Marco de referencia para la contratación de servicios de cómputo en la nube

Para la protección de datos personales

V1.2

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FIRMA DEL RESPONSABLE
1.0	Creación del documento	Jazmín Torres Blanco	Septiembre 2018	
1.0	Adecuaciones en apartado de seguridad del documento.	José Antonio Galván Estrada	Enero 2019	
1.1	Revisión del documento	Blanca Estela Carrillo Sánchez	Febrero 2019	
1.2	Actualización del documento	Blanca Estela Carrillo Sánchez	Agosto 2021	

CONTENIDO

OBJETIVO

Establecer un marco común de referencia que permita identificar a los responsables las medidas básicas de seguridad y cláusulas contractuales a considerar para la contratación y operación del servicio de cómputo en la nube con la finalidad de cumplir con los principios, deberes, derechos y obligaciones para la protección de los datos personales.

ALCANCE

El presente documento es aplicable para los órganos ejecutivos, técnicos de vigilancia, en materia de transparencia, y de control, a nivel central y desconcentrado que, por sus funciones, traten datos personales en el INE y que utilizan o pretendan utilizar el servicio de cómputo en la nube.

REFERENCIAS NORMATIVAS

- Ley General de Protección de Datos en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.
- Norma Mexicana NMX-I-27018-NYCE-2016.

TÉRMINOS Y DEFINICIONES

Aplicación cliente: Aplicación utilizada para conectarse de una computadora local a un servidor remoto.

Ciclo de vida de la información: Estados por los que pasa la información, desde su creación hasta la destrucción.

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Constancia o certificado de eliminación: Documento que indica de manera clara el proceso de eliminación segura, detallando cuándo, cómo y quién lo llevó a cabo.

Criptosistema: Conjunto de elementos (Texto plano, método de cifrado, claves, texto cifrado) que conforman el proceso de cifrado**.**

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

Datos personales sensibles: Aquellos que se refiere a la esfera más íntima del titular, o cuya y utilización indebida puede dar origen a discriminación que conlleve un riesgo grave para este. De manera enunciativa más no limitativa, se considera sensibles los datos personales que pueden relevar aspectos como origen racial o técnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Eliminación segura. Proceso a través del cual se hacen ilegibles o irrecuperables los datos en medios impresos o electrónicos, a pesar de aplicar un esfuerzo considerable al intentar recuperar los datos.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que solo o junto con otras, trate datos personales a nombre y por cuenta del responsable. En este caso, es el encargado del servicio de cómputo en la nube.

Evaluación de Impacto: Es un documento mediante el cual el responsable valora los impactos reales respecto de un tratamiento intensivo o relevante de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes, derechos y demás obligaciones en la materia.

Firewall: Dispositivo de seguridad que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

HTTPS: Protocolo de Transferencia de Hipertexto Seguro (Hyper Text Transfer Protocol Secure). Es un protocolo destinado a la transferencia segura de la información.

IaaS (Infrastructure as a Service)**:** Infraestructura como servicio. Servicio en donde un tercero proporciona una infraestructura de TI altamente automatizada y escalable (almacenamiento, alojamiento, procesamiento, redes)

ISO (International Organization for Standardization)**:** Organismo Internacional de Estandarización que busca la homologación de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

KMIP: Por sus siglas en ingles Key Management Interoperability Protocol.

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

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

Medidas de Seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.

Nube Pública: Modelo de cómputo en nube que considera el acceso público y es controlada por el encargado de servicios en la nube.

Nube Privada: Modelo de cómputo en la nube que establecido para una única organización.

PaaS (Platform as a Service**):** Plataforma como servicio. Servicio en donde los usuarios pueden desarrollar, ejecutar y administrar aplicaciones sin preocuparse por la infraestructura

Responsable: El área responsable de los datos personales.

Responsable: Los sujetos obligados a los que hace referencia el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que deciden sobre el tratamiento de los datos personales. En este caso el responsable serán las áreas dueñas de la información (responsables) de este Instituto que traten datos personales y utilicen o pretendan utilizar el servicio de cómputo en la nube.

Reglamento: Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

Remisión: Toda comunicación de datos personales realizados exclusivamente entre responsable y encargado, dentro o fuera del territorio mexicano.

SaaS (Software as a Service**)**: Software como servicio. Servicio que permite el alquiler y uso de aplicaciones instaladas y administradas por el proveedor de nube a través de internet.

SFTP (SSH File Transfer Protocol**):** Protocolo de transferencia de archivos segura. Protocolo de red que provee acceso, administración y transferencia de archivos sobre el flujo de datos utilizando técnicas de cifrado.

SOC: Controles de organización de servicio.

SSH: (Secure Shell): Protocolo que facilita la comunicación segura entre dos sistemas cifrando la sesión de conexión, lo cual permite que toda la información que viaja a través de él este cifrada.

Titular: La persona física a quien corresponden los datos personales.

TLS (Transport Layer Security): Protocolo criptográfico que protege toda información que se envía entre dos sistemas utilizando algoritmos de cifrado para que esta sólo sea leída por entes autorizados.

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

Usuario: El área autorizada para acceder a los datos. Son quienes utilizan la información.

Vulneración: Se refiere a la pérdida o destrucción, robo, extravió o copia no autorizada; el uso, acceso o tratamiento no autorizado; o el daño, la alteración o modificación no autorizada de los datos personales.

INTRODUCCIÓN

Los servicios de cómputo en la nube, en la actualidad, se han convertido en una herramienta que permite optimizar el tratamiento de la información al interior de las organizaciones.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en el artículo 30 señala que el responsable puede optar por cualquier mecanismo para el tratamiento de los datos personales, con el compromiso de que cumplan por defecto con las obligaciones que la misma establece; en su artículo 63, indica que el responsable puede contratar un servicio de cómputo en la nube, siempre que se garanticen las políticas de protección de datos personales, así como los deberes, derechos y principios, delimitando el tratamiento de los datos personales en contratos o instrumentos jurídicos.

La Ley General de Datos, en su artículo 3 fracción VI, define al cómputo en la nube como un modelo de provisión externa de servicio de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

El cómputo en la nube es un servicio que permite a las organizaciones optimizar el tratamiento de datos a través de infraestructura tecnológica (hardware y software) de un tercero que es utilizada y accedida bajo demanda a través de internet, que refiere un costo económico menor que cuando los datos son tratados en infraestructura tecnológica propia. Sin embargo, por las características propias del servicio, es necesario contar con cláusulas contractuales y medidas de seguridad específicas en caso de que la información en la nube contenga datos personales.

Adicional a lo anterior, el Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales, establece en su artículo 54 que *"El Instituto está obligado a prever cláusulas y obligaciones a cargo del encargado para asegurar que realice las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el Instituto, considerando al menos, las previstas en el artículo 59 de la Ley General, así como a observar lo dispuesto en el artículo 64 del mismo ordenamiento, tratándose de servicios de cómputo en la nube y otras materias".*

Por lo antes señalado, **la Unidad Técnica de Transparencia y Protección de Datos Personales (UTTyPDP) elaboró el presente documento, con la finalidad de que los responsables del tratamiento de los datos personales, al interior del Instituto, dispongan de un marco de referencia contractual y de seguridad cuando la información a tratarse a través de servicios de cómputo en la nube contenga datos personales**.

El presente documento se integra de la siguiente forma:

- El primer apartado establece la facultad que otorga la Ley General de Datos para la contratación del servicio de cómputo en la nube entre las que se encuentran las características que debe de cumplir el encargado de conformidad con la legislación, especificando políticas de protección y certificaciones; esto con la finalidad de que el responsable -en este caso las áreas de este Instituto- se cercioren de que el encargado brindará un servicio confiable y no pondrá en riesgo los datos de los titulares.
- En el segundo apartado, se determina la formalización de la relación jurídica entre el responsable y el encargado, esto a través de un contrato o cualquier instrumento jurídico, el cual deberá contener cláusulas bases con la finalidad de mitigar las vulneraciones; asimismo, se especifica el fuero en caso de controversias, debido a que el cómputo en la nube se caracteriza por la deslocalización.
  En este apartado se incluye la posibilidad de subcontratar un servicio. Al igual que en el caso del encargado, la Ley General de Datos establece las características que debe de cumplir el subcontratista, así como la manera de formalizar la relación contractual.
- El apartado de incumplimiento contempla las acciones que deben considerarse en el caso de que el encargado recaiga en cualquier supuesto de incumplimiento, señalando las sanciones –que pueden ser de carácter administrativo, civil o penal a las que se hará acreedor el encargado.
- Asimismo, se abordará el tema de la finalización del servicio, que puede derivar del término establecido por las partes o del incumplimiento del encargado. En dicho apartado se establecen las acciones resultado de la terminación de la relación entre responsable y encargado.
- Se dará una breve explicación de la evaluación de impacto, con base en las Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales[1].
- El último apartado trata sobre las medidas básicas de seguridad para la protección de los datos personales en el servicio de cómputo en la nube, que son las acciones mínimas que se deben cumplir para su tratamiento, en el servicio de cómputo en la nube, incluyendo procesos de autenticación y control de acceso.

[1] Publicadas en el Diario Oficial de la Federación el 23 de enero del 2018.

Marco de Referencia

1 BASES CONTRACTUALES

1.1 CARACTERÍSTICAS DEL ENCARGADO

La Ley General de Datos establece en su artículo 64 que en caso de que el responsable decida contratar servicios de cómputo en la nube, el encargado debe cumplir, al menos con lo siguiente:

I. **Tener y aplicar políticas de protección de datos personales afines a los principios, deberes y derechos que establece la Ley General de Datos y la normatividad mexicana**.

Por lo tanto, el responsable debe:

a) Comprobar que las políticas de protección de datos personales del posible encargado del servicio son compatibles con las establecidas en México; asimismo, que cumplan con los principios en la materia[2].

Para llevar a cabo lo anterior, se debe verificar que el posible encargado cuente con alguna de las siguientes certificaciones:

- ISO/IEC 27018[3]
- ISO/IEC 27001[4]
- SOC 1, SOC 2, SOC 3[5]

En caso de que la información contenga datos de tarjeta de crédito o débito, se recomienda:

- PCI DSS6

b) Analizar el aviso de privacidad del posible encargado del servicio para conocer los propósitos de la empresa, así como la forma en la que dan tratamiento a los datos personales, el cual deberá de contener como mínimo:

[2] Los principios que se encuentran contemplados en el artículo 16 de la Ley General de Datos, estos son: licitud, finalidad, lealtad, consentimiento, calidad, información y responsabilidad en el tratamiento de los datos personales.

[3] Para más información, consultar https://www.iso.org/standard/61498.html

[4] Para más información, consultar https://www.iso.org/isoiec-27001-information-security.html

[5]Para más información consultar: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html

[6] Para más información, consultar https://www.pcisecuritystandards.org/pci_security/

- La denominación del encargado, en su papel de responsable.
- Cómo clasifica y trata los datos del cliente.
- Las finalidades del tratamiento deberán de concordar con las del responsable.
- La manera en la que compartirán los datos, en las instalaciones de la institución y con terceros, si es el caso.
- La fecha del aviso de privacidad.
- El método que utilizaran para comunicar cambios en los avisos de privacidad.

c) Verificar que el encargado se abstenga de incluir condiciones en la prestación del servicio que le autorice o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
A continuación, se señala, de forma enunciativa y no limitativa, condiciones que el responsable **debe evitar incluir** en el clausulado:

- Permitir realizar pruebas con la información que se encuentre en la nube.
- Autorizar la eliminación de la información sin autorización del responsable.
- Consentir que generen respaldos de la información en una temporalidad no establecida en el instrumento legal donde conste su relación.
- Facultar al encargado de hacer uso de la información para fines diferentes a los pactados.

II. En sus procesos de contratación, disponga la **firma de convenios de confidencialidad** con cada persona que participe en el tratamiento de los datos personales, en los cuales se obligue al personal a guardar estricta confidencialidad de los datos personales tratados.

III. **Contar con procedimientos para informar al responsable sobre los cambios de sus políticas de privacidad o condiciones sobre los que se preste el servicio**, a través de un oficio o documento oficial que indique la razón de los cambios, así como el alcance que tendrán en el servicio, mismo que deberá estar firmado por la persona que fue designada como punto de contacto.

IV. **Contar con mecanismos para garantizar la supresión de los datos personales** a través del uso de técnicas de eliminación segura. Para profundizar el tema referirse al apartado 2.9 Eliminación segura de datos personales.

V. **Contar con mecanismos para impedir el acceso a personas que no cuenten con privilegios de acceso**. Para profundizar el tema referirse al apartado 2.2 Control de Acceso, de este documento.

VI. **Hacer del conocimiento al responsable la ubicación de sus centros de datos en donde se almacenará la información incluyendo los respaldos**. Lo anterior, con la finalidad de determinar los alcances normativos atendiendo a la ubicación geográfica de la infraestructura.

VII. Disposición de que el responsable seleccione la localización para el almacenamiento de los datos.

1.2 FORMALIZACIÓN DE LA RELACIÓN ENTRE RESPONSABLE-ENCARGADO

El responsable y el encargado deberán formalizar su relación, toda vez que de conformidad con lo establecido en el artículo 59 de la Ley General de Datos, esta formalización puede realizarse a través de un contrato o cualquier otro instrumento jurídico que decida el responsable, mismo que deberá contemplar en su clausulado, al menos, las siguientes **disposiciones para el encargado**:

a) Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.
b) Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
c) En caso de alguna vulneración, debe informar al responsable -en un plazo máximo de 36 horas a partir de su confirmación- a través de un oficio o documento oficial dirigido al administrador del contrato por parte del INE, marcando copia a los firmantes del contrato o instrumento jurídico en el cual conste:
    - La naturaleza del incidente.
    - La información que se vio comprometida.
    - El nombre de la persona que reporto el incidente.
    - Las acciones correctivas que utilizará el encargado para solucionar la vulneración, con base el procedimiento del punto anterior.
    - Las partes, encargado-responsable, deberán señalar un procedimiento para operar en caso de vulneraciones.
d) Guardar confidencialidad respecto a los datos tratados y establecerán convenios de confidencialidad con su personal.
e) Bloquear, suprimir o devolver los datos personales objeto de tratamiento, incluidos los respaldos, una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija su conservación[7], de conformidad con

[7] En el artículo 23 de la LGPDPPSO, se contempla el **bloqueo** de los datos personales. Este sentido el bloqueo se realiza con el **propósito de determinar responsabilidades en relación con su tratamiento**, hasta el plazo de prescripción legal o contractual, en ese periodo los datos no son objeto de tratamiento, se procede a la cancelación de la base de datos que corresponda.

el Cuadro General de Clasificación Archivística del INE[8]. El bloqueo y la supresión se profundiza en el apartado "2.9 Eliminación segura de los datos personales" de este documento.

f) Abstenerse de transferir los datos personales, salvo en caso de que:
   - El responsable así lo determine,
   - La comunicación derive de una subcontratación, o
   - Por mandato expreso de la autoridad competente.

   Lo anterior debe comunicarse mediante oficio o documentación oficial al administrador del contrato por parte del INE, marcando copia a los firmantes del contrato o instrumento jurídico, señalando lo siguiente:

   - La autoridad que solicitó la transferencia.
   - Acto que derivó la solicitud por parte de la autoridad.
   - Fecha de la transferencia.
   - Los datos personales que fueron transferidos.
   - Las medidas de seguridad que se implementaron en la transferencia.

Los Lineamiento Generales en su artículo 109, establecen que, además de lo señalado en el artículo 59 de la Ley General de Datos, se debe de contemplar en el clausulado que el encargado debe:

a) Permitir al responsable realizar verificaciones en el lugar donde se realice el tratamiento de los datos.
b) Colaborar con el INAI en las investigaciones y verificaciones proporcionando la información y documentación que se considere necesaria.
c) Contar con documentación actualizada con la que acredite el cumplimiento de sus obligaciones.

Así mismo, se considera necesario establecer en el contrato o instrumento jurídico, que el encargado deberá proporcionar al responsable las especificaciones principales que se plantean en su Plan de Recuperación de Desastres (DRP, por sus siglas en inglés), con la finalidad de que el responsable tenga los elementos base para actuar en caso de una contingencia.

En el contrato o instrumento jurídico en el que conste la relación entre el responsable y el encargado, el responsable debe especificar el propósito por el que realiza la contratación del servicio de cómputo en la nube, **delimitando el tipo de tratamiento que se dará a la información**, asimismo, **debe resaltar que la información que será tratada contiene datos**

[8] Disponible en: https://norma.ine.mx/unidades-tecnicas/unidad-tecnica-de-transparencia-y-proteccion-de-datos-personales/vigente/normativo/acuerdos

personales y, en su caso, señalar que se trata de datos personales y su categorización (ver el anexo IV).

El encargado se regirá por la normativa mexicana aplicable, con independencia a la ubicación geográfica. Por lo que todo conflicto derivado del servicio de cómputo en la nube se someterá a la jurisdicción de los tribunales competentes del Estado Mexicano, renunciando a cualquier otro fuero que pudiera corresponder debido a su ubicación geográfica.

1.2.1 SUBCONTRATACIONES

De conformidad con el artículo 61 de la Ley General de Datos y con relación al artículo 110 de los Lineamientos, el encargado podrá subcontratar el servicio, siempre y cuando cumpla lo siguiente:

a. Contar con la **autorización** del responsable de los datos de conformidad con lo establecido en el artículo 62 de la Ley General de Datos-a través de una cláusula contractual- en la que las partes acuerdan que el encargado podrá subcontratar servicios relacionados a la operación, sin que esto exima al encargado de dar aviso al responsable de su intención de subcontratar.
b. El encargado, mediante oficio o documento oficial, dará **aviso** al administrador del contrato por parte del INE, marcando copia a los firmantes del contrato o instrumento jurídico, sobre su intención de subcontratar el servicio, señalando: *la finalidad de la subcontratación, la temporalidad, así como la participación que tendrá el subcontratista en el tratamiento de los datos personales.*
c. En el caso que la empresa a la que se pretende subcontratar necesite certificaciones debido a los servicios que presta, el encargado remitirá, de manera electrónica al responsable del contrato por parte del INE con **copia** para el responsable y los firmantes del contrato o instrumento jurídico, el escaneo de las certificaciones con las que cuente. El encargado determinará la viabilidad de la subcontratación, en caso de que el responsable la autorice a través de un oficio o documento oficial.
d. El encargado deberá **formalizar** la relación que tendrá con el subcontratista a través de un contrato o cualquier instrumento jurídico que decida, señalando el objeto y los alcances del servicio que será brindado, así como la relación contractual entre el responsable y el encargado, además de lo que establece la Ley General de Datos en particular para el subcontratista. Dicho contrato o instrumento jurídico una vez que sea firmado, deberá ser remitido al administrador del contrato por parte del INE en copia.

1.3 VERIFICACIÓN DE ACCESOS

El responsable –de manera interna o a través de la contratación de un tercero- debe auditar los accesos en la nube con la finalidad de determinar las personas que accedieron al servicio y el tipo de información que trataron. Los plazos para realizar la auditoría los determinará el responsable de los datos personales atendiendo a sus actividades. Lo anterior, debe quedar establecido en las cláusulas contractuales.

En el caso de una solicitud fundada y motivada de una autoridad competente de acceso a la información, el encargado deberá informar al administrador del contrato y con copia para las personas que hayan firmado el contrato o instrumento jurídico por parte del INE, mediante oficio o documento oficial, en el que se especifique:

- Fecha de la solicitud.
- Tipo de solicitud.
- Acto que derivó la solicitud por parte de la autoridad.
- Tipo de información a la cuál solicitó acceso.
- Medidas que aplicará el encargado respecto a la solicitud.

El responsable no debe adherirse a un servicio que no cumpla con lo antes establecido, toda vez que no garantizará la protección de los datos personales de los titulares, atendiendo a lo establecido en el artículo 19 de la Ley General de Datos y el artículo 18 del Reglamento.[9]

1.4 INCUMPLIMIENTO

De conformidad con lo establecido en el artículo 60 de la Ley General de Datos, mismo que se relaciona con el artículo 112 de los Lineamientos, en caso de que el encargado o subcontratista incumpla con lo establecido en el contrato o en el instrumento jurídico donde conste la relación del responsable – a través de la figura del responsable- con el encargado, o en su caso, incumpla con los principios establecidos por la Ley General de Datos, recaerá en un supuesto de **incumplimiento**.

Cabe destacar que no existirá un catálogo sobre acciones de incumplimiento, puesto que será derivado de lo establecido en el contrato o instrumento jurídico que pacten las partes, por lo tanto, se proporcionan ejemplos enunciativos más no limitativos de causas de incumplimiento, como son:

- El encargado da a conocer información almacenada en la nube, violando la confidencialidad.

[9] Los artículos mencionados establecen el principio de lealtad, por el que el responsable no debe de obtener ni tratar datos personales a través de medios fraudulentos o engañosos, privilegiando la protección de datos del titular.

- El encargado no da aviso al responsable sobre actos de vulneración a la seguridad de los datos personales.
- El encargado no cuenta con certificaciones vigentes.
- El encargado no realiza acciones de eliminación segura de datos.
- El encargado trata los datos de una forma diversa a los señalados por el responsable.
- No cumplir con lo establecido en los niveles de servicio (*SLA por sus siglas en inglés*).

En el contrato o el instrumento jurídico donde conste la relación de las partes, se deberán señalar las consecuencias del incumplimiento, estableciendo por parte del responsable, por lo menos lo siguiente:

- Dar por terminada la relación con el encargado.
- Instruir al encargado la restauración de la información, ya sea a la infraestructura del INE o a los servidores de un nuevo encargado.
- Solicitar la eliminación segura de los datos personales que consten en la nube, atendiendo a lo establecido en el apartado "2.9 Eliminación segura de los datos personales" de este documento.

Derivado del incumplimiento, el encargado será sujeto de sanciones, mismas que deberán establecerse en el contrato, en atención a lo establecido en el artículo 60 de la Ley General de Datos. [10]

El artículo 163 de la Ley General de Datos señala las causas de sanción por incumplimiento, las cuales el responsable debe tomar en cuenta para sancionar al encargado, sin olvidar que es causa de incumplimiento no acatar lo establecido en el contrato o instrumento jurídico celebrado.

Las causas contempladas en el artículo en comento son las siguientes:

- Actuar con negligencia, dolo o mala fe al atender solicitudes para el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).
- Incumplir en los plazos para dar respuestas a las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo su derecho.
- Usar, sustraer, divulgar, ocultar, mutilar, destruir o inutilizar total o parcialmente y de manera indebida los datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento.

[10] Dicho artículo establece que en caso de incumplimiento el encargado asumirá el carácter de responsable.

- Dar tratamiento, de manera intencionada, a los datos personales en contravención a los principios o deberes establecidos en la normatividad aplicables.
- No contar con un aviso de privacidad o que dicho acuerdo no cuente con los elementos establecidos en el artículo 27 de la Ley General de Datos.
- Incumplir con el deber de confidencialidad.
- No establecer medidas de seguridad.
- Presentar vulneraciones a la seguridad de los datos personales por falta de implementación de medidas de seguridad.
- Llevar a cabo transferencias de datos personales, en contravención de la Ley General de Datos o en lo pactado en el contrato o instrumento jurídico celebrado entre las partes.
- Obstruir en la verificación de la autoridad.
- Crear bases de datos con la información proporcionada por el responsable sin su instrucción o autorización, que no provenga de fuentes de acceso público[11]. El artículo 5 de la Ley General de Datos, señala las siguientes:
    - Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;
    - Los directorios telefónicos en términos de la normativa específica;
    - Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;
    - Los medios de comunicación social, y
    - Los registros públicos conforme a las disposiciones que les resulten aplicables.

Además, el responsable debe de tomar en cuenta lo establecido en el artículo 165 de la Ley General de Datos, la cual ordena que sean las sanciones penales, administrativas y civiles sean independientes.

En el caso de **sanciones penales**, se encuentran contempladas en los artículos 211 bis 2 y 211 bis 3 del El Código Penal Federal, Título Noveno Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, a continuación, se señalan algunas de las sanciones establecidas en la normatividad en materia penal.

- **Artículo 211 bis 2.** Al que *sin autorización modifique, destruya o provoque pérdida de información* contenida en sistemas o equipos de informática del Estado,

[11] Para que sea considerada fuente de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contra prestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita (articulo 5, Ley General de Datos).

protegidos por algún mecanismo de seguridad, se le impondrán de *uno a cuatro años de prisión y de doscientos a seiscientos días multa*.

Al que *sin autorización conozca o copie información* contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de *seis meses a dos años de prisión y de cien a trescientos días multa.* […]

- **Artículo 211 bis 3.** Al que, *estando autorizado para acceder* a sistemas y equipos de informática del Estado, *indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa*.

  Al que, estando *autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información* que contengan, se le impondrán de *uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa*. […]

Referente a las **responsabilidades administrativas**, estas serán de conformidad con la Ley General de Responsabilidades Administrativas, en razón de que la Ley General de Datos establece en su artículo 60 que, en caso de *incumplimiento el encargado, asumirá el carácter de responsable.*

En cuanto a las **sanciones civiles**, en caso de que exista un incumplimiento de contrato se deberá atender a lo establecido en el Libro Cuarto, Titulo Cuarto, Capítulo I del Código Civil Federal, en el cual se establece el incumplimiento de las obligaciones.

Cabe señalar que el presente apartado opera de la misma manera en cuestiones de incumplimiento por parte del subcontratista, cuando se afecte a la protección de los datos personales.

1.5 FINALIZACIÓN DEL SERVICIO

El responsable podrá dar por terminado el contrato atendiendo a la vigencia pactada por las partes o derivado del incumplimiento, visto en el apartado 1.4 Incumplimiento.

El encargado deberá entregar al responsable un respaldo actualizado de la información que se encuentra en la nube. El procedimiento de entrega la determinará el responsable atendiendo a sus actividades; asimismo, fijará el tiempo en el que el encargado deberá entregar la copia de la información tomando las medidas necesarias para realizar la eliminación de los datos personales, con forme a lo establecido en el apartado “2.9 Eliminación segura de los datos personales” de este documento.

Para la parte técnica, el proceso de término o conclusión del servicio requiere de medidas de seguridad como:

- Establecer que ninguno de los datos del responsable permanezca con el encargado, lo cual debe establecerse en los acuerdos contractuales de confidencialidad.
- El encargado deberá de asegurarse que cualquier copia que tenga, donde sea que haya sido almacenada se elimine de manera segura, lo anterior incluyendo copias de seguridad.

Al finalizar el servicio, el encargado deberá entregar al responsable un documento de confirmación en el que indique que el servicio está concluido y que los datos de los clientes han sido eliminados de la nube.

Los documentos de auditoría y eventos asociados deben conservarse según lo señalado en el Cuadro General de Clasificación Archivística.

1.6 EVALUACIÓN DE IMPACTO

En el supuesto de que los datos personales alojados en la nube sean sometidos (o se presuma que puedan ser sometidos) a un tratamiento intensivo, el responsable deberá llevar a cabo una evaluación de impacto.

Conforme a lo dispuesto en las Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales (en adelante Disposiciones)[12], se incluye, como tratamiento intensivo o relevante de datos personales, las siguientes acciones:

a) De carácter general

- Existan riesgos inherentes[13] a los datos personales a tratar, entendiéndolos como el valor potencial cualitativo[14] o cuantitativo[15], que pudieran tener estos para una tercera persona o persona no autorizada.
- Se traten datos sensibles.
- Se efectúen o pretendan hacer una transferencia de datos personales.

b) De carácter particular

- Cambiar la o las finalidades que justifiquen el tratamiento de los datos personales, generando incompatibilidad con las finalidades que originaron la captación.

[12] Consultar en https://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018
[13] Entendiéndose como el riesgo asociado a los datos, con base en la susceptibilidad del dato, sin tener en cuenta los controles que pudieran protegerlo.
[14] La asignación de un valor monetario al riesgo asociado con el dato.
[15] La valoración del riesgo se realiza tomando las características de las bases de datos en el escenario del riesgo, esto es la calificación del riesgo asignado a la base como básico, moderado, crítico y severo.

- Realizar acciones tendientes a la creación de perfiles, que produzcan efectos jurídicos, que establezcan o puedan establecer diferencias de trato o discriminación.
- Tratar datos personales de grupos vulnerables o datos sensibles.
- Crear bases de datos con número elevado de titulares.
- Incluir o agregar categorías de datos personales a bases que se tengan, por lo que es posible que se presente una vulneración que afecte a la esfera del titular.
- Realizar un tratamiento frecuente y continuo de grandes volúmenes de datos personales.
- Utilizar tecnologías que impliquen tratamiento de datos personales a gran escala, se señalan de forma enunciativa y no limitativa sistema de video vigilancia, minería de datos, biometría, geolocalización y tecnología de las cosas.
- Permitir acceso de terceros a grandes cantidades de datos que anteriormente no tenían acceso.
- Realizar transferencias internacionales con países que no garanticen la protección de los datos personales.
- Revertir la disociación de datos personales para finalidades determinadas.
- Realizar un tratamiento a gran escala de datos sensibles o relativos a condenas o infracciones penales.
- La observación sistemática a gran escala de una zona de acceso pública.

Como lo establece la Ley General de Datos en su artículo 74, el responsable tiene la obligación de realizar una evaluación de impacto, en caso de que pretenda poner en operación y/o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier tecnología que implique un **tratamiento intensivo**.

Las Disposiciones contemplan la opinión técnica del Oficial de Protección de Datos –artículo 27. A la fecha, el INE no cuenta con dicha figura, por lo que las áreas deberán elaborar junto con la Unidad Técnica de Transparencia y Protección de Datos Personales, la evaluación de impacto, atendiendo a lo señalado en los artículos 14 al 21 de las Disposiciones.

La evaluación de impacto deberá contener al menos la siguiente información:

- La **descripción** de la política pública, programa, sistema o plataforma informática, aplicación informativa o cualquier otra tecnología que implique un tratamiento intensivo.
- La **justificación** de la necesidad de implementación.
- La **representación** del ciclo de vida de los datos personales a tratar.
- La **identificación**, análisis y descripción de la gestión de riesgos inherentes para la protección de datos personales.

- El **análisis** de cumplimiento normativo en materia de protección de datos personales, de conformidad con lo establecido en la normatividad aplicable.
- En caso de que se haya efectuado una consulta externa, los resultados de esta.
- Cualquier otra información que se considere relevante.

Cabe señalar, que existen excepciones para llevar a cabo la evaluación de impacto, estas son:

- En el caso de que se comprometan los efectos que se buscan al implementar la política pública, programa, sistema o plataforma informática, aplicación informativa o cualquier otra tecnología que implique un tratamiento intensivo,
- En el caso de emergencia o urgencia.

2 ESPECIFICACIONES DE SEGURIDAD

Las medidas que se describen a continuación son las mínimas requeridas para asegurar el tratamiento de los datos personales en el servicio de cómputo en la nube; se debe considerar, además, que el proveedor de servicios en la nube debe cumplir con la norma internacional ISO/IEC 27017:2015[16] e ISO/IEC 27018:2019[17].

Para determinar e implementar medidas de seguridad eficientes y eficaces es necesario considerar:

a) El número de titulares a los que pertenecen los datos personales y el tipo de estos,
b) El resultado de los análisis de riesgos que se ejecuten, y
c) El resultado de la evaluación de impacto -en caso de aplicar- del servicio de nube que se requiere implementar.

Las medidas de seguridad en el tratamiento de los datos personales dependerán de su clasificación (estándar, sensible, especial).

2.1 RESPONSABILIDAD COMPARTIDA

En función del servicio contratado -Saas, PaaS o IaaS-, será el grado de control que el responsable de los datos personales tenga de los componentes de software y hardware que conforman la nube y del nivel de seguridad que es posible aplicar al servicio y por consecuencia a los datos que se manejan.

[16] Para más información, consultar: https://www.iso.org/standard/43757.html
[17] Para más información, consultar: https://www.iso.org/standard/76559.html

La seguridad en la nube es una responsabilidad compartida, donde el encargado es responsable del correcto funcionamiento de la nube y el responsable, dependiendo del servicio, de la administración de componentes y de los datos que se encuentran en la misma.

Las obligaciones del responsable y encargado se verán afectadas de acuerdo con los servicios que se requieran. De manera general se listan las siguientes:

- El encargado opera, administra y controla los recursos de los componentes del sistema operativo, de la capa de virtualización, de middleware, infraestructura tecnológica del anfitrión o host y ofrece la seguridad física en las instalaciones en las que se encuentran los servidores.
- El responsable asume la responsabilidad y la administración -entre otros elementos y dependiendo del servicio- del sistema invitado o huésped, de cualquier otro software de aplicación asociada, así como de la configuración de componentes de seguridad.

Las gráficas ejemplifican lo señalado anteriormente:

Figura 3 Responsabilidad en servicio tipo IaaS

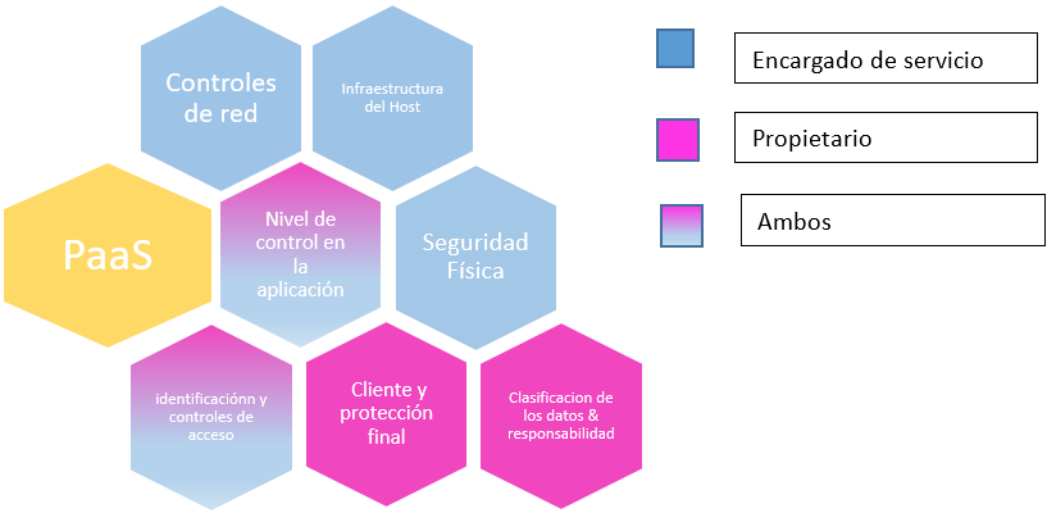

Figura 2 Responsabilidad en servicio tipo PaaS

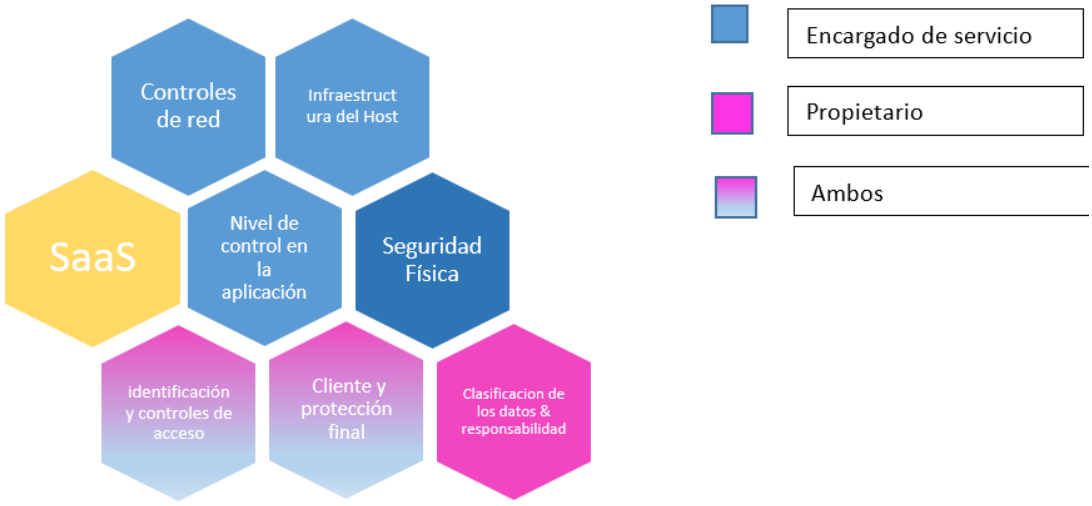

Figura 1 Responsabilidad en servicio tipo SaaS

2.2 CONTROL DE ACCESO

El encargado y el responsable, en sus respectivos ámbitos de responsabilidades, atendiendo al esquema de servicio contratado, deberán considerar el listado que a continuación se presenta y deberán contar con los procedimientos respectivos para ello:

a) Administrar la asignación de cuentas de usuario –altas, bajas y cambios- para las personas y/o aplicaciones que requieran acceder a la información y sistemas que la tratan.
b) La creación de cuentas de usuario debe estar autorizada y/o aprobadas por el responsable; dicha aprobación debe estar alineada a las funciones y/o roles que el usuario desempeñe para el desempeño de sus actividades.
c) Administrar la asignación, revocación, supresión y modificación de los privilegios de acceso a la información y sistemas de información otorgados a los usuarios y/o aplicaciones con base en sus roles.
d) Para lo anterior, considerar siempre el principio de menor privilegio y necesidad de saber (*Need-to-know*), es decir, prohibir todo acceso salvo que esté expresamente permitido.
e) Disponer de, al menos, un mecanismo de autenticación para los dispositivos antes de permitir el acceso a los sistemas de información.
f) Denegar el acceso y uso de la información del sistema de datos personales y la infraestructura que lo soporta, a todos los usuarios y dispositivos no autorizados.
g) Disponer de un monitoreo de accesos de usuario.
h) Uso de certificados digitales emitidos por autoridades certificadoras autorizadas para la autenticación de los servidores.
i) Uso de canales de comunicación cifrados.
j) Uso de contraseñas de usuarios robustas considerando al menos; longitud, minúsculas, mayúsculas, números y caracteres especiales.
k) Temporalidad y no coincidencia con contraseñas anteriores.
l) Es aconsejable la autenticación multifactor para los usuarios.

Además de lo anterior, el encargado deberá disponer de un documento que contenga:

a) El listado de usuarios autorizados con accesos a los centros de cómputo donde reside la información; esta lista deberá mantenerse actualizada.
b) La bitácora de accesos a los servidores donde reside la información, identificando detalladamente los accesos realizados por usuario con su respectiva autorización, esta debe contar con, al menos: nombre del usuario, fecha y hora del acceso, sistema accedido, tipo de acceso y si éste fue autorizado o denegado, cantidad de accesos fallidos, dirección IP desde donde se acceso.

c) Los datos no podrán ser indexados por ningún motor de búsquedas, sin previo consentimiento del responsable.
d) El encargado deberá entregar las bitácoras que se le soliciten en caso de sufrir algún incidente.
e) Los mecanismos de seguridad para acceso de los usuarios u otras entidades[18]al sistema, lo que implicará proteger tanto el acceso en sí mismo como el canal de acceso remoto.

2.2.1 MECANISMOS DE AUTENTICACIÓN

Con relación a la verificación de la identidad del personal que tienen acceso al servicio de cómputo en la nube, se deberá especificar en el contrato o en cualquier otro instrumento jurídico que:

a) Las credenciales[19] estarán bajo el control exclusivo del responsable.
b) El responsable reconocerá que recibió las credenciales, y que conoce y acepta las obligaciones que implica tenerlas (el deber de debida diligencia, protección de su confidencialidad e información inmediata en caso de pérdida).
c) En el caso que se requiera compartir la contraseña entre uno o más usuarios, deberá ser documentado.
d) Las credenciales se cambiarán con una periodicidad marcada por el responsable, atendiendo a la categoría del sistema al que se accede.
e) Las credenciales se retirarán y serán deshabilitadas cuando la entidad a la que autentican dichas credenciales termina su relación con el sistema.
f) Las credenciales se suspenderán tras un periodo definido de no utilización, el cual debe definirse claramente.
g) Para la información secreta de autenticación de usuario, se deben establecer mecanismos de control para que no pueda ser descubierta, revelada o visualizada.
h) Determinar si es posible el uso de dos factores de autenticación.
i) Son aceptables los siguientes métodos y protocolos de autenticación:
    - Token USB
    - Kerberos
    - RADIUS (*Remote Authentication Dial-In User Server*),
    - TLS (*Transport Layer Security*),
    - IPSec (*IP Security*)
    - EAP (*Extensible Authentication Protocol*),

[18] Se entenderá como entidad una persona, equipo o proceso.
[19] Se entenderá como credenciales los mecanismos de autenticación que se utilicen en el sistema, pudiendo ser: algo que se tiene, algo que se sabe o algo que se es.

2.3 CIFRADO DE LA INFORMACIÓN EN TRÁNSITO Y EN REPOSO

Para proteger datos personales sensibles es fundamental que se encuentren resguardados utilizando algoritmos robustos de cifrado. Por lo tanto, se recomienda especificar, en el contrato o cualquier otro instrumento jurídico, lo siguiente:

a) Cifrar los datos personales durante su almacenamiento (en reposo).
b) Garantizar la autenticidad y no-repudio del emisor.
c) Comunicar y transmitir los datos de manera cifrada desde los servidores de cómputo en la nube y las estaciones clientes (en tránsito):[20]
    - Cifrado de canales de transmisión de datos (VPN/TLS);
    - Cifrado y firmado de correo electrónico;
    - Interconexión de centros de datos (LAN TO LAN, L2L);
d) Incorporar, al menos, un algoritmo de cifrado simétrico para cifrar los archivos electrónicos que contienen datos personales antes de su transmisión o almacenamiento, tomando en cuenta que para otorgar un nivel de seguridad equivalente a 128[21] bits se supone el uso de:
    - Claves de 128 bits (o superiores) para el sistema de cifrado simétrico AES.
    - Claves de entre 256 y 283 bits para los sistemas basados en curvas elípticas.
    - Claves de al menos 3072 bits para el criptosistema RSA.

Se recomienda que las claves criptográficas sean generadas en dispositivos criptográficos basados en hardware, conocidos como HSM (Hardware Security Module)[22] y se deben proteger durante todo su ciclo de vida, es decir, en la generación, transporte, custodia durante la operación, el archivado posterior a su retirada de operación activa y su destrucción final, considerando lo siguiente:

- Los dispositivos criptográficos estarán aislados de los medios de explotación.
- El archivado de las claves de operación que requieran ser retiradas, deberá realizarse en medios separados de los de operación.

2.3.1 CONSIDERACIONES PARA EL CIFRADO DE DATOS EN REPOSO

Para realizar el cifrado de los datos en reposo se sugiere aplicar, en la medida de lo posible, un cifrado selectivo, es decir, elegir únicamente los campos, columnas o bases de datos que contengan datos personales.

[20] Se entenderá como cliente el equipo que está conectado a una red local de computadoras
[21] Para más información consultar: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/guias-de-acceso-publico-ccn-stic.html
[22] Para más información, consultar https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

La decisión del enfoque a tomar dependerá de las capacidades tecnológicas proporcionadas por el encargado y de las necesidades de seguridad del responsable con base en el tipo de dato personal. Algunas recomendaciones generales para aplicar el cifrado a la información son:

a) El algoritmo para el cifrado debe estar soportado por estándares[23].
b) Las llaves no deben almacenarse junto a los datos:
   - Para IaaS y PaaS las llaves las puede almacenar el responsable y pasar a la aplicación según sean necesario.
   - El cifrado en SaaS es responsabilidad del encargado. Además del cifrado, se debe verificar que cuenten con un procedimiento de supervisión de la actividad de la base de datos, así como la exploración de vulnerabilidades.

2.3.2 CONSIDERACIONES PARA EL CIFRADO DE DATOS EN TRÁNSTIO

Respecto a los datos en tránsito, se sugiere considerar los estándares según lo requerido, es decir, implementar HTTPS para las conexiones de clientes al servicio de nube a través de internet, SFTP si realiza transferencia masiva de datos y TLS 1.2 (preferentemente TLS 1.3) para proveer una conexión segura y privada entre dos aplicaciones.

Respecto a los controles para confidencialidad e integridad de las transmisiones de datos en movimiento –con respecto al cifrado de la información- se pueden considerar como referencia los controles de seguridad SC-8 (SISTEMA Y PROTECCIÓN DE COMUNICACIONES)[24].

2.4 TRANSMISIÓN SEGURA DE LA INFORMACIÓN

Dependiendo del nivel del servicio, el responsable o el encargado, según sea el caso deberá verificar:

a) Que la transmisión de información se realice desde y hacia los entes autorizados, en tiempo y forma (utilizando mecanismos como estampa de tiempo, firma digital, entre otras), y sobre medios de transmisión seguros, empleando algoritmos criptográficos robustos. Es altamente recomendable implementar la última versión de TLS[25].
b) Tener una lista actualizada de los entes autorizados para el envío y recepción de los datos.
c) La firma electrónica para la estampa de tiempo se hará mediante una clave RSA de, al menos, 3072 bits, recomendándose el uso de 4096 bits, o curvas elípticas con

[23] Para más información, consultar https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
[24] Para más información, consultar https://nvd.nist.gov/800-53/Rev4/control/SC-8
[25] Para más información, consultar https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

claves de, al menos, 284 bits, y una función resumen (HASH) de las incluidas en la serie SHA-2 o SHA-3 con una seguridad mayor o igual que SHA-256.

2.4.1 TIME STAMP

Los sellos de tiempo (*timestamp o timestamping*) previenen la posibilidad del repudio posterior (no-repudio):

a) Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia técnica y jurídica en el futuro.
b) Los elementos que contiene el *timestamp* para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
c) Si la información seguirá en tratamiento, se deben renovar regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida.
d) Los sellos de tiempo deben atender lo establecido en el RFC 3161 "Internet X.509 *Public Key Infraestructure Time Stamp Protocols*".

2.4.2 FIRMA DIGITAL

Se sugiere el uso de la Firma Electrónica Avanzada del Instituto[26] para comprobar la autenticidad de la procedencia y la integridad de la información, ofreciendo las bases para evitar el repudio.

La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionales a los niveles de seguridad requeridos por el sistema:

a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados digitales, estos deberán ser emitidos por autoridades certificadoras válidas y autorizadas por otras entidades de mayor confianza, hasta llegar a la autoridad de mayor jerarquía –Autoridad Certificadora Raíz-, es decir, debe ser clara la ruta de certificación del certificado digital utilizado.
b) Se debe revisar y validar la vigencia del certificado digital cada vez que se verifique la procedencia e integridad de la información, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la política de firma electrónica. En ese caso, se adjuntará al certificado digital, o se referenciará, toda la información pertinente para su verificación y validación.

[26] Consultar https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/86280/CGex201310-28_ap_8_x1.pdf?sequence=2&isAllowed=y

De acuerdo con los lineamientos específicos para el uso de la firma electrónica, todas las evidencias criptográficas de la firma, incluyendo su verificación en un periodo posterior, se registrarán y en su caso se obtendrán de la infraestructura tecnológica de la Firma Electrónica Avanzada.

2.5 SEGURIDAD EN LA RED

El responsable debe implementar los mecanismos de seguridad entre la red del encargado y la red del responsable para que la transferencia de la información transmitida sea llevada a cabo de manera segura; además, el responsable y el encargado deben determinar la segmentación de sus redes de comunicaciones de acuerdo la sensibilidad de los activos que se encuentran conectados a ella.

La segmentación de la red deberá garantizar:

a) Una correcta gestión de usuarios para cada segmento de la red.
b) El control de tráfico de entrada en cada segmento.
c) El control de tráfico de salida de la información en cada segmento.
d) Las redes se pueden segmentar por dispositivos físicos o lógicos; el único requisito es que el punto de interconexión debe estar asegurado, mantenido y monitorizado.

Además, se deberá de disponer de:

a) Un firewall que separe la red interna del exterior. Todo el tráfico deberá pasar por el firewall que sólo deje transitar los flujos previamente autorizados.
b) Se debe adoptar una política de menor privilegio para los puertos de comunicación, de tal manera que únicamente los puertos estrictamente necesarios deben estar habilitados.
c) Se recomienda contar con dos o más equipos de firewall de diferentes fabricantes, dispuestos en cascada.
d) Se dispondrán firewalls redundantes.

Se recomienda que el encargado cuente con los controles de seguridad de red alineados con las normas ISO/IEC 27001:2013 e ISO/IEC 27033:2015[27]. Si los encargados no cuentan con la certificación ISO/IEC 27001:2013, pueden proporcionar un informe certificado sobre los controles, como un informe tipo SOC2.

Sin embargo, se debe considerar que, si no cuenta con una certificación o un certificado de los ya mencionados, el responsable deberá asegurarse que el encargado haya documentado y aprobado procesos para:

[27] Para mayor información, consultar https://www.iso.org/standard/63461.html

- Controles de acceso para la administración de la red.
- Gestión adecuada de vulnerabilidades de la infraestructura de la red.
- Segmentación de redes apropiada, es decir, separación de redes dependiendo su sensibilidad.
- Filtrado de tráfico, detección y prevención de intrusos.
- Mitigación de los efectos de ataques.
- Registro y notificación de eventos.
- Monitoreo de seguridad.

Finalmente, si es posible, considerar los siguientes controles:

- *SC-7 Boundary Protection* [28].
- *SC-8 Transmission Confidentiality and Integrity*[29].
- *FedRAMP (Federal Risk and Authorization Management Program)*[30]

2.6 RESPALDOS

El encargado y el responsable, en conjunto, deben definir una política de respaldos y replicación (*backups*) de datos almacenados en la nube.

El encargado:

a) Deberá realizar copias de seguridad con una periodicidad establecida por el responsable, que permita recuperar datos perdidos, accidental o intencionadamente.
b) Deberá realizar las copias de seguridad de acuerdo con el tipo de respaldo –Completo, incremental o diferencial-, definida en la política de respaldos y replicación.
c) Deberá cifrar las copias de seguridad de acuerdo con los requerimientos establecidos en la política de respaldos y replicación.
d) Deberán ser almacenadas en medios de almacenamientos distintos a los que contienen los datos originales.
e) Las copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad.
f) Contar con flexibilidad o interoperabilidad para que, en su caso, se puedan realizar respaldos con las herramientas institucionales.
g) Contar con flexibilidad o interoperabilidad para exportar los respaldos realizados.
h) Proteger el acceso a los respaldos mediante mecanismos de autenticación.

[28] Para mayor información, consultar https://nvd.nist.gov/800-53/Rev4/control/SC-7
[29] Para mayor información, consultar https://cyuber.co.uk/security-controls/system-communications-protection-sc/transmission-confidentiality-integrity-sc-8/
[30] Para mayor información, consultar https://www.fedramp.gov/

i) Los procedimientos para las copias de seguridad deberán contener:
   - La información con la cual trabaja el personal del responsable.
   - Qué aplicaciones de operación tratan los datos, incluyendo los sistemas operativos.
   - Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
   - Claves utilizadas para preservar la confidencialidad de la información.
   - Bitácora de respaldos, incluyendo los medios y ubicaciones donde se resguarda.

j) Definir procedimientos y/o instrucciones de operación para que el responsable pueda realizar respaldos y recuperación de la información de los datos, sistemas operacionales y aplicaciones, cuando así lo requiera.

k) Realizar pruebas regulares de los respaldos realizados para asegurarse que estos son confiables en caso de alguna contingencia que requiera su restauración, lo anterior de acuerdo con lo que estipule la política de respaldos y replicación del Instituto.

l) Contar con procedimientos para realizar de restauración de los respaldos, considerando que no se deben sobrescribir los datos originales en caso de que la restauración falle.

2.7 PROTECCIÓN CONTRA CÓDIGO MALICIOSO

El encargado debe contar son sistemas para asegurar que la información y sistemas de procesamiento de información estén protegidas contra código malicioso, