CENACE®

CENTRO NACIONAL DE CONTROL DE ENERGÍA

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DEL CENTRO NACIONAL DE CONTROL DE ENERGÍA (CENACE)

<table>
<tr><th colspan="2">Acuerdo por el que se modifica el Documento de Seguridad para la Protección de Datos Personales del Centro Nacional de Control de Energía.</th></tr>
<tr><td rowspan="3">Marco Normativo Aplicable:
• Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 5 de febrero de 2017, entrada en vigor el 5 de febrero de 1917. Última reforma el 24 de febrero de 2017.
• Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
• Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018.
• Decreto por el que se crea el Centro Nacional de Control de Energía
Publicado en el Diario Oficial de la Federación el 28 de agosto de 2014.
• Estatuto Orgánico del Centro Nacional de Control de Energía, última publicación en el Diario Oficial de la Federación el 20 de abril de 2018.</td><td>Fecha de emisión:
11 de octubre de 2018</td></tr>
<tr><td>Alcance:
Todas las áreas del CENACE</td></tr>
<tr><td>Aprobado:
Mediante el acuerdo CT/ORD36/007/2018, del Comité de Transparencia del Centro Nacional de Control de Energía, tomado en la Trigésima Sexta Sesión General Ordinaria, celebrada el 11 de octubre de 2018

Modificado:
Mediante el acuerdo CT/ORD29/2020, del Comité de Transparencia del Centro Nacional de Control de Energía, tomado en la Vigésima Novena Sesión General Ordinaria, celebrada el 10 de julio de 2020</td></tr>
<tr><td colspan="2">Anexos:
• Anexo 1 Formato de Inventario de Datos Personales y de los Sistemas de Tratamiento
• Anexo 2 Inventario de Datos Personales y de los Sistemas de Tratamiento (actualizado al 30 de junio de 2020)
• Anexo 3 Análisis de Riesgos (emitido al 03 de julio de 2020)
• Anexo 4 Análisis de Brecha
• Anexo 5 Plan de Trabajo
• Anexo 6 Mecanismos de monitoreo y revisión de las medidas de seguridad
• Anexo 7 Programa de Capacitación (autorizado el 17 de enero de 2020)</td></tr>
</table>

C O N S I D E R A N D O

I. Que la Constitución Política de los Estados Unidos Mexicanos, en su artículo 6, Base A, fracción II refiere que la vida privada y que los datos personales serán protegidos con las excepciones que fijen las leyes correspondientes;

II. 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 y cancelación de estos, 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 de principios de orden público, seguridad y salud pública o para proteger los derechos de terceros;

III. Que el 26 de enero de 2017, se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos en Posesión de Sujetos Obligados, misma que entró en vigor al día siguiente de su publicación, la cual es de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal y que en su Transitorio Séptimo establece que los sujetos obligados deberán tramitar, expedir o modificar su normatividad interna a más tardar dentro de los dieciocho meses siguientes a la entrada en vigor del citado Decreto;

IV. Que el CENACE es un organismo público descentralizado de la Administración Pública Federal, con personalidad jurídica y patrimonio propio que tiene a su cargo el Control Operativo del Sistema Eléctrico Nacional; la operación del Mercado Eléctrico Mayorista y garantizar el acceso abierto y no indebidamente discriminatorio a la Red Nacional de Transmisión y las Redes Generales de Distribución, así como proponer la ampliación y modernización de la Red Nacional de Transmisión y los elementos de las Redes Generales de Distribución que correspondan al Mercado Eléctrico Mayorista; y cuenta con el carácter de Sujeto Obligado de conformidad con los artículos 1 y 3, fracción XXVIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

VI. Que en el artículo 33 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se establecen las actividades interrelacionadas que deben realizar los responsables para establecer y mantener las medidas de seguridad para la protección de los datos personales. Asimismo, en el artículo 35 de la Ley en cita se señala la obligación de elaborar un documento de seguridad que cumpla con los requisitos establecidos en el mencionado numeral.

