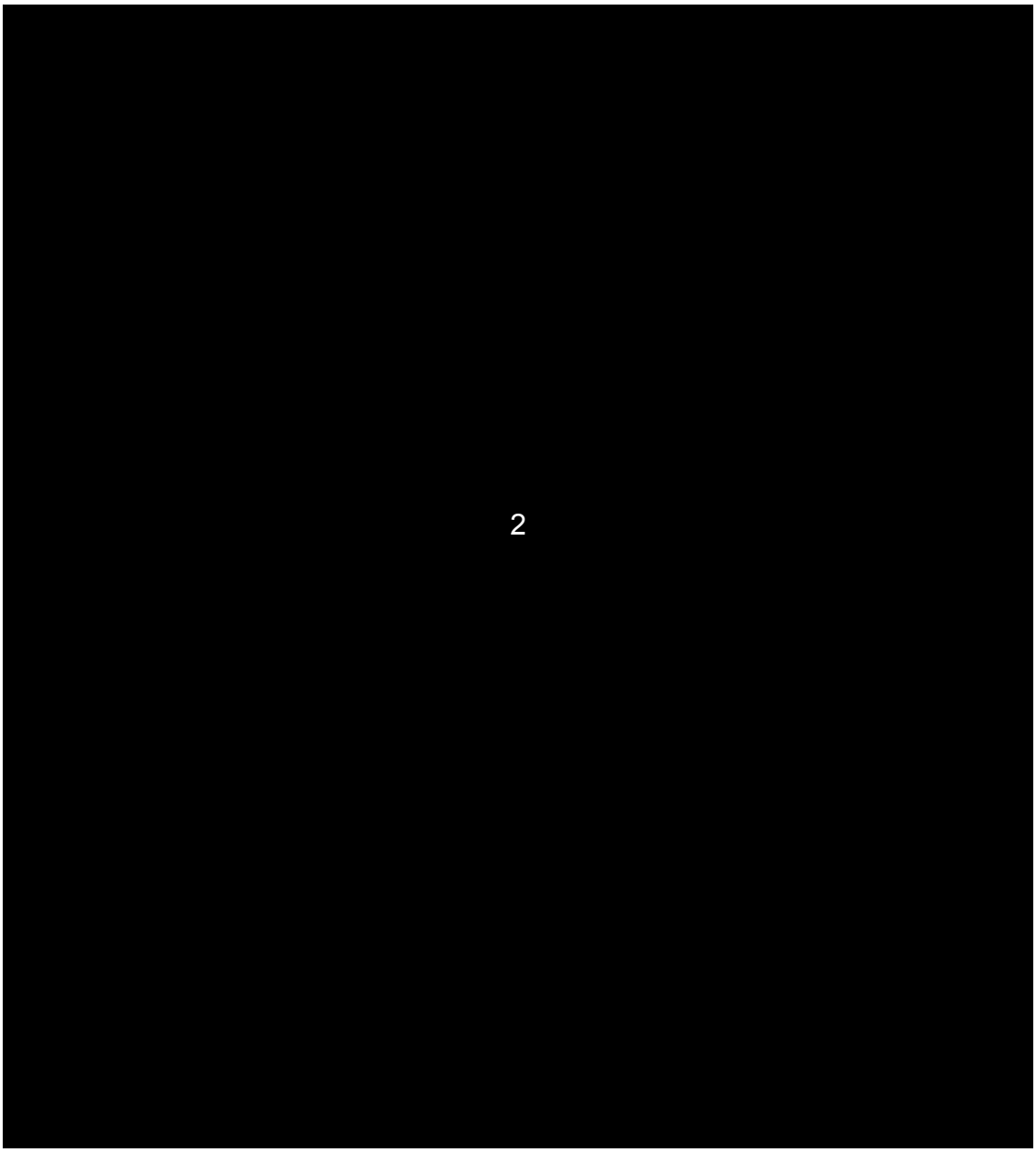
   En caso de duda, el enlace podrá establecer comunicación con la CTAG para que se le oriente en la definición de conceptos, implementación, trámites o demás dudas relacionadas con la normatividad de la materia aplicable a la UdeG.

V. CONTROLES PARA VALIDAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS DATOS PERSONALES



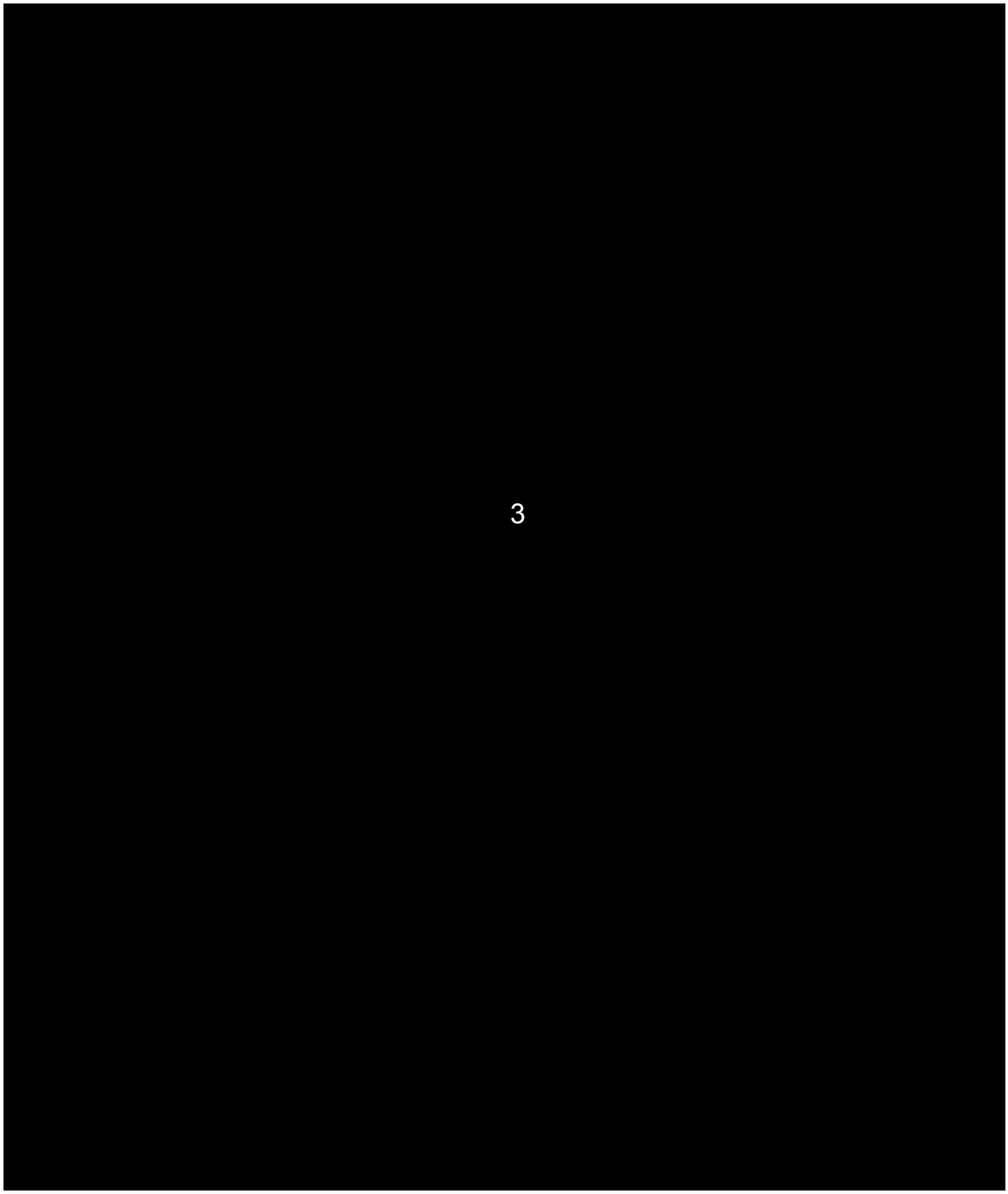
[1] Artículo 3, punto 1, fracción XXVI de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx



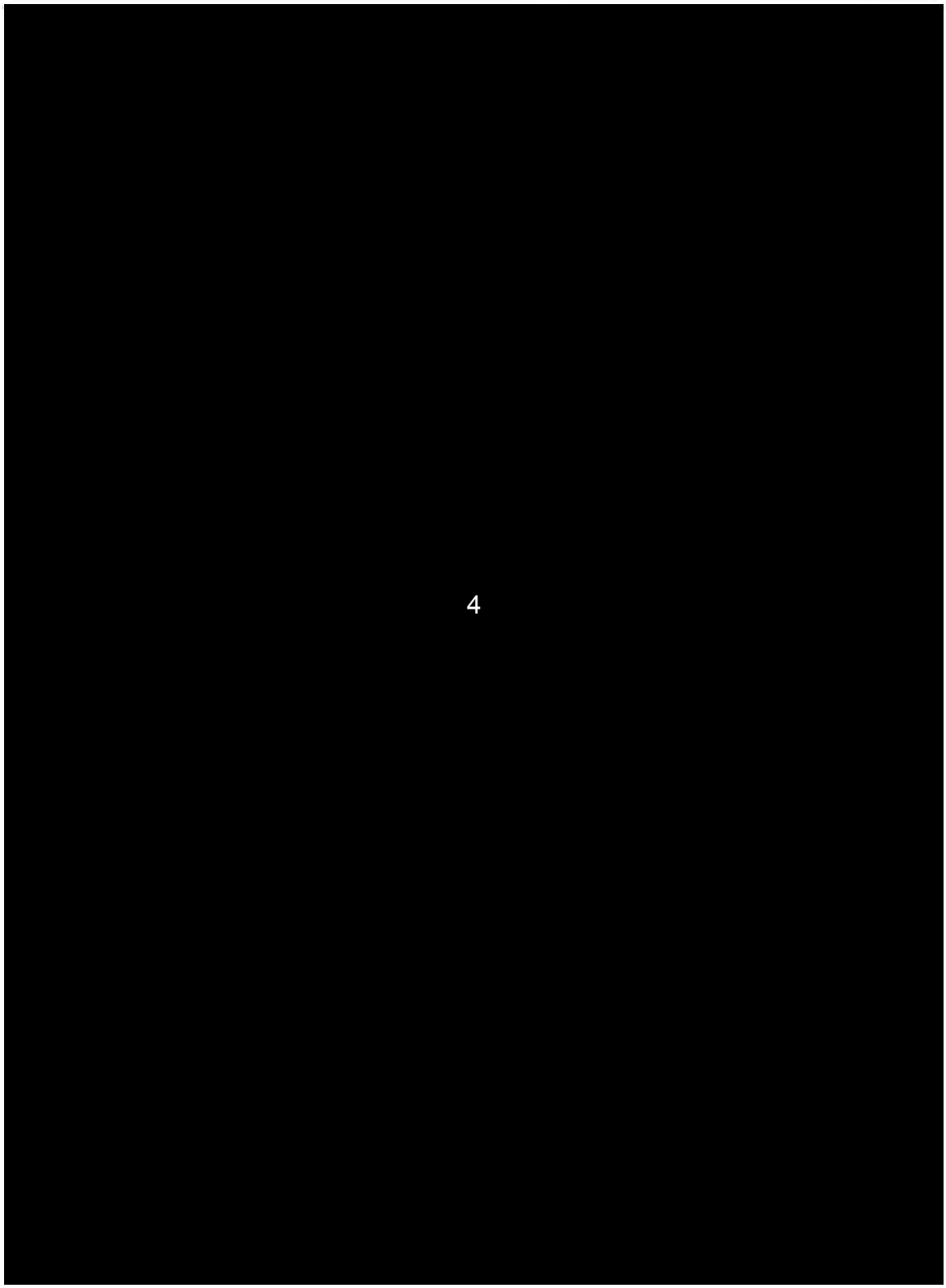
[2] Lineamiento Cuadragésimo Quinto, fracciones I, III, IV, VII y IX de los Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
[3] Artículo 3, punto 1, fracción XXVII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
[4] Lineamiento Cuadragésimo Quinto, fracciones II y V de los Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx

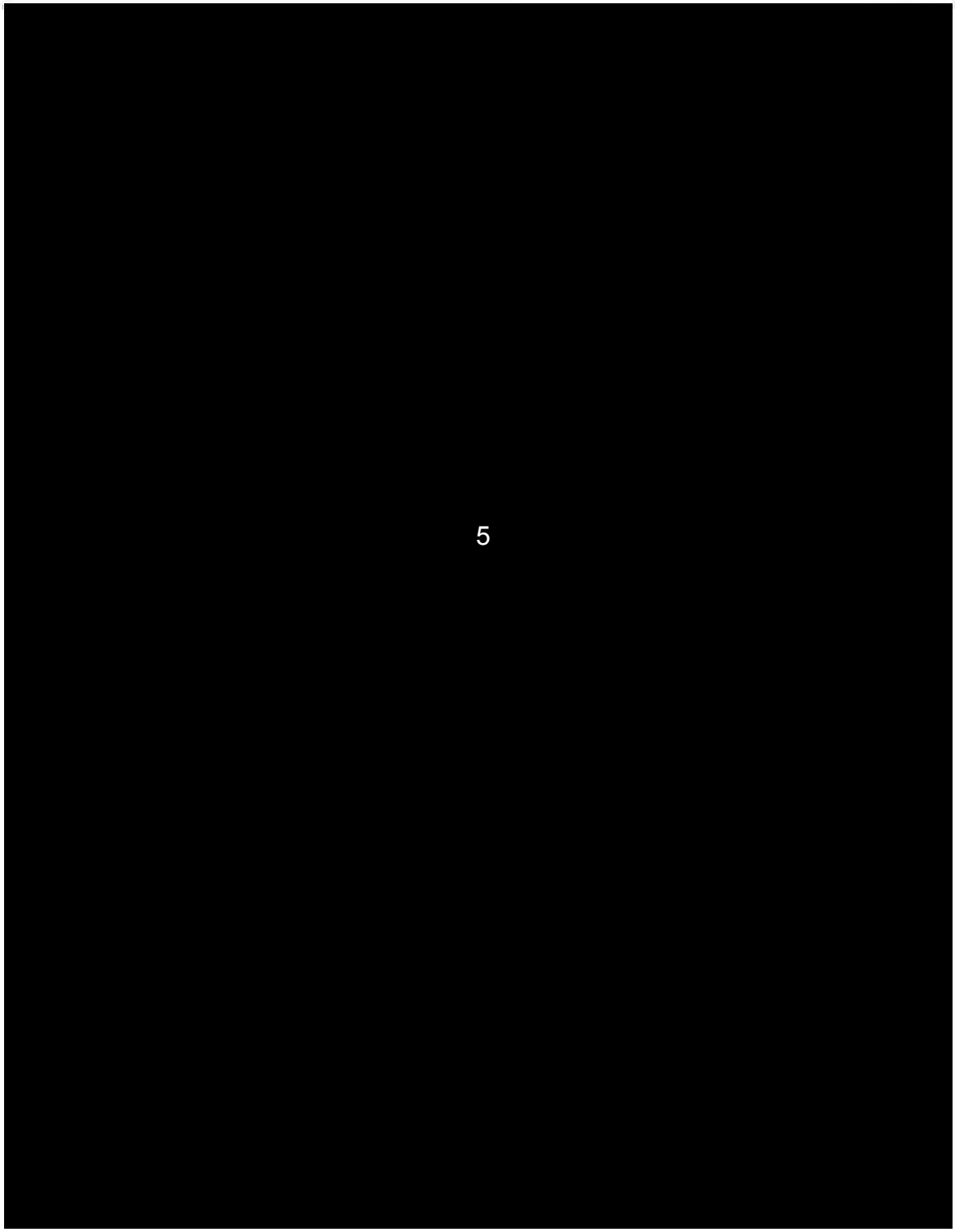


[5] Artículo 3, punto 1, fracción XXVIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
[6] Lineamiento Cuadragésimo Quinto, fracciones VI y VIII de los Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

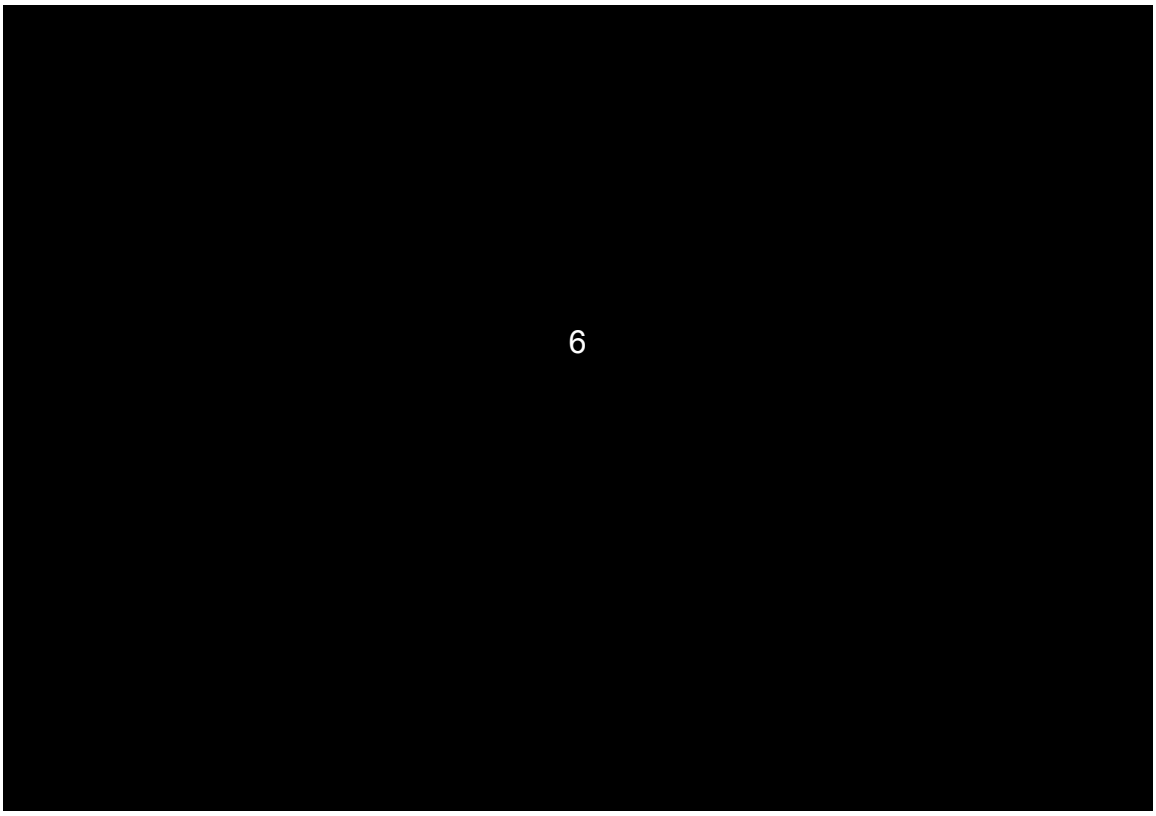
Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx



Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx



[7] Artículos 68 y 69 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.



VI. ACCIONES PARA RESTAURAR LA DISPONIBILIDAD Y EL ACCESO A LOS DATOS PERSONALES DE MANERA OPORTUNA EN CASO DE UN INCIDENTE FÍSICO O TÉCNICO

1. **Seguridad relacionada con respaldos que permitan garantizar la disponibilidad de la información confidencial, cuando se encuentre en medios magnéticos o digitales:** de ser posible, se realizará una digitalización completa de la información confidencial o reservada, única y exclusivamente para su respaldo y almacenamiento en discos duros, asimismo, se realizará un respaldo incremental:

   Una operación de respaldo incremental sólo 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[8].

En virtud de que los respaldos incrementales contienen fecha y hora, tanto inicial como final, la recuperación se realizará cruzando la fecha del incidente y el último respaldo.

Aunado a lo anterior, se tomará en consideración lo siguiente:

a) Se deberá repetir con cierta periodicidad las copias para probar que por un lado, sigue la información disponible, y por otro, para incluir en dichas copias la nueva información que se haya generado; y
b) Se gestionarán programas de capacitación respecto al uso de equipos de cómputo, el uso e instalación de antivirus y actualización del software; pues aunque una de las pérdidas de información más frecuentes es el borrado accidental, también puede ser debido a la acción de algún virus capaz de cifrar o borrar la información. También porque el dispositivo dejó de funcionar.

VII. MEDIDAS CORRECTIVAS EN CASO DE IDENTIFICAR UNA VULNERACIÓN O INCIDENTE

Antes que la dependencia informe a la CTAG sobre una vulneración o incidente, resulta sustancial que se identifiquen una serie de conceptos interrelacionados para tener un mejor contexto de la situación; para ello habrá que definir qué son activos, amenaza, vulneración, riesgo e incidente.

[8] Para más información consulte el Documento de Seguridad para la Protección de Datos Personales del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), pp. 5 y 6.

Un activo es todo elemento de valor para una organización, involucrado en el tratamiento de datos personales, por ejemplo, en el caso de la dependencia podría ser una base de datos de empleados, alumnos, proveedores, los equipos de cómputo, el correo electrónico institucional[9].

Los activos son susceptibles a amenaza, es decir, a factores externos que tienen el potencial de dañarlos, por ejemplo, una descarga eléctrica puede dañar el equipo de cómputo, una persona podría tener acceso a información sin que esté autorizado para ello[10].

Para que una amenaza tenga efecto, requiere explotar una vulnerabilidad, debilidad o falla propia de un activo, por ejemplo, la descarga eléctrica sólo puede afectar a los equipos de cómputo que no tengan un regulador de voltaje. Asimismo, una persona podría acceder sin autorización a una base de datos si ésta no está protegida con una contraseña segura[11].

Finalmente, las amenazas y las vulnerabilidades se combinan para generar riesgos, cuando un riesgo se materializa, ocurre un incidente de seguridad[12].

A continuación se deja una lista explicativa, pero no limitativa de algunos ejemplos de incidentes de seguridad:

Ejemplos de alertas de seguridad	
Categoría	**Ejemplos**
Desastre natural (más allá del control humano)	Terremotos, erupción de un volcán, tsunami, huracán, etc.
Inestabilidad social	Huelgas, terrorismo, guerra.
Daño físico (accidental o deliberado)	Incendio, inundación, malas condiciones ambientales (contaminación, polvo, corrosión, congelamiento), radiación o pulso electromagnético, destrucción parcial o total

[9] Revisar: ITEI (2018). Guía Práctica para Elaborar un Documento de Seguridad. Pág. 22.
[10] Ibídem.
[11] Ibídem.
[12] Ibídem.

Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx

	de medios de almacenamiento físico o electrónico.
Falla técnica	Fallas de hardware, mal funcionamiento del software, sobrecarga o saturación en el uso de los sistemas, falta de mantenimiento.
Software malicioso	Diferentes categorías de software malicioso (malware) como virus, troyanos, software de acceso y control remoto (RAT, por sus siglas en inglés) Ransomware.
Ataques técnicos	Explotación de vulnerabilidades de la configuración, protocolos o programas, normalmente a la fuerza. Escaneo de redes, utilización de puertas traseras en el software, intentos de acceso no autorizado, inferencia de contraseñas, ataques de denegación de servicios.
Incumplimiento de las reglas o políticas (accidental o deliberado)	Uso no autorizado de activos, uso de activos autorizados, pero para finalidades no autorizadas, uso de software, o dispositivos no permitidos, instalación de programas o aplicaciones no autorizadas o ilegales, copia o sustracción de documentos o información no autorizada.
Información dañada	Sobre escritura accidental, error de captura o almacenamiento.
Intercepción de información	Espionaje, intervención de comunicaciones, ingeniería social, robo, pérdida o extravío de información.
Divulgación de contenido perjudicial	Difusión en medios masivos de comunicación de contenido ilegal, malicioso, abusivo o que pueda dañar los derechos morales o patrimoniales de las personas.

Tabla (ITEI, 2018. Guía Práctica para la Elaborar un Documento de Seguridad, pp. 23 y 24).

En relación con lo anterior, resulta importante además tomar en consideración las vulneraciones de seguridad, las cuales pueden consistir en:

a) La pérdida o destrucción no autorizada de la información;
b) El robo, extravío o copia no autorizada de la información;
c) El uso, acceso o tratamiento no autorizado de la información; y,

d) El daño, la alteración o modificación no autorizada de la información[13].

