Santa Catarina

saber hacer para competir

DOCUMENTO DE SEGURIDAD EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD TECNOLÓGICA SANTA CATARINA

Documento de Seguridad de la Universidad Tecnológica Santa Catarina

INTRODUCCIÓN

Las reformas constitucionales realizadas en 2009 y 2014 a los artículos 16 y 6, propiciaron, por un lado, la emisión de la ley en la materia con el propósito de garantizar este derecho fundamental y, por otro, fijar las bases para la emisión de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual es publicó el 26 de enero de 2017.

En dicha ley, se establece las bases, principios y procedimientos para garantizar el citado derecho, siendo aplicable en los tres niveles de gobierno; con lo que se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Por otro lado, en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León se establecen las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales de los ciudadanos en posesión del sujeto obligado denominado Universidad Tecnológica Santa Catarina.

En cumplimiento con lo establecido en los artículos 35 de la Ley General de Protección de Datos Personales e Posesión de Sujetos Obligados y 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León se crea el presente documento de seguridad con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales.

Este documento de seguridad brindará homogeneidad en la organización y procesos para la protección de los datos personales del organismo descentralizado. Asimismo, el presente documento controlará internamente el universo de datos personales en posesión de la universidad, el tipo de datos personales que contienen los archivos, los responsables, las obligaciones, el análisis de riesgos y los mecanismos de monitoreo y revisión de las medidas de seguridad.

GLOSARIO

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada e identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Documento de seguridad: Instrumento que describe y da cuenta de manera 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.

Hardware: es el conjunto de componentes físicos de los que está hecho el equipo.

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

INFONL: Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

LPDPPSONL: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimiento para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

Titular: Persona física a quien pertenecen los datos personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.

Tratamiento: De manera enunciativa más no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimiento 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 los datos personales.

Sistema de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Unidad administrativa: Son aquellas unidades creadas mediante alguna normatividad previamente establecida, con atribuciones específicas, que forman parte de la base orgánica de la Universidad Tecnológica Santa Catarina.

UTSC: Universidad Tecnológica Santa Catarina.

UTUTSC: Unidad de Transparencia de la Universidad Tecnológica Santa Catarina.

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

De conformidad con los artículos 33, fracción III, y 35, fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 38, fracción III, y 41, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y 54 y 55 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León; se presenta el inventario.

Unidad Administrativa	Tipo de datos personales	Finalidad del tratamiento	Forma de obtención de los datos personales	Formato de almacenamiento	Ciclo de vida	Servidores públicos con acceso
Subdirección de Servicios Escolares	• Nombre • Fecha de nacimiento • Lugar de nacimiento • CURP • Estado civil • Edad • Domicilio • Celular/teléfono • Correo electrónico • Imagen (fotografía) • Firma autógrafa	• Inscripciones • Reingreso • Revalidación • Solicitud de titulación.	Directa	• Electrónico • Físico	Permanente	Personal adscrito a la subdirección de servicios escolares. (Los cargos adscritos a la unidad administrativa se pueden consultar en el organigrama publicado en la plataforma de transparencia). https://transparencia.nl.gob.mx/archivos/3ad44c7698e425e50ce752138dfe68431712768439.pdf
Subdirección de planeación y evaluación	• Nombre • Fecha de nacimiento • CURP • Estado civil • Edad • Domicilio • Celular/teléfono • Correo electrónico • Imagen (fotografía) • Firma autógrafa	Identificar candidatos a capacitar, evaluar y certificar en estándar de competencia del ECE035-II	Directa	• Electrónico • Físico	Permanente	Personal adscrito a la subdirección de planeación y evaluación. (Los cargos adscritos a la unidad administrativa se pueden consultar en el organigrama publicado en la plataforma de transparencia). https://transparencia.nl.gob.mx/archivos/3ad44c7698e425e50ce752138dfe68431712768439.pdf
Dirección Académica	• Nombre • Fecha de nacimiento • Lugar de	• Prevención • Seguimiento • Deserción	Directa	• Electrónico • Físico	Permanente	Personal adscrito a la Subdirección de cada carrera.