VII.- Que el 26 de enero del 2018, se publicaron en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público, mismos que en su artículo 47 cita que el responsable deberá elaborar e implementar políticas y programas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos los procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continúa, y;

VIII.- Que con el objeto de atender los deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y del marco normativo aplicable a la materia, en la Trigésima Sexta Sesión Ordinaria del Comité de Transparencia del CENACE, celebrada el 11 de octubre de 2018 se aprobó el Acuerdo por el que se emite el Documento de Seguridad para la Protección de Datos Personales del Centro Nacional de Control de Energía, mismo que éste el órgano colegiado considera pertinente modificar a efecto de que se consideren todas las actividades necesarias para la generación de los elementos que conforma el Documento de Seguridad del Centro Nacional de Control de Energía.

Derivado de lo anterior, en la Vigésima Novena Sesión General Ordinaria, celebrada el 10 de julio de 2020, el Comité de Transparencia aprobó el

ACUERDO POR EL QUE SE MODIFICA EL APARTADO NORMATIVO DEL DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DEL CENTRO NACIONAL DE CONTROL DE ENERGÍA

CAPÍTULO I
OBJETO Y ÁMBITO DE APLICACIÓN

Primero.- El presente apartado normativo del Documento de Seguridad para la Protección de Datos Personales del Centro Nacional de Control de Energía, es de observancia obligatoria para todas las personas servidoras públicas del CENACE, y tiene por objeto establecer las directrices y actividades para la generación de cada uno de los elementos que conforman el Documento de Seguridad para la protección de los datos personales en posesión de las áreas de este organismo público descentralizado, con independencia del formato en el que se encuentren.

CAPÍTULO II
DISPOSICIONES GENERALES

Segundo.- Para efectos del presente apartado normativo del Documento de Seguridad para la Protección de Datos Personales del Centro Nacional de Control de Energía, se entenderá, en singular o en plural, por:

I. **Activos:** Todo elemento de valor para el CENACE, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel;

II. **Análisis de riesgos:** El estudio de las causas de las posibles amenazas y probables eventos no deseados, así como los daños y consecuencias que éstas puedan producir en la información en posesión del Centro Nacional de Control de Energía;

III. **Áreas**: Las instancias del Centro Nacional de Control de Energía, previstas en el Estatuto Orgánico, que traten o puedan tratar datos personales;

IV. **CENACE**: El Centro Nacional de Control de Energía;

V. **Comité:** El órgano colegiado al que hacen referencia los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

VI. **Datos personales:** La 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;

VII. **Datos personales sensibles:** Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos de origen racial, étnico, estados de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

VIII. **Documento de Seguridad**: El instrumento que describe y da cuenta de manare general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

IX. **Encargado:** La persona física o moral, del ámbito público o privado, ajeno al CENACE, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del CENACE;

X. **INAI:** El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XI. **Incidente:** Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas del CENACE, que afecte la confidencialidad, la integridad o la disponibilidad de los datos personales;

XII. **Inventario:** El inventario de datos personales y sistemas de tratamiento cuya finalidad es tener el control documentado de los tratamientos que realizan las áreas del CENACE, realizado con orden y precisión;

XIII. **Ley General**: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

XIV. **Lineamientos:** Lineamientos Generales de Protección de Datos Personales para el Sector Público;

XV. **Medidas de seguridad:** El conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger la información en posesión del CENACE;

XVI. **Medidas de seguridad físicas:** Las 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;

XVII. **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre CENACE y el Encargado, dentro o fuera del territorio mexicano;

XVIII. **Sistema de gestión:** El conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales;

XIX. **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a personas distinta del titular, del CENACE, o del encargado;

XX. **Titular:** Persona física a quien corresponden los datos personales;

XXI. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;

XXII. **Unidad de Transparencia:** La instancia a la que hace referencia el artículo 85 de la Ley General;

XXIII. **Vulnerabilidad:** La circunstancias o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño, y

XXIV. **Vulneración de seguridad:** El incidente de seguridad que afecta a los datos personales en cualquier fase de su tratamiento.

CAPÍTULO III
DEL CONTENIDO Y ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

Tercero.- De conformidad con lo establecido en el artículo 35 de la Ley General, el Documento de Seguridad debe contener:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Cuarto.- Conforme al artículo 36 de la Ley General, el Documento de Seguridad deberá ser actualizado por la Unidad de Transparencia en coordinación con las áreas respectivas del CENACE, cuando ocurran los siguientes eventos:

I.- Se produzcan modificaciones sustanciales al tratamiento de datos personales que se deriven en un cambio en el nivel de riesgo;
II.- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III.- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e
IV.- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

CAPÍTULO IV
DEL INVENTARIO DE DATOS PERSONALES

Quinto.- La Unidad de Transparencia en coordinación con las áreas respectivas del CENACE que traten datos personales, deberán elaborar un inventario de datos personales y de los sistemas de tratamiento, el cual contendrá lo siguiente:

I.- El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
II.- Las finalidades de cada tratamiento de datos personales;
III.- El catálogo de los tipos de datos personales que se traten, indicado si son sensibles o no;
IV.- El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V.-La lista de servidores públicos que tiene acceso a los sistemas de tratamiento;
VI.- En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable;
VII.-En su caso, los destinatarios o terceros receptores de la transferencia que se efectúan, así como las finalidades que justifican éstas, y
VIII.- Fundamento legal para su tratamiento.

(Anexo 2 Inventario de Datos Personales y de los Sistemas de Tratamiento)

Sexto.- En la elaboración del inventario, la Unidad de Transparencia y las áreas deberán considerar conforme al artículo 33 fracción I, de la Ley General, el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. El uso de los datos personales conforme su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El Bloqueo de los Datos Personales, en su caso, y
VI. La Cancelación, Supresión o destrucción de los datos personales.

La Unidad de Transparencia y las áreas deberán identificar el riesgo inherente de los Datos Personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software o cualquier otro recurso humano o material que resulte pertinente considerar.

Séptimo.- A efecto de dar cumplimiento a lo establecido en el artículo 33 fracción III, de la Ley General y al numeral Quinto de este instrumento, la Unidad de Transparencia pondrá a disposición de las áreas del CENACE que posean datos personales el formato de Inventario de Datos Personales y de los Sistemas de Tratamiento (Anexo 1) para la debida requisición de cada uno de los rubros contenidos en el mismo, conforme a los siguientes criterios:

Rubros	Criterios
1.- Nombre del sistema	El área tratante de los datos personales deberá precisar el nombre del sistema en donde se encuentren alojados éstos.
2.- Formato de Almacenamiento	El área deberá seleccionar una de las siguientes opciones: **Físico**: Para aquellos datos contenidos en registros manuales, impresos o visuales. **Electrónico:** Para aquellos datos que se encuentran contenidos en dispositivos informáticos o en una herramienta tecnológica específica para su acceso, recuperación o tratamiento. **Mixto:** Aquellos datos que se encuentran contenidas en ambas modalidades (físico y electrónico).
3.- Finalidades del tratamiento de datos personales	Precisar el propósito del tratamiento de los datos personales, los cuales deberán estar relacionados con las atribuciones conferidas al área tratante en la normatividad aplicable.
4.-Fundamento Jurídico para el tratamiento	Se requiere señalar los artículos, numerales, fracciones, apartados e incisos, así como el nombre de la normativa que faculta al área para llevar a cabo el tratamiento de los datos personales.
5.- Datos personales que se recaban	Enlistar los datos personales que se recaban en el sistema, precisando aquellos que sean de carácter sensible.
6.-Descripción general de la ubicación de los datos personales	Señalar la ubicación física o electrónica en donde se alojan los datos personales, precisando la oficina, número de archivero, almacén, bodega nombre del programa, nombres de las carpetas en donde se encuentran los datos y las computadoras de las personas servidoras públicas tengan acceso a éstos.
7.- Realiza transferencias de datos personales	Seleccionar la opción según corresponda “Sí” o “No”.

8.-Destinatarios o receptores de las transferencias	En caso de haber seleccionado la opción “Sí” en el rubro que antecede, se debe precisar las personas físicas o morales, nacionales o internacionales receptores de los datos personales. Este apartado deberá permanecer vacío en caso de haber seleccionado la opción “No” en el rubro número 7.
9.-Finalidades que justifican las transferencias	Precisar las razones por las cuales se transfirieron los datos a los destinatarios citados en el rubro 8. Este apartado deberá permanecer vacío en caso de haber seleccionado la opción “No” en el rubro número 7.
10.-Listado de servidores públicos que tienen acceso al sistema	Colocar el nombre, cargo y área de adscripción de las personas servidoras públicas que tienen acceso al sistema
11.-Nombre del encargado que trata datos por cuenta y a nombre del CENACE	Precisar el nombre de la persona física o moral, pública o privada ajena al CENACE, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de este organismo público descentralizado. Este apartado deberá permanecer vacío si no existe una relación con un encargado.
12.-Instrumento Jurídico que formaliza la prestación de los servicios que brinda al CENACE	Precisar el nombre del instrumento jurídico, así como la fecha de celebración de este, a través del cual se formaliza la relación entre el encargado y el CENACE.
13 y 14 Nombre del Proceso de(los) Procedimiento(s)	Esta información será requisitada por la Unidad Administrativa responsable del Sistema Físico y/o Electrónico que contenga datos personales, en caso de contar con dicha información, de lo contrario la requisitará la Dirección de Estrategia y Normalización, en concordancia con el inventario de procesos institucional.

Las áreas del CENACE, deberán requisitar el formato de Inventario de Datos Personales y de los Sistemas de Tratamiento (Anexo 1) por cada uno de los sistemas en donde recaben y traten datos personales.

Octavo.- Anualmente, la Unidad de Transparencia requerirá a las áreas del CENACE la actualización de los formatos de Inventario, y en su caso, la inclusión y/o eliminación de los sistemas que correspondan. Por lo que, como resultado de dicha actividad se actualizará el Inventario de Datos Personales y de los Sistemas de Tratamiento (Anexo 2)

CAPÍTULO V
DE LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Noveno.- De conformidad al artículo 33 fracción II, de la Ley General, las personas servidoras públicas de las áreas del CENACE que, en el ejercicio de sus funciones, traten datos personales tendrán, de manera enunciativa mas no limitativa las siguientes funciones y obligaciones:

I.- Tratar los datos personales que obren en su poder, conforme a las atribuciones de su área de adscripción observando los principios de licitud, lealtad, consentimiento, información, proporcionalidad, finalidad, calidad y responsabilidad;
II.- Guardar confidencialidad respecto de los datos personales tratados, dicha obligación subsistirá aún después de finalizar las relaciones laborales con el CENACE y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública;

III- Acatar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que emitan las áreas competentes para tal efecto en documentos normativos del CENACE;
IV.- Informar a la Unidad de Transparencia en caso de que se presente una vulneración u ocurra un incidente a la seguridad de los datos personales;
V.- Requisitar el formato de Inventario de Datos personales, conforme a lo establecido en el numeral Séptimo del presente Documento y con el acompañamiento de la Unidad de Transparencia;
VI.- Solicitar a la Unidad de Transparencia la generación de los Avisos de Privacidad que, en su caso, requiera con la finalidad de ponerlos a disposición de los titulares de datos personales;
VII.- En caso de requerir servicios que impliquen el tratamiento de datos personales por un tercero, informar a la Unidad de Trasparencia, la Dirección Jurídica y a la Dirección de Administración y Finanzas para que, en el ámbito de sus respectivas competencias, se efectúe la formalización de la relación jurídica entre el Encargado y CENACE. Cuando el Encargado solicite una autorización para subcontratar servicios que impliquen el tratamiento de datos personales, informar a la Unidad de Trasparencia, la Dirección Jurídica y a la Dirección de Administración y Finanzas para que procedan conforme a sus atribuciones a efecto de deliberar lo conducente respecto de la subcontratación y, en su caso, autorizar y formalizar la misma mediante el instrumento jurídico que resulte aplicable conforme al marco normativo del CENACE;
VIII.-En caso de requerir transferir o remitir datos personales en los ámbitos nacional e internacional, informar a la Unidad de Trasparencia y a la Dirección Jurídica, para que procedan conforme a sus atribuciones en cuanto a la formalización de la relación jurídica entre el responsable y el receptor mediante la suscripción del instrumento jurídico idóneo, de conformidad con la normatividad que resulte aplicable al CENACE, que permita demostrar el alcance del tratamiento de los datos personales así como las obligaciones y responsabilidades asumidas por las partes, y
IX.- Suprimir los datos personales objeto de tratamiento una vez que se extingan las causas de su tratamiento o previa instrucción de la o el superior jerárquico, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales conforme a la normatividad aplicable.