Una vez identificado lo anterior, la dependencia a través de su titular deberá generar una bitácora que contendrá al menos lo siguiente:

1. La fecha en la que ocurrió la vulneración;
2. El motivo de la vulneración. Por ejemplo, archivos dañados por humedad; y,
3. Las acciones correctivas implementadas de forma inmediata y definitiva. Por ejemplo, en el caso de la inundación, recuperar el acervo documental, separar las hojas con el debido cuidado, dejar secar bajo la sombra utilizando ventiladores que no generen humedad.[14]

Además, se deberá notificar a la CTAG a más tardar el día hábil siguiente de que se cometa una vulneración o incidente, señalando lo siguiente:

1. La naturaleza del incidente. Por ejemplo, desastre natural, concerniente a una inundación;
2. Los datos personales comprometidos. Por ejemplo, identificativos, concernientes a nombres, domicilios, teléfonos particulares, etc.;
3. Las recomendaciones y medidas que el titular de los datos personales puede adoptar para proteger sus intereses;
4. Las acciones correctivas realizadas de forma inmediata; y,
5. Los medios donde el titular de los datos personales puede obtener más información al respecto.[15]

[13] Artículo 38 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
[14] Artículo 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
[15] Artículo 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx

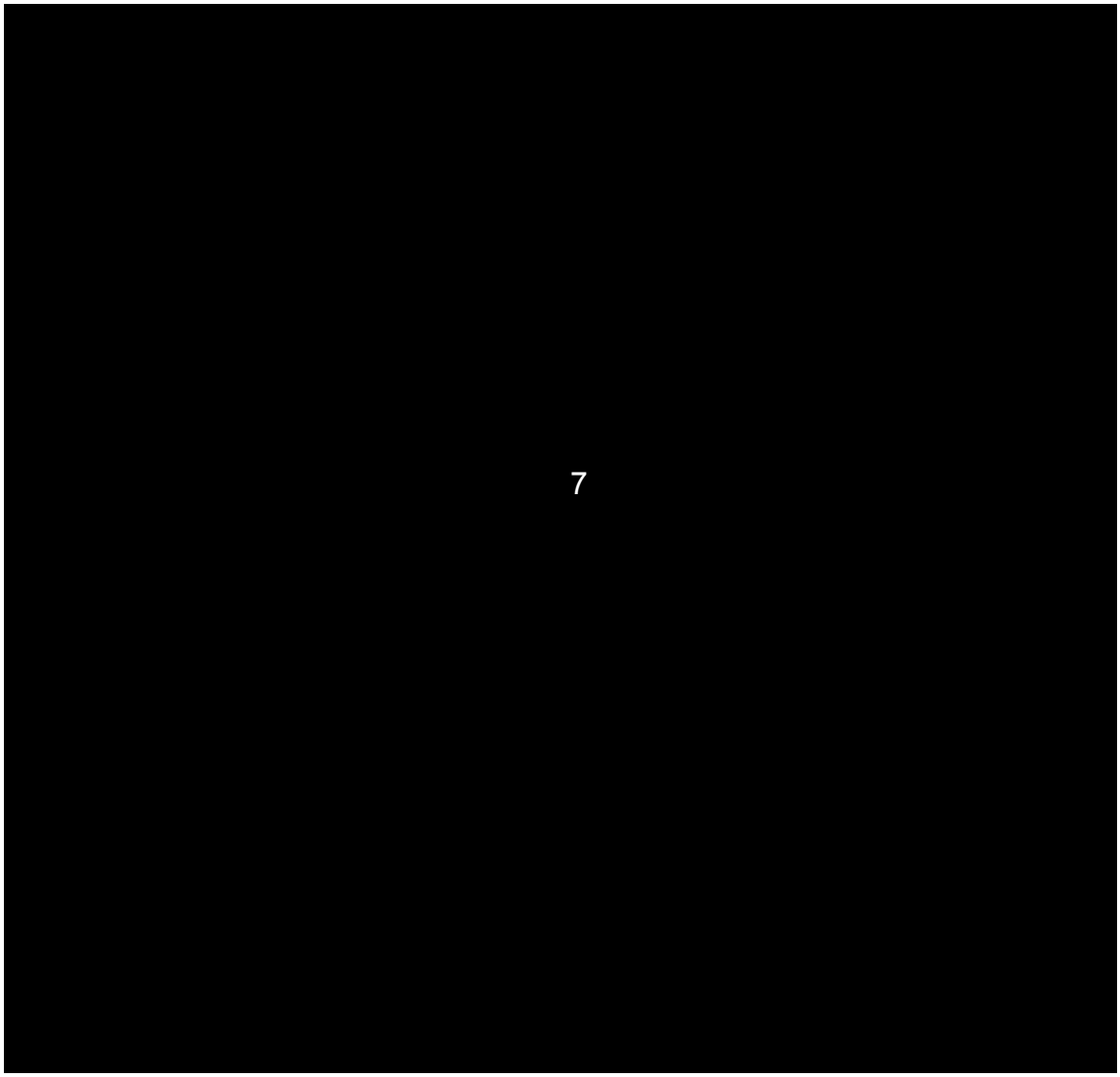
Cuando ocurre una vulneración a la seguridad de los datos personales, el Enlace en coordinación con la CTAG y el titular de la dependencia deberán analizar las causas por las cuales se presentó e implementar un plan de trabajo, identificando las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, si fuera el caso, a efecto de evitar que la vulneración se repita. Por ejemplo, resguardar los documentos en cajas de plástico, colocarlas en lugares altos para evitar que se vuelvan a dañar o incluso mudarlos de lugar a un piso alto.

VIII. PROCESO PARA EVALUAR PERIÓDICAMENTE LAS POLÍTICAS, A EFECTO DE MANTENER SU EFICACIA

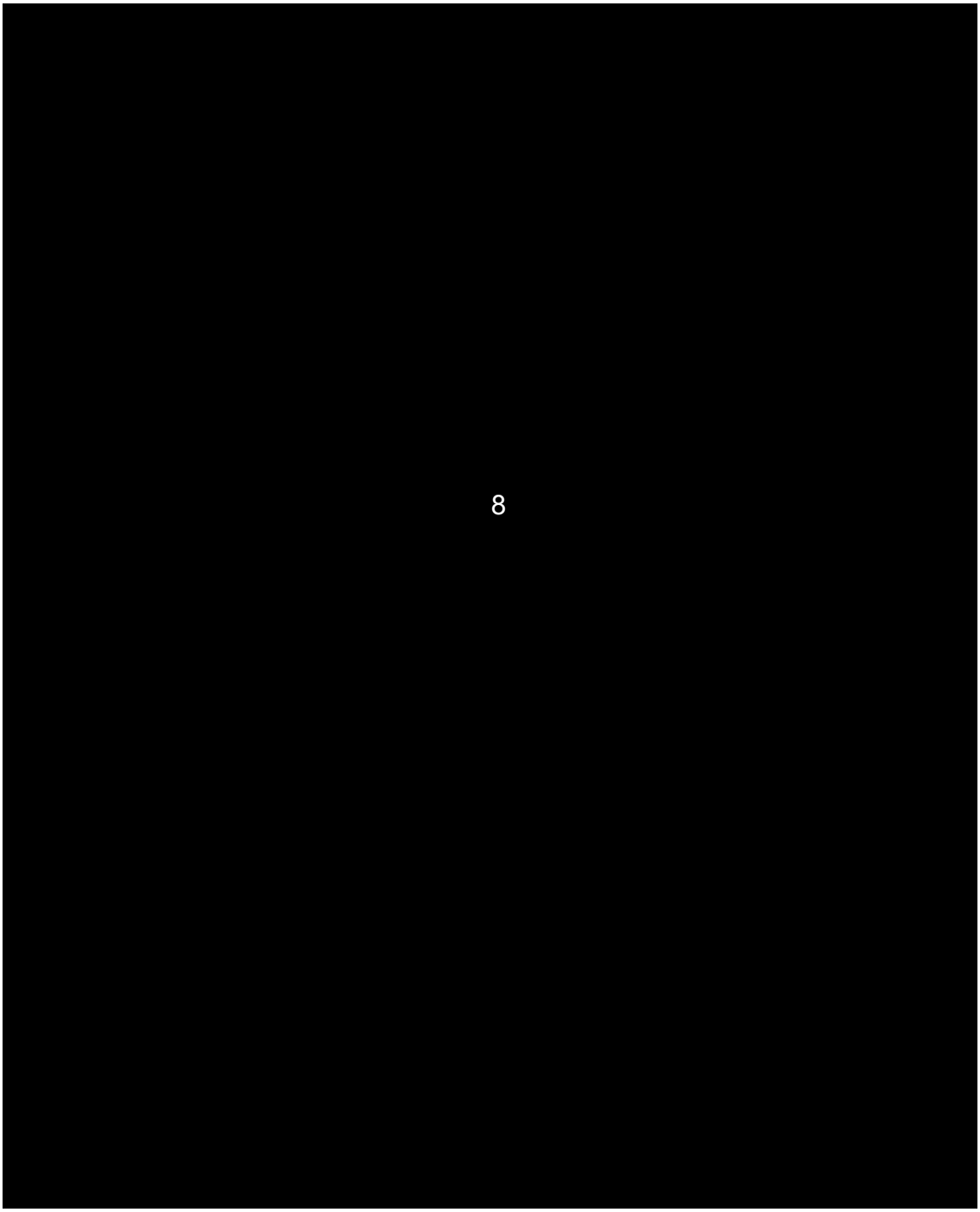
1. **Plan de capacitación:** la CTAG desarrollará el programa general de capacitación a fin de crear campañas de concientización, sensibilización y educación respecto a la implementación de las presentes Políticas, así como demás normativa en materia de seguridad y protección de la información.
2. **Distribución de responsabilidades:** el Enlace de transparencia deberá coordinarse con el personal administrativo y académico de su dependencia a fin de revisar las leyes, reglamentos y estatutos internos para comenzar a identificar las funciones y atribuciones que le corresponden a cada área o unidad administrativa, y con base en lo anterior, se comience a delegar y distribuir responsabilidades con la finalidad de implementar las presentes Políticas.
3. **Mecanismos de monitoreo y revisión de las presentes políticas:** el enlace de transparencia de cada dependencia deberá revisar periódicamente que esté resultando positiva la implementación de la normativa interna en materia de protección de datos personales y seguridad de la información.

4. **Verificación del cumplimiento:** en relación con el punto anterior, el enlace de transparencia verificará que se estén cumpliendo los objetivos y propósitos de las normativas en materia de protección de datos.
5. **Responsabilidades:** en su caso, se determinarán las acciones que se estimen pertinentes para el mejoramiento de las medidas de seguridad.

IX. CONTROLES PARA GARANTIZAR QUE ÚNICAMENTE EL PERSONAL AUTORIZADO PODRÁ TENER ACCESO A LOS DATOS PERSONALES

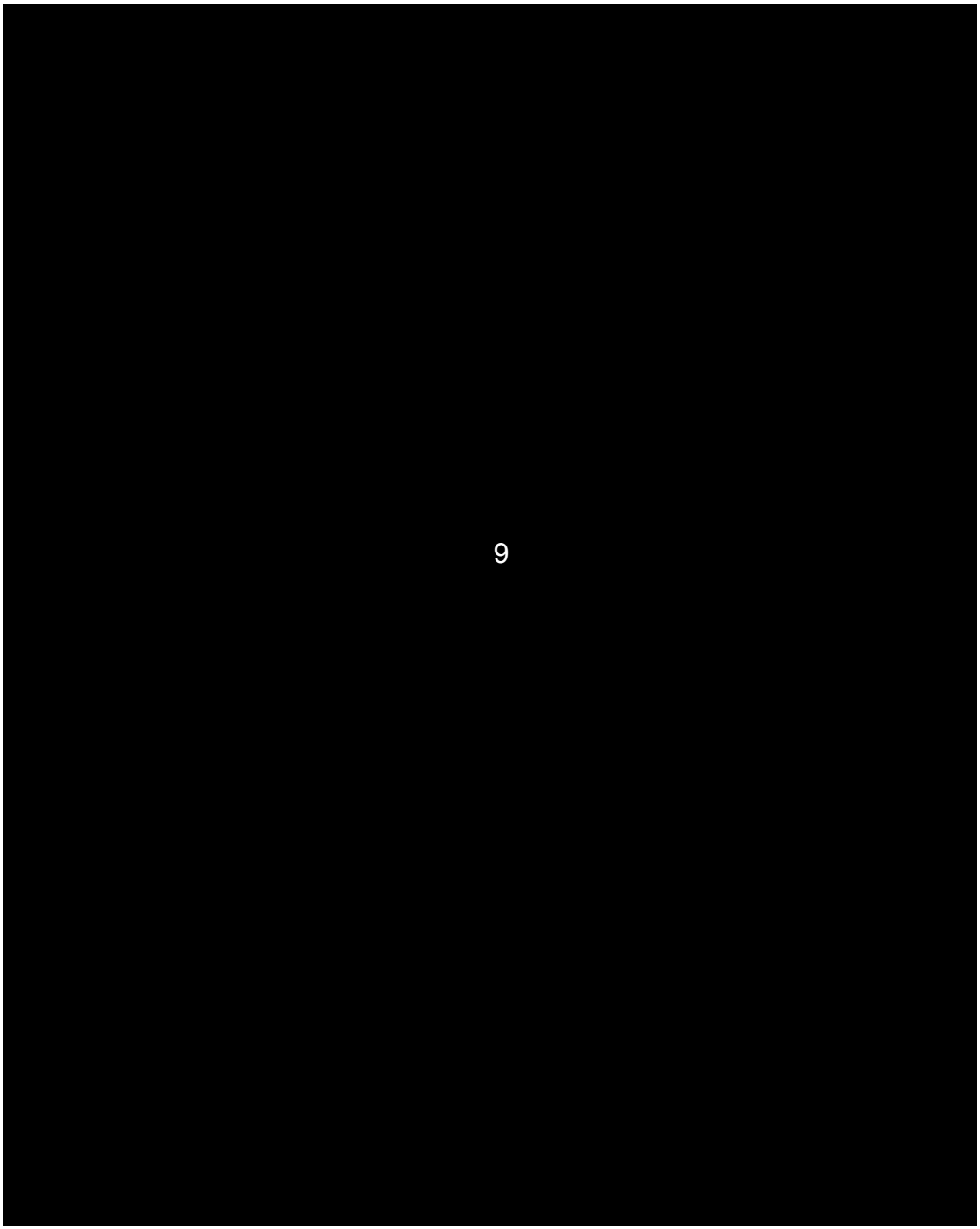


Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx

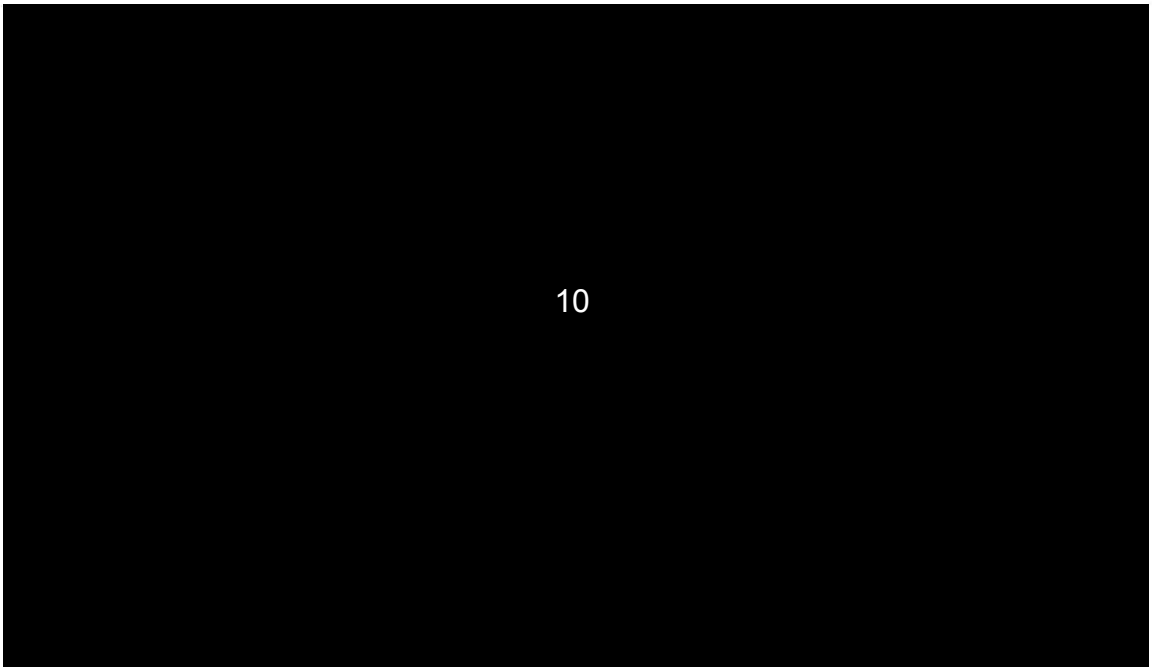


[16] Artículo 3, punto 1, fracción XXXI de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
[17] Artículo 3, punto 1, fracción XXXVI de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

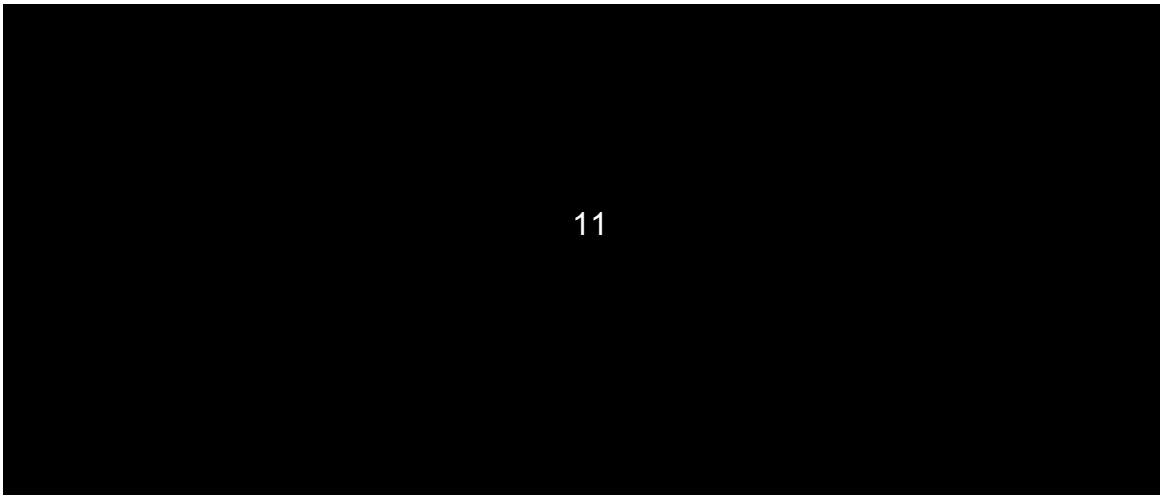
Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx



[18] Lineamientos Cuadragésimo Segundo y Cuadragésimo Tercero de los Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán observar los sujetos obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

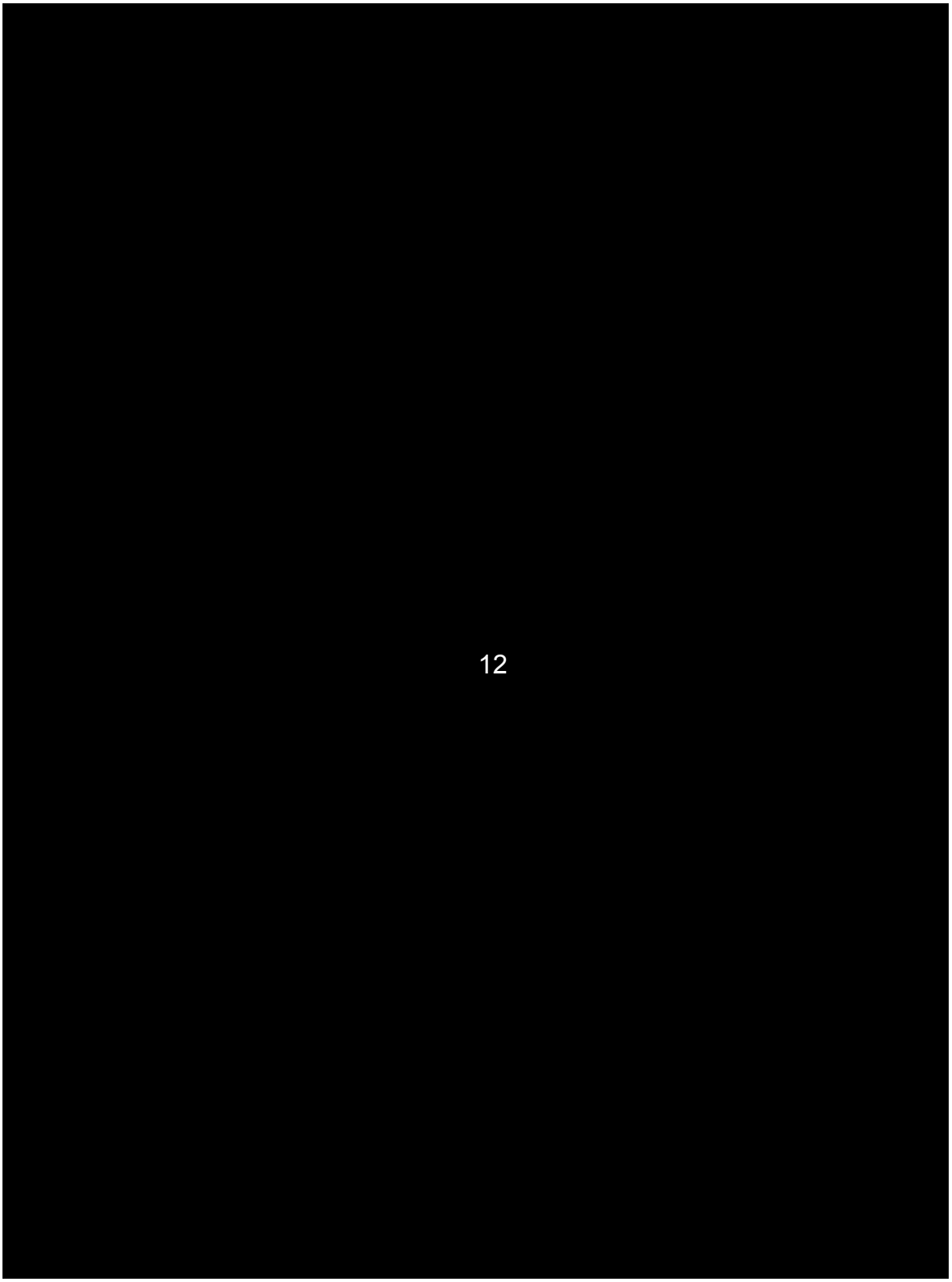


X. MEDIDAS PREVENTIVAS PARA PROTEGER LOS DATOS PERSONALES CONTRA SU DESTRUCCIÓN ACCIDENTAL O ILÍCITA, SU PÉRDIDA O ALTERACIÓN Y EL ALMACENAMIENTO, TRATAMIENTO, ACCESO O TRANSFERENCIAS NO AUTORIZADAS O ACCIONES QUE CONTRAVENGAN LAS DISPOSICIONES DE LA LEY