	nacimiento • CURP • Estado civil • Edad • Domicilio • Celular/teléfono • Correo electrónico • Matrícula					(Los cargos adscritos a la unidad administrativa se pueden consultar en el organigrama publicado en la plataforma de transparencia). https://transparencia.nl.gob.mx/archivos/3ad44c7698e425e50ce752138dfe68431712768439.pdf
Dirección de Administración y Finanzas	• Nombre • Fecha de nacimiento • Lugar de nacimiento • CURP • Estado civil • Edad • Domicilio • Celular/teléfono • Correo electrónico • Matrícula	• Contratación • Pagos de nómina	Directa	• Electrónico • Físico	Permanente	Personal adscrito a la Jefatura de Departamento de Recursos Humanos y Nomina. (Los cargos adscritos a la unidad administrativa se pueden consultar en el organigrama publicado en la plataforma de transparencia). https://transparencia.nl.gob.mx/archivos/3ad44c7698e425e50ce752138dfe68431712768439.pdf
Dirección de Vinculación	• Nombre • Fecha de nacimiento • Lugar de nacimiento • CURP • Estado civil • Edad • Domicilio • Celular/teléfono • Correo electrónico • Matrícula • Imagen (fotografía) • Datos de salud	• Vinculación con empresas • Medidas de inclusión • Educación Dual	Directa	• Electrónico • Físico	Permanente	• Personal adscrito a la Jefatura de Departamento de Vinculación. • Personal adscrito a la Jefatura de Departamento de Movilidad Internacional, Nacional y Educación Vial • Personal adscrito a la Jefatura de Inclusión Laboral y Educativa. (Los cargos adscritos a la unidad administrativa se pueden consultar en el organigrama publicado en la plataforma de transparencia). https://transparencia.nl.gob.mx/archivos/3ad44c7698e425e50ce752138dfe68431712768439.pdf

2. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

De conformidad con los artículos 3, fracciones XXII y XXIII y 35, fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 3, fracciones XXVII y XXVIII, y 41, fracción II, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, el inventario de datos personales y el Manual de Organización de la Universidad Tecnológica Santa Catarina, las obligaciones y funciones son las siguientes:

A. De cualquier servidor público.

I. Conocer, aplicar y sujetarse al aviso de privacidad y al documento de seguridad de Universidad Tecnológica Santa Catarina en el tratamiento de datos personales.

II. Tratar los datos personales siempre de manera lícita, siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

III. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina.

IV. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

V. Tomar periódicamente cursos, talleres o capacitación sobre el tratamiento de datos personales.

VI. Apegarse, en todo momento, a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

B. Del servidor público que se encargue de la recepción de datos personales.

I. Tener a la vista el documento denominado Aviso de Privacidad de la Universidad Tecnológica Santa Catarina.

II. Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.

III. Al obtener los datos personales, cerciorarse de que la información esté completa, actualizada y comprensible.

IV. Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se percate

de alguna inconsistencia.

V. Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales durante el periodo en el que posea los datos personales.

VI. Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

C. Del servidor público involucrado en el tratamiento de datos personales.

I. Aplicar las medidas de seguridad correspondientes a los datos personales tratados o el sistema de protección en el que participa.

II. Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

D. Del servidor público que administra los datos personales.

I. Conocer e implementar las medidas de seguridad establecidas en el documento de seguridad.

II. Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.

III. Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada trámite o sistema.

IV. Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

V. Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.

VI. Informar a la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

VII. Acudir a la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina en caso de requerir asesoría sobre el tratamiento de datos personales.

VIII. Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.

IX. Dar aviso al Comité de Transparencia, a través del titular de la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

E. Del servidor público responsable de cada sistema o del titular de la Unidad Administrativa responsable de cada sistema.

I. Implementar las medidas de seguridad que establece el documento de seguridad.

II. Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.

III. Informar al titular de la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

IV. Monitorear la implementación de las medidas de seguridad.

V. Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.

VI. Dar aviso al Comité de Transparencia o en su defecto al titular de la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

VII. Presentar propuestas de mejora o modificación del documento de seguridad a través del titular de la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina.

VIII. Emitir reportes en relación con el tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Universidad Tecnológica Santa Catarina.

IX. Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales emita el Comité de Transparencia, el INFONL, INAI, así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

F. Del Responsable de la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina.

I. Auxiliar en difundir al interior de la Universidad Tecnológica Santa Catarina los avisos de privacidad y el documento de seguridad de la institución.

II. Auxiliar en la revisión física anual a dos unidades administrativas sobre el tratamiento de datos personales y la implementación de medidas de seguridad, mismas que serán sugeridas por el Comité de Transparencia de la Universidad.