Décimo.- Corresponde a la Unidad de Transparencia, a la Dirección Jurídica y a la Dirección de Administración y Finanzas con el área requirente, verificar la formalización de la relación jurídica que, en su caso, se efectúe entre el Encargado y el CENACE, a través del instrumento jurídico idóneo, de conformidad con la normativa que resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

En caso, de que el Encargado solicite autorización para llevar a cabo una subcontratación, deberán deliberar lo conducente respecto de la misma y, en su caso, autorizarla y formalizarla mediante un contrato o cualquier otro instrumento jurídico que resulte aplicable conforme al marco normativo del CENACE.

Décimo primero.- Corresponde a la Dirección de Administración y Finanzas, a través de la Subdirección de Administración, establecer las medidas de seguridad de carácter administrativo y físico para la protección de los activos involucrados en el tratamiento de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley General, en coordinación con todas las áreas del CENACE, particularmente con la Dirección de Tecnologías de la Información y Comunicaciones.

Por lo que hace a las medidas de seguridad físicas, la Dirección de Administración y Finanzas, a través de la Subdirección de Administración deberá implementar 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, considerarán las siguientes actividades:

I.- Prevenir el acceso no autorizado al perímetro del CENACE, sus instalaciones físicas, áreas críticas, recursos e información;

II.- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información del CENACE;

III.- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir del CENACE, y

IV.- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Décimo segundo.- La Dirección de Administración y Finanzas, a través de la Subdirección de Administración, por medio del Área Coordinadora de Archivos, establecerá los procedimientos para la conservación y supresión de los datos personales.

Décimo tercero.- Corresponde a la Dirección de Tecnologías de la Información y Comunicaciones:

I.-Establecer y mantener las medidas de seguridad de carácter técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, en coordinación con todas las áreas del CENACE que traten Datos Personales. Dentro del 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 los recursos involucrados en su tratamiento, de manera enunciativa mas no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware del CENACE, y

c) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

II.- Cerciorarse en coordinación con la Unidad de Transparencia de que los servicios, aplicaciones e infraestructura de cómputo y otras materias para el tratamiento de datos personales a los que se adhiera el CENACE, cumplan con las disposiciones establecidas en la Ley General.

CAPÍTULO VI
DEL ANÁLISIS DE RIESGOS, EL ANÁLISIS DE BRECHA Y EL PLAN DE TRABAJO

Décimo cuarto.– La Dirección de Estrategia y Normalización a través de la Jefatura de Unidad de Riesgos y la Dirección de Tecnologías de la Información y Comunicaciones, por medio de la Subdirección de Infraestructura de Tecnologías de la Información y Comunicaciones y de la Jefatura de Unidad de Seguridad Informática, en coordinación con la Unidad de Transparencia, en el ámbito de sus respectivas atribuciones, realizarán una matriz de riesgos aplicada a las áreas del CENACE que tratan datos personales, de la cual emanará el documento de Análisis de Riesgos que contendrá por lo menos, lo siguiente:

I.-Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;

II.-El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;
III.- El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV.-Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;
V.-El riesgo inherente a los datos personales tratados, considerando los activos, las amenazas y las vulnerabilidades;
VI.-La sensibilidad de los datos personales tratados;
VII.-El desarrollo tecnológico;
VIII.- Las posibles consecuencias de una vulneración para los titulares;
IX.- Las transferencias de datos personales que se realicen;
X.- El número de titulares;
XI.- Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
XII.- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

(Anexo 3 Análisis de Riesgos)

Décimo quinto.– La Dirección de Estrategia y Normalización a través de la Jefatura de Unidad de Riesgos y la Dirección de Tecnologías de la Información y Comunicaciones, por medio de la Subdirección de Infraestructura de Tecnologías de la Información y Comunicaciones y de la Jefatura de Unidad de Seguridad Informática, conforme a sus respectivas atribuciones en coordinación de la Unidad de Transparencia realizarán un análisis de brecha, el cual contendrá por lo menos, lo siguiente:

I.-Las medidas de seguridad existentes y efectivas;
II.-Las medidas de seguridad faltantes, y
III.-La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

(Anexo 4 Análisis de Brecha)

Décimo sexto.– La Dirección de Estrategia y Normalización a través de la Jefatura de Unidad de Riesgos y la Dirección de Tecnologías de la Información y Comunicaciones, por medio de la Subdirección de Infraestructura de Tecnologías de la Información y Comunicaciones y de la Jefatura de Unidad de Seguridad Informática, conforme a sus respectivas atribuciones en coordinación con la Unidad de Transparencia y con la previa aprobación del Comité, elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, se realizará tomando en consideración los recursos designados, el personal interno y externo del CENACE, y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes, para lo cual se requerirá de la participación de la Dirección de Administración y Finanzas, a través de la Subdirección de Administración y de la Subdirección y Finanzas.

(Anexo 5 Plan de Trabajo)

CAPÍTULO VII
DE LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Décimo séptimo.– La Dirección de Administración y Finanzas, la Dirección de Tecnologías de la Información y Comunicaciones, la Dirección Jurídica y la Unidad de Transparencia conforme a sus respectivas atribuciones en coordinación con las Áreas del CENACE que realicen o puedan realizar tratamiento de datos personales, deberán realizar mecanismos de monitoreo y revisión de las medidas de seguridad que protegen datos personales de manera periódica, conforme a lo siguiente:

I.- Los nuevos activos que se incluyan la gestión de riesgos;
II.- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
III.- Las nuevas amenazas que podrían estar activas dentro y fuera del CENACE y que no han sido valoradas;
IV.- La posibilidad de que las Vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
V.- La Vulnerabilidad identificada para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
VI.- El cambio en el impacto o consecuencia de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgos, y
VII.- Las Vulnerabilidades que se presenten y las Vulneraciones de seguridad ocurridas.

Aunado a lo anterior, las Áreas en función a sus atribuciones del CENACE, deberán contar con un programa de auditoria, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

(Anexo 6 Mecanismos de monitoreo y revisión de las medidas de seguridad)

CAPÍTULO VIII
DEL PROGRAMA DE CAPACITACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Décimo octavo.- La Unidad de Transparencia, previa aprobación del Comité, deberá diseñar e implementar un programa a corto, mediano y largo plazo que tengan por objeto capacitar a las personas servidoras públicas del CENACE. Para el diseño e implementación de los programas de capacitación, se deberá tomar en cuenta lo siguiente:

I.- Los requerimientos y actualizaciones del sistema de gestión;
II.- La legislación vigente en materia de protección de datos personales y las mejores prácticas para el tratamiento de éstos;
III.- Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
IV.- Las herramientas relacionadas o utilizadas para el tratamiento de los datos personales y para a implementación de las medidas de seguridad.

(Anexo 7 Programa de Capacitación)

CAPÍTULO IX
DE LOS INCIDENTES Y VULNERACIONES A LA SEGURIDAD

Décimo noveno.- La Dirección de Administración y Finanzas, por medio de la Subdirección de Administración y la y la Dirección de Tecnologías de la Información y Comunicaciones, por medio de la Subdirección de Infraestructura

de Tecnologías de la Información y Comunicaciones y de la Jefatura de Unidad de Seguridad Informática, implementarán sistemas de detección y/o registro de alertas de seguridad que adviertan respecto de anomalías o cambios no deseados en los activos del CENACE.

Las alertas de seguridad podrán ser manuales o automatizadas y originarse a través de diversas fuentes tales como: los titulares de los datos personales, usuarios de los sistemas de tratamiento, provenientes de la Dirección de Tecnologías de la Información y Comunicaciones o de proveedores de servicios de telecomunicaciones, medios masivos de comunicaciones o sitios web especializados.
Conforme a lo anterior, la Dirección de Administración y Finanzas y la Dirección de Tecnologías de la Información y Comunicaciones, en el ámbito de sus respectivas competencias, deberán asegurarse de que el CENACE cuente al menos con los siguientes tipos de alertas:

Entorno	Tipo de alerta
Para entorno físico	Alarmas para desastres naturales como incendios o terremotos
	Alarmas contra robo o intrusos en las instalaciones
	Alertas del personal de vigilancia o a través de circuito cerrado de televisión.
	Aviso de desaparición o extravío de equipos de cómputo, medios de almacenamiento o documentos.
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento físico.
Para entorno electrónico	Notificaciones sobre softwares maliciosos o vulnerabilidades técnicas descubiertas
	Alertas de sistemas automatizados como firewalls, antivirus, filtros de contenido, sistemas de detección de intrusos o gestores de seguridad de la información
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento automatizados, medios de almacenamiento y equipos de cómputo

Vigésimo.- De manera enunciativa mas no limitativa, se entenderá como vulneraciones de seguridad a los incidentes que afectan los datos personales en cualquier fase del tratamiento de los mismos, tales como; los siguientes:

I.- La pérdida o destrucción no autorizada;
II.- La divulgación no autorizada;
IV.- El robo, extravío o copia no autorizada;
V.- El uso, acceso o tratamiento no autorizado, y
VI.- El daño, alteración o modificación no autorizada.

Vigésimo primero.– Las personas servidoras públicas del CENACE que tengan acceso datos personales, tendrán la obligación de notificar, de manera inmediata, al o la superior jerárquico y a la Unidad de Transparencia de cualquier incidente detectado, debiendo notificar mediante escrito dentro de los siguientes tres días hábiles a que tuvo conocimiento, al menos, lo siguiente:

I.- La información de la persona que ha detectado el incidente tales como nombre, extensión, área de adscripción y correo electrónico institucional;
II.-La hora y fecha de la identificación de la vulneración;
III.- La descripción de las circunstancias generales en torno a la vulneración; tales como localización del incidente, tipo de sistema de tratamiento (físico, automatizado o mixto), nombre del responsable del sistema de tratamiento y descripción de lo sucedido;

IV.- Los datos personales comprometidos;
IV.- Las recomendaciones dirigidas que, en su caso, se puedan adoptar para proteger los datos personales;
V.- Las acciones correctivas realizadas que, en su caso, se hayan llevado a cabo, y
VI.- Cualquier otra información y documentación que considere conveniente hacer del conocimiento.

Vigésimo segundo.- Una vez que la Unidad de Transparencia reciba el escrito citado en el numeral que antecede, en coordinación con la Dirección de Administración y Finanzas y la Dirección de Tecnologías de la Información y Comunicaciones, deberán realizar una investigación sobre el incidente, con la finalidad de determinar el alcance de la afectación a los datos.

En caso de que un Incidente afecte de forma significativa los derechos patrimoniales o morales del titular, la Unidad de Transparencia deberá informar lo conducente tanto al titular como al INAI, en un plazo máximo de setenta y dos horas, en los términos que fijen los Lineamientos y la Ley General.

Vigésimo tercero.– Posterior a la investigación y, con independencia del tipo de incidente de que se trate, las áreas en donde se haya presentado éste, en coordinación con la Dirección de Administración y Finanzas y/o la Dirección de Tecnologías de la Información y Comunicaciones, conforme a sus respectivas atribuciones, realizarán un plan de implementación de medidas de seguridad para mitigar el incidente y prevenir eventos de dicha naturaleza, mismo que deberá ser informado a la Unidad de Transparencia.

Vigésimo cuarto.- Las áreas del CENACE que traten datos personales, deberán elaborar una bitácora de los incidentes a la seguridad, la cual será requisitada por una persona servidora pública designada para tal efecto y debe contener por lo menos los siguientes datos:

I.- La fecha en la que ocurrió el incidente;
II.- La o las causas del incidente de la Información Restringida;
III.- El tipo de Información Restringida que fue vulnerada, y
IV.- Las acciones correctivas que, en su caso, se hayan implementado.

Dicha bitácora deberá ser informada a la Unidad de Transparencia, dentro de los cinco días hábiles posteriores a la implementación de las acciones correctivas que se hayan implementado.

CAPÍTULO X
DE LA INTERPRETACIÓN

Vigésimo quinto.- El Comité será el encargado de interpretar el presente apartado normativo del Documento de Seguridad y de resolver cualquier asunto no previsto en el mismo.

TRANSITORIOS

PRIMERO. El presente apartado normativo del Documento de Seguridad entrará en vigor al día siguiente de su aprobación por el Comité de Transparencia.

SEGUNDO. El apartado normativo del Documento de Seguridad deberá ser difundido a todo el personal a través del correo electrónico institucional y publicado en la Intranet institucional.

TERCERO. Instrúyase a la Unidad de Transparencia, para que realice el acompañamiento a las áreas respectivas del CENACE en la elaboración o complementación y/o actualización de lo siguiente: Inventario de Datos Personales

y de los Sistemas de Tratamiento; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; los Mecanismos de monitoreo y revisión de las medidas de seguridad y el Programa de Capacitación.