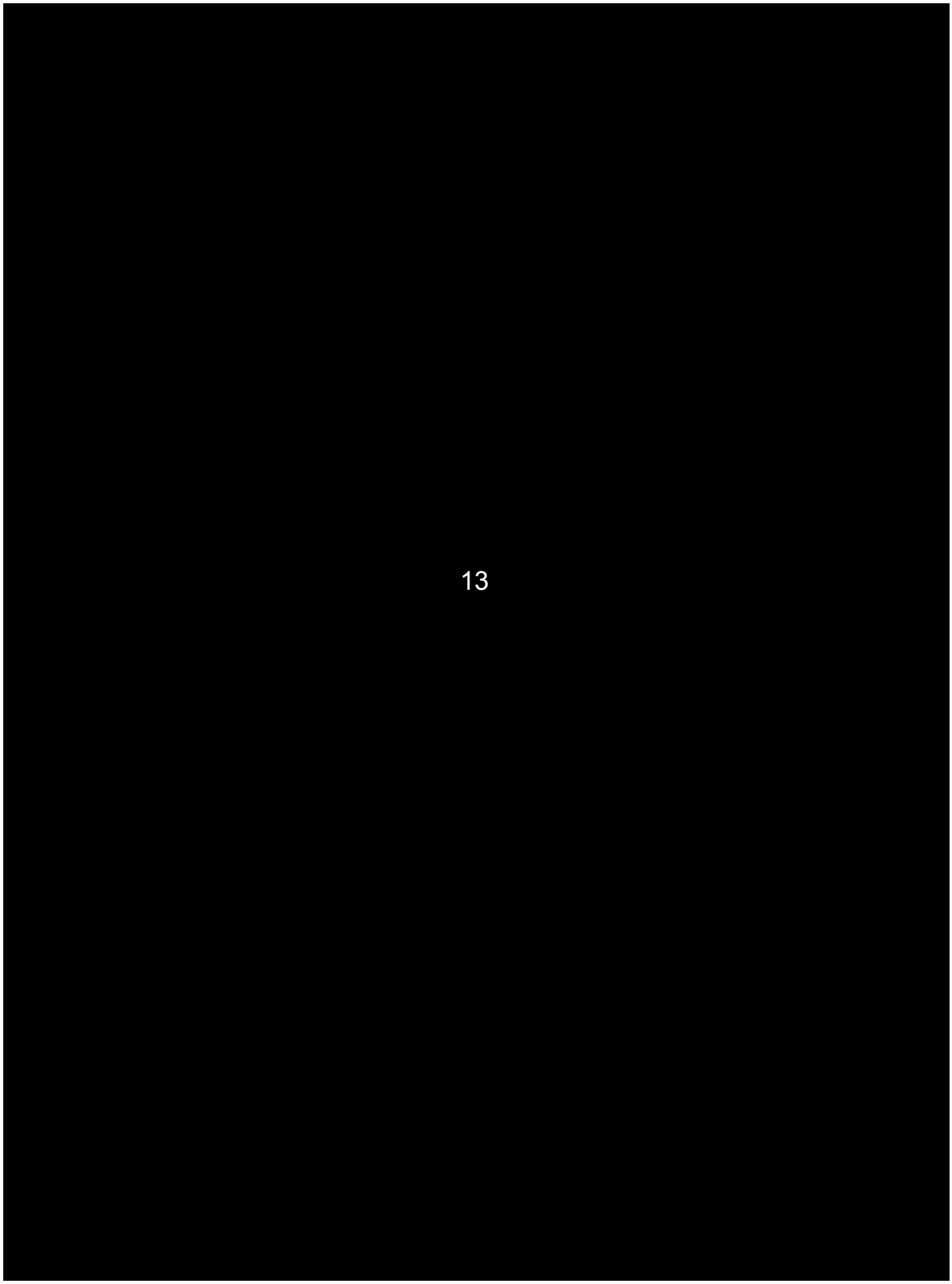


[19] Lineamiento Cuadragésimo Cuarto de los Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán observar los sujetos obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

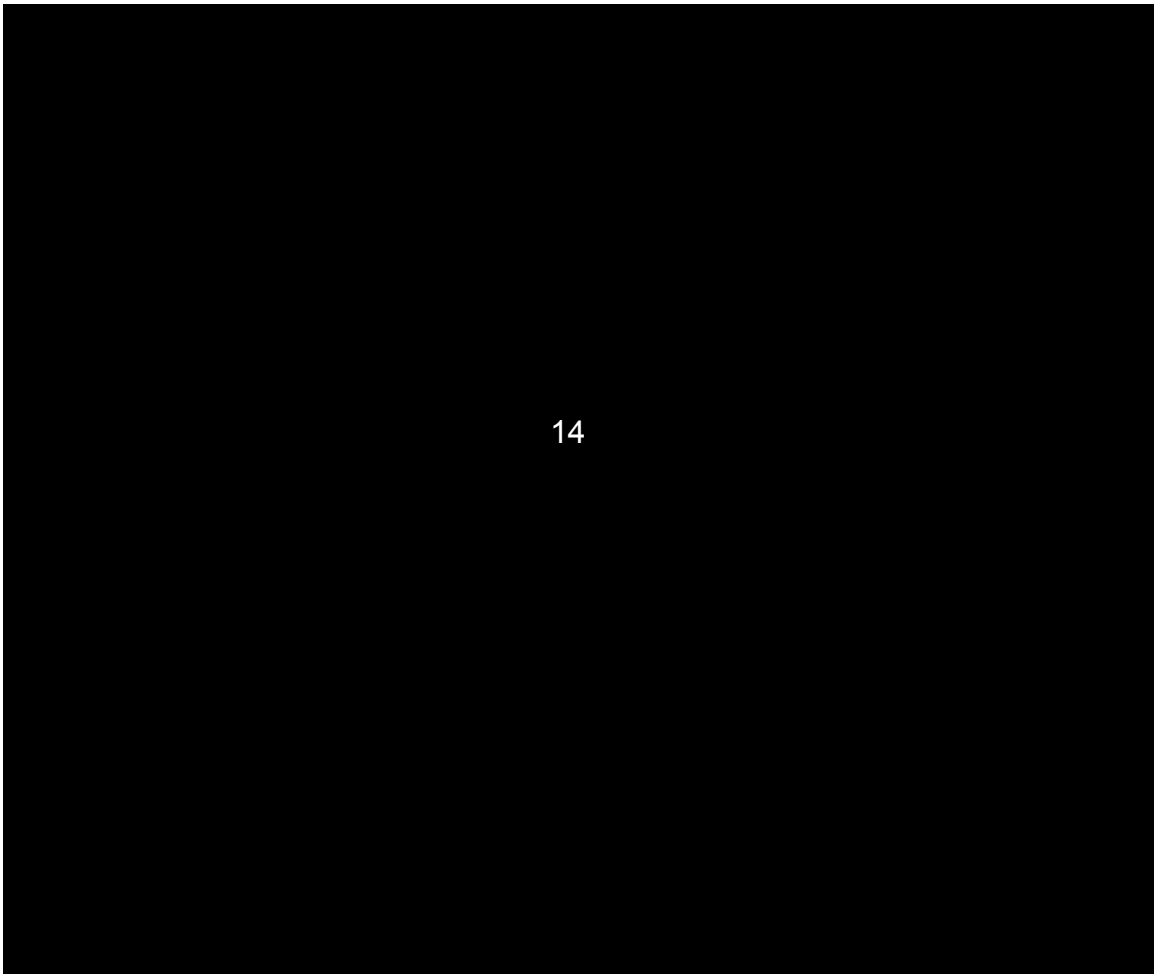
Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx



Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx



Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx



Finalmente, se hace del conocimiento de la comunidad universitaria que la CTAG está para acompañarlos en este proceso y dar cumplimiento a las nuevas disposiciones normativas.

XI. REFERENCIAS

Congreso de la Unión. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en:

http://www.transparencia.udg.mx/sites/default/files/Ley%20General%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20en%20Posesi%C3%B3n%20de%20Sujetos%20Obligados.pdf

Congreso del Estado de Jalisco. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. Disponible en:

http://www.transparencia.udg.mx/sites/default/files/Ley%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20en%20Posesi%C3%B3n%20de%20Sujetos%20Obligados%20del%20Estado%20de%20Jalisco%20y%20sus%20Municipios.pdf

INAI. (2015) Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales:

http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

ITEI. (2018). Guía para elaborar un Documento de Seguridad. Disponible en:

http://www.itei.org.mx/v3/documentos/guias/guia_documento_seguridad_so_31082018.pdf

NYMITY. (2015). Estudio sobre responsabilidad demostrada (Accountability). Maximice la eficacia de su programa de protección de datos con base en los recursos disponibles. Disponible en:

https://latam.nymity.com/~/media/NymityAura/Resources/LATAM%20Website/Alcanzar%20est%C3%A1ndares%20de%20responsabilidad%20demostrada%20-%20Sept%2018%20-%20Espa%C3%B1ol.pdf

OEA. (2018). Oportunidades y desafíos para las PYMES en el contexto de una mayor adopción de las TIC. Disponible en:

http://www.oas.org/es/sms/cicte/docs/white-papers/ESP_Digital_-_white_paper_3.pdf

Secretaría de la Función Pública. (2016). Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias. Disponible en:

http://dof.gob.mx/nota_detalle.php?codigo=5532585&fecha=23/07/2018

Maillo Fernández, Juan Andrés. (2017). Sistemas Seguros de Acceso y Transmisión de Datos; Editorial Ra-Ma.

Pedro Moreno 834, Col. Centro, C.P 44100
Guadalajara, Jalisco, México, Teléfonos [52] (33) 3134-2200, extensión 12470
www.transparencia.udg mx

JUSTIFICACIÓN DE LA VERSIÓN PÚBLICA DE LAS POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE LA UNIVERSIDAD DE GUADALAJARA

1. Eliminados tres párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
2. Eliminados nueve párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
3. Eliminados cinco renglones y cinco párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
4. Eliminados nueve párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
5. Eliminados seis párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
6. Eliminados tres renglones y tres párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
7. Eliminados seis párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
8. Eliminados dos renglones y cinco párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

9. Eliminados ocho renglones y cuatro párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
10. Eliminados dos renglones y tres párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
11. Eliminado un párrafo con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
12. Eliminados catorce párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
13. Eliminados cinco párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
14. Eliminados dos renglones y tres párrafos con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

Documento de Seguridad para el Tratamiento de Datos Personales de la Universidad de Guadalajara

Nombre de los sistemas de tratamiento o base de datos personales	La información puede consultarse en el sistema PROINFO de la Universidad de Guadalajara: http://www.transparencia.udg.mx/proinfo
Nombre del administrador de cada sistema de tratamiento y/o base de datos personales	La información puede consultarse en el sistema PROINFO de la Universidad de Guadalajara: http://www.transparencia.udg.mx/proinfo
Funciones y obligaciones de las personas que traten datos personales	El personal administrativo y académico que en ejercicio de sus atribuciones o funciones traten datos personales, deberán guardar la confidencialidad, autorizar los accesos, llevar el control de las bitácoras de acceso y vigilar que se cumplan las medidas de seguridad administrativas, físicas y técnicas.
Inventario de los datos personales tratados en cada sistema de tratamiento y/o base de datos personales	La información puede consultarse en el sistema PROINFO de la Universidad de Guadalajara: http://www.transparencia.udg.mx/proinfo
Estructura y descripción de los sistemas de	1. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan	[redacted] 2. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
Controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen	a) Se le informará a quien recibe la información de las medidas de seguridad o en su caso, otras que se consideren pertinentes, con la finalidad de no afectar la confidencialidad de la información; b) Se incluirá una carátula al inicio del documento, con una nota relativa al tipo de información que contiene, así como el nombre y cargo del destinatario; c) En el caso de un documento electrónico se deberá remitir en un formato de archivo que no permita la edición o

	manipulación y deberá estar protegido de origen contra impresión o copiado no autorizado, parcial o total, de su contenido; d) Se implementarán mecanismos que aseguren que la información únicamente será tratada por el destinatario autorizado que la reciba, dichos mecanismos son los siguientes: si se van a enviar documentos físicos o documentos electrónicos contenidos en soporte físico, se colocarán dentro de un sobre cerrado y sellado y la persona que reciba en el acuse, se pedirá que coloque una nota que diga: “recibí sobre cerrado e inviolado”; cuando se trate de documentos electrónicos, éstos se cifrarán y se enviará una contraseña que permitirá acceder al documento en un primer correo, inmediatamente después se enviará el correo con el documento que contiene la información protegida. e) Se comunicará a los destinatarios sobre la responsabilidad que éstos adquieren al recibir la información protegida, se adjuntará el Aviso de Privacidad de la UdeG a efecto de hacerle saber al destinatario las políticas de privacidad de esta Casa de Estudios; y f) El traslado de la información será a cargo de trabajadores de la UdeG autorizados por su superior jerárquico y preferentemente con oficio de comisión.
Resguardo de los soportes físicos y/o electrónicos de los datos personales	3. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

personales	[redacted] 4. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
Bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	En las bitácoras de acceso se deberá registrar la siguiente información: I. Datos de quien accede: a) Nombre y cargo; b) Propósito de acceso; c) Fecha de acceso; y, d) Fecha de devolución. II. Respecto a las operaciones cotidianas, las actividades consistirán, en lo siguiente: a) Cada dependencia deberá contar con un enlace que conocerá de los temas de transparencia, protección de datos personales y archivos; b) Dicho enlace de transparencia creará y mantendrá una cultura consciente de la protección de datos personales y

	archivos en su dependencia; c) El enlace de transparencia buscará mejoras de recursos, tales como recursos materiales y humanos; y, d) Cada dependencia deberá cumplir con la normatividad y las políticas en materia de protección de datos personales. III. Respecto a las vulneraciones de los datos personales, la bitácora contendrá, lo siguiente: a) Nombre de quién reporta el incidente; b) Cargo; c) La fecha en la que ocurrió; d) El motivo de la vulneración de seguridad; y e) Las acciones correctivas implementadas de forma inmediata y definitiva.
Análisis de riesgos	5. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
Análisis de brecha	6. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

	7. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

Gestión de vulneraciones	Al identificarse un incidente de seguridad, deberán realizarse las siguientes acciones de manera interrelacionadas: 1. Identificar el incidente. 2. Identificar los datos personales comprometidos. 3. Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 4. En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes. 5. Determinación de la magnitud de la afectación, proponer las recomendaciones para los titulares y hacerlas llegar a la Coordinación de Transparencia y Archivo General de esta Casa de Estudios. 6. Elaborar un informe y propuesta de medidas correctivas a corto y mediano plazo y enviarlas a la Coordinación de Transparencia y Archivo General de esta Casa de Estudios; 7. Notificar a la Coordinación de Transparencia y Archivo General a más tardar al día hábil siguiente de ocurrido el incidente. 8. Llenar la bitácora de vulneraciones conforme al artículo 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. La bitácora deberá contener, lo siguiente: a) Nombre de quién reporta el incidente; b) Cargo; c) La fecha en la que ocurrió;

	d) El motivo de la vulneración de seguridad; y e) Las acciones correctivas implementadas de forma inmediata y definitiva.
Medidas de seguridad físicas aplicadas a las instalaciones	[redacted] 8. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

	[redacted]
Controles de identificación y autenticación de usuarios	9. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
Procedimientos de respaldo y recuperación de datos personales	Se llevará a cabo un procedimiento de digitalización completa de la información protegida, única y exclusivamente para su respaldo y su almacenamiento en discos duros; para tal efecto, se realizará un respaldo incremental de la información: *Una operación de respaldo incremental sólo 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*[1]. En virtud de que los respaldos incrementales contienen fecha y hora, tanto inicial como final, la recuperación se llevará a cabo cruzando la fecha del incidente y el último respaldo.
Plan de	[redacted]

[1] Documento de Seguridad para la Protección de Datos Personales del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), pp. 5 y 6.

contingencia	[redacted] 10-11. Eliminadas dos secciones con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

12. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

13. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.

Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Se optará por las siguientes técnicas de borrado de datos personales priorizando aquellas que no generen impactos importantes al medioambiente: a) **Físicas:** uso de químicos, cremación o el uso de trituradoras de papel a partículas. b) **Electrónicas:** destrucción física, desmagnetización o sobreescritura.
Plan de trabajo	[redacted] 14. Eliminada una sección con fundamento en el artículo 17, párrafo 1, fracción I, inciso a) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Lineamiento Trigésimo Primero, fracción I, inciso b) de los Lineamientos Generales en materia de Clasificación de Información Pública, que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. En virtud de ser información de carácter reservado.
Mecanismos de monitoreo y revisión de las medidas de	**Generar un plan de capacitación:** que consistirá en la organización de campañas de concientización, sensibilización y capacitación, mismas que irán dirigidas principalmente al personal administrativo y académico que en el ejercicio de sus

seguridad	funciones o atribuciones traten datos personales. **Distribución de responsabilidades:** el enlace de transparencia deberá coordinarse con el personal administrativo y académico de su dependencia a fin de revisar las leyes, reglamentos y estatutos internos para comenzar a identificar las funciones y atribuciones que le corresponden a cada área o unidad administrativa, y con base en lo anterior, se comience a delegar y distribuir responsabilidades. **Mecanismos de monitoreo y revisión:** el enlace de transparencia de cada dependencia deberá revisar periódicamente que esté resultando positiva la implementación de la normativa interna en materia de protección de datos personales y seguridad de la información. **Verificación del cumplimiento:** en relación con el punto anterior, el enlace de transparencia verificará que se estén cumpliendo los objetivos y propósitos de las normativas en materia de protección de datos. **Responsabilidades:** En su caso, se determinarán las acciones que se estimen pertinentes para el mejoramiento de las medidas de seguridad, como pueden ser el apercibimiento al área o unidad administrativa que esté siendo omisa o informarle al órgano de control interno, a fin de que éste realice una recomendación o amonestación al área o unidad administrativa omisa.

Programa general de capacitación	La Coordinación de Transparencia y Archivo General, desarrollará el programa general de capacitación de esta Casa de Estudios en la Red Universitaria, para tal efecto, realizará la calendarización y análisis de los temas que se estimen pertinentes sobre la protección de datos personales. Dicho programa tendrá como objetivo la capacitación de todo el personal académico y administrativo que en el ejercicio de sus funciones o atribuciones trate información protegida.