III. Proponer al Comité de Transparencia de la Universidad actualizaciones o modificaciones al documento de seguridad.

IV. Demás que señalen leyes, reglamentos y lineamientos federales y locales.

G. Del Comité de Transparencia de la Universidad Tecnológica Santa Catarina.

I. Revisar anualmente las políticas o lineamientos en materia de protección de datos personales establecidos en el presente documento.

II. Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.

III. Requerir anualmente a las áreas responsables que tratan datos personales, a través del titular de la Unidad de Transparencia de la Universidad Tecnológica Santa Catarina, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

IV. Demás que señalen leyes, reglamentos y lineamientos federales y locales.

3. EL ANÁLISIS DE RIESGOS

De conformidad con los artículos 33, fracción IV, y 35, fracción III, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 38, fracción V, y 41, fracción III, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y 56 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León; se presenta el análisis de riesgos.

Para emitir dicho análisis de riesgos se tomó en cuenta los siguientes aspectos:

A. Información general

I. La identificación de los datos personales que se obtienen o reciben.

II. Motivo por el cual se recaban o reciben los datos personales.

B. Finalidades del tratamiento

I. La denominación del tratamiento de datos personales que realiza y la forma en que se opera, detallando el fundamento legal y normativo aplicable al tratamiento.

II. La categoría correspondiente a los datos personales tratados, es decir, si se ejerce sobre datos de carácter identificativo, de características personales, circunstancias sociales, datos académicos y profesionales, detalles del empleo, de información comercial, datos económicos o financieros y de seguro.

III. La duración del tratamiento que realiza, es decir, si es instantáneo, o si tiene un periodo de duración de días, semanas, meses, años, o resulta de tiempo indeterminado.

IV. Si la obtención de los datos tiene como finalidad el tratamiento de datos personales sensibles.

V. Si la finalidad del tratamiento pudiera cumplirse recabando un menor número de datos personales.

VI. Si la finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad.

VII. Si el tratamiento de los datos personales tiene la finalidad de elaborar documentos, perfiles o es utilizado para la toma de decisiones.

VIII. Si el número de personas servidoras públicas involucradas en el tratamiento de datos personales resulta insuficiente, suficiente o excesivo.

C. Tecnologías empleadas para el tratamiento

I. La tecnología implementada en el tratamiento de datos personales, describiendo el nombre y el modo de empleo.

D. Transferencia de datos personales

I. Si en el tratamiento de datos personales se realiza una transferencia de datos a entidades diversas a la UTSC, destacando la normatividad correspondiente y el instrumento legal en el que se convino dicha transferencia.

II. Si en el tratamiento de datos personales se realiza una transferencia de datos a otras entidades, señalando la normatividad correspondiente, el nombre y entidad y describa el instrumento legal en el que se convino dicha transferencia.

E. Controles existentes

I. Respecto de los controles que se encuentran instaurados para la protección de los datos personales, se identificó el nombre del control, su objetivo, la forma en que se instrumenta, el nombre y cargo de las personas servidoras públicas involucradas en la ejecución del control, el documento en que se registra la existencia del control destacando el nombre y cargo de la persona servidora pública responsable, así como los resultados y demás cuestiones inherentes a su elaboración.

II. Identificación de la naturaleza de los controles existentes, es decir, de carácter preventivo o correctivo.

III. Controles ejecutados en los casos en que el tratamiento de datos personales se encuentre documentado en papel.

IV. Controles ejecutados en los casos en que el tratamiento de datos personales sea documentado de forma electrónica.

V. La efectividad de los controles implementados para garantizar la seguridad de los datos personales.

F. Percepción de la existencia de un riesgo

I. Previa reflexión de los controles implementados, consideración relativa a si el tratamiento de datos personales puede conllevar una pérdida o alteración de la información.

II. Si los controles y medidas de seguridad existentes para la obtención, tratamiento, resguardo y archivo de los datos personales cumplen su objetivo de manera efectiva.

III. Si los riesgos considerados pueden afectar los controles y medidas de seguridad implementadas en el tratamiento de datos personales.

IV. La forma en la que los riesgos señalados pueden reducirse a futuro.

V. Si los riesgos identificados pueden ser compartidos con otra instancia.

VI. Si las formas de reducir los riesgos identificados pueden ser compartidas con otra instancia.

MATRIZ DE ANÁLISIS DE RIESGOS				
Identificación		Análisis		Evaluación
Riesgo	Vulnerabilidad	Gravedad	Probabilidad	Nivel del riesgo
Falla en los equipos de cómputo	Mantenimiento insuficiente	Baja	Baja	Bajo
Equipos de cómputo dañados	Falta de presupuesto para cambiar equipos	Baja	Baja	Baja
Robo de información en equipo de cómputo	Equipos sin seguridad suficiente	Medio	Baja	Medio
Pérdida de documentos físicos	Error humano en el manejo de papeles.	Bajo	Bajo	Bajo
Personal divulgue datos personales sin justificación	Falta de capacitación	Bajo	Bajo	Bajo
Titular de datos personales no quiera proporcionar datos personales	No cuenta con la información de cómo se resguardan los datos	Bajo	Bajo	Bajo

4. EL ANÁLISIS DE BRECHA

De conformidad con los artículos 33, fracción V, y 35, fracción IV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 38, fracción V, y 41, fracción IV, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y 57 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León; se presenta el análisis de brecha.

Las brechas fueron analizadas atendiendo los siguientes factores:

A. Si los controles de seguridad declarados han resultado efectivos para garantizar la seguridad de los datos personales.

B. Si después del análisis de los controles de seguridad, se considera que el tratamiento de datos personales puede conllevar una pérdida o alteración de la información.

C. Si los controles y medidas de seguridad existentes para la obtención, tratamiento, resguardo y archivo de los datos personales cumplen su objetivo de manera efectiva.

D. Los riesgos que se consideran pueden afectar los controles y medidas de seguridad implementadas en el tratamiento de datos personales.

E. La forma en la que se estima que los riesgos señalados pueden reducirse a futuro.

El resultado de lo anterior es lo siguiente:

A. Las medidas de seguridad existentes y efectivas.

   I. Equipos de cómputo con seguridad del sistema operativo Windows.

   II. Servidor con firewall, detector de intrusos y antivirus

   III. Archiveros para guardar documentación física

   IV. Existencia de avisos de privacidad.

   V. Publicación de avisos de privacidad.

   VI. Programa de capacitación

B. Las medidas se seguridad faltante

   I. Capacitación más frecuente y que llegue a más personal de la UTSC

C. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno más

controles implementados actualmente.

I. Reducir al mínimo la utilización del papel en los trámites de la UTSC para reducir riesgos de divulgación de datos personales.

II. Que sólo unos cuantos servidores públicos puedan tratar datos personales.

III. Ampliar la capacitación de datos personales a la mayoría del personal de la UTSC.

Para un mejor entendimiento, es importante diferenciar y aplicar las siguientes medidas.

A. **Medidas de seguridad físicas**, para evitar daños, sustracciones o intromisiones no autorizadas en las instalaciones y archivos de información del sujeto obligado.

I. Asignar un espacio seguro y adecuado para el tratamiento de datos personales, que no se encuentre a la vista del público y que preferentemente no sea un área de paso frecuente por el personal de trabajo o ajeno al mismo.

II. Tener bajo llave o asegurados los archiveros, archivos, cajas y almacenes en donde se encuentre almacenada la información de datos personales.

III. Evitar descuidar o tener sin la atención debida documentos que contengan datos personales.

IV. Implementar un plan de contingencia con protocolos de seguridad, que incluya, cuando menos, la designación de responsables por área administrativa, procedimientos de control, señalizaciones y medidas de protección física contra incendio, inundación, sismo, explosión y cualquier otra forma de desastre natural o humano.

V. Verificar que en ningún caso y bajo ninguna circunstancia los documentos que contengan datos personales se utilicen como papel reciclable ni de doble uso, ya que una vez transcurridos los plazos en que deban cancelarse o al tratarse de proyectos no utilizables, deberán ser destruidos.

B. **Medidas de seguridad en el entorno**, para evitar el acceso físico no autorizado a las instalaciones y a su información:

I. Registrar a visitantes que accedan a instalaciones de la Universidad Tecnológica Santa Catarina.

II. Identificar a los servidores públicos adscritos al sujeto obligado.

C. **Medidas de seguridad administrativa relacionadas con el recurso humano**, para asegurar que tanto los servidores públicos como terceros con quienes se tenga una relación, sean aptos y de perfil idóneo para desarrollar sus responsabilidades, funciones u obligaciones contractuales, según corresponda, en el tratamiento y

protección de datos personales, buscando reducir con ello el riesgo de robo, fraude, transmisiones no autorizadas o en general, cualquier mal uso de esta información, se deberán implementar las siguientes acciones:

I. Definir el perfil del servidor público, empleado o proveedor que realiza o realizará las funciones relacionadas con el tratamiento de datos personales.

II. Verificar los antecedentes laborales de los aspirantes al empleo en el servicio público, contratistas u otros terceros con que se inicie una relación contractual, cuyas labores estarán relacionadas con el tratamiento de datos personales en posesión de sujetos obligados.

III. Cuando resulte pertinente, una reorganización interna, según los perfiles autorizados, de los servidores públicos que deberán dar tratamiento a la información de datos personales, sin afectación de derechos laborales.

IV. Procurar permear la información señalada en la fracción inmediata anterior al personal que ya labora en la institución.

V. Requerir, como parte de su obligación contractual con servidores públicos o terceros, que se acepten y firmen los términos, condiciones y obligaciones relacionados con el debido tratamiento de datos personales y la seguridad de información en términos de la Ley y demás normatividad aplicable.

VI. Procurar capacitar, conforme resulte procedente, a terceros con que se tenga una relación contractual sobre el debido tratamiento de datos personales, la existencia de amenazas de seguridad, de cómo pueden ser prevenidas mediante el debido cumplimiento de sus responsabilidades, obligaciones y de la pertinencia de la seguridad de la información.

VII. Capacitar de manera periódica a los servidores públicos que lleven a cabo el tratamiento de datos personales para que se especialicen, concienticen y actualicen en relación con las medidas que se deben adoptar, los procedimientos de seguridad y el uso correcto de los medios disponibles para el procesamiento de la información con el objeto de minimizar los posibles riesgos.

VIII. Establecer en los acuerdos que se suscriban entre la Universidad Tecnológica Santa Catarina y terceros, temas relacionados a la confidencialidad con servidores públicos o terceros que actualmente estén relacionados con la seguridad de los servicios de procesamiento de la información y el tratamiento de datos personales en posesión de sujetos obligados, según resulte procedente o bien comunicarles las responsabilidades de tipo administrativo o penal en caso de incumplimiento a la normatividad aplicable.

D. **Medidas de seguridad en la finalización o modificación de la relación laboral o contractual,** para que una vez que concluya o se modifique la misma con los empleados base o por honorarios, o bien, con terceras personas, se adopten las medidas necesarias para la desvinculación organizada de funciones e información, reiterando la subsistencia del deber de respeto a los principios de confidencialidad, máxima privacidad y seguridad en términos de la legislación aplicable:

   I. Actualizar el documento de seguridad en lo relacionado con el padrón de servidores públicos Responsables y Encargados que sean designados.

   II. Identificar y revisar con frecuencia que los acuerdos de confidencialidad y protección de la información no pierdan vigencia y contemplen la no divulgación de los datos personales.

   III. Establecer vías idóneas para recordar al personal que subsisten los deberes de respeto a los principios de confidencialidad y secrecía en relación con la informaciónde datos personales a la que tuvieron conocimiento o acceso con motivo de su empleo, cargo o prestación de servicio, independientemente de que haya concluido ya su fase de acceso o cualquier otro tipo de tratamiento.

E. **Medidas de seguridad técnicas,** es importante referir en este punto que las medidas de seguridad técnicas consisten en mecanismos que se valen de la tecnología, aseguran el acceso a las bases de datos relacionados con el software y hardware, es decir protegen el entorno digital de los datos personales.

   I. Registrar habitualmente la información que corresponda en el Sistema de Datos Personales y mantenerlo actualizado en todo momento;

   II. Requerir el apoyo del área de tecnologías de la información para la implementación de medidas tecnológicas idóneas para proteger la información;

   III. Inventariar el equipo tecnológico que tiene la Universidad Tecnológica Santa Catarina, tales como computadoras, impresoras, escáneres y copiadoras, para efectos de:

      a. Verificar que durante los mantenimientos y monitoreo que el personal interno o externo brinde al equipo, no se vulnere la seguridad de la información contenida en su disco duro o cualquiera de sus dispositivos de almacenamiento en la forma que adopten, debiendo estar acompañados por un servidor público autorizado para tal efecto;

      b. Eliminar por completo del disco duro del equipo o cualquiera de sus dispositivos de almacenamiento, previamente a su devolución, tras la terminación del contrato respectivo, tratándose de arrendamiento

o similar, o encaso de que sean dados de baja, toda la información que obre del sujeto obligado, particularmente, la que corresponde a datos personales, para que solo quede bajo la custodia de la Universidad Tecnológica Santa Catarina.

IV. Implementar los demás procedimientos y medidas de seguridad técnicas necesarias para el tratamiento y conservación de datos personales contenidos en sus archivos, registros, bancos y bases de datos, que deriven de lo dispuesto en la Ley y la demás normatividad aplicable.

F. **Medidas de seguridad en equipos computacionales que contengan documentos, archivos o sistemas de datos personales:**

I. Contar con seguridad de acceso lógico a los equipos como contraseñas en el sistema operativo para el personal autorizado.

II. Establecer restricciones de acceso a Internet, a los sitios que pudieran resultar dañinos o maliciosos, o bien, que pudieran permitir la transmisión de información de los datos personales de forma no autorizada.

III. Limitar o restringir por completo el uso de internet en los equipos que se estime pertinente.

IV. Establecer acceso restringido a la red, únicamente a los archivos o carpetas necesarias para el desempeño de funciones.

G. **Medidas de seguridad en caso de incendios.**

I. Se cuenta con detectores y sensores contra incendios, humos y gases, los cuales se encuentran ubicados en puntos estratégicos dentro de la Universidad Tecnológica Santa Catarina, a detectar un incendio emiten una señal avisando que el siniestro está ocurriendo en un lugar determinado.

II. Contar con extintores especiales para controlar los incendios en aparatos electrónicos.

H. **Otras**

I. Trituración mediante corte cruzado o en partículas, consiste en cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados “partículas”, lo cual hace prácticamente imposible que se puedan unir.

II. Destrucción de los medios de almacenamiento electrónicos a través de la desintegración, a fin de que deje de existir la información que se desea eliminar, se separa, completa o parcialmente los elementos que la conforman.

5. EL PLAN DE TRABAJO

De conformidad con los artículos 33, fracción VI, y 35, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 38, fracción VI, y 41, fracción V, y 58 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León; se presenta el plan de trabajo.

Se implementarán las medidas de seguridad faltantes y se efectuará la planeación de las acciones necesarias para dar cumplimiento a las medidas de seguridad plasmadas en el presente documento a través de los responsables de las unidades administrativas adscritas a la Universidad Tecnológica Santa Catarina, llevando un control periódico de las mismas a efecto de mitigar cualquier riesgo en relación con el tratamiento de los datos personales en los formatos respectivos.

6. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

De conformidad con los artículos 33, fracción VII, y 35, fracción VI, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 38, fracción VII, y 41, fracción VI, y 59 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León; se presenta los mecanismos de monitoreo y revisión de las medidas de seguridad.

A fin de supervisar y garantizar el cumplimiento y mejora continua de las medidas de seguridad que se encuentran implementadas en cuanto a la cultura de los empleados, el entorno de trabajo físico, así como el entorno de trabajo digital, se han definido controles de monitoreo periódicos que el Comité de Transparencia de la Universidad Tecnológica Santa Catarina aprobará en el plan anual de trabajo. Los resultados de las medidas implementadas deberán de ser informadas al mismo comité.

Las acciones, mecanismos y reportes deben estar relacionados con los siguientes factores.

A. Los nuevos activos que se incluyan en la gestión de riesgos.

B. Las modificaciones necesarias a los activos, como podría ser el cambio o migración de tecnología.

C. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas.

D. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

E. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

F. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgos,

G. Los incidentes y vulneraciones de seguridad ocurridas.

7. EL PROGRAMA GENERAL DE CAPACITACIÓN.

De conformidad con los artículos 33, fracción VIII, y 35, fracción VII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 38, fracción VIII, y 41, fracción VII, y 60 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León; se aborda el programa general de capacitación.

El programa de capacitación será aprobado por el Comité de Transparencia de la Universidad Tecnológica Santa Catarina y deberán de auxiliarse de los entes públicos expertos en la materia. Los resultados de dicho Comité deberán presentarse al mismo comité.

Los temas que debe incluir la capacitación deben ser en los siguientes temas:

A. Los requerimientos y actualizaciones de sistemas de gestión;

B. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;

C. Las consecuencias de incumplimiento de los requerimientos legales o requisitos organizacionales;

D. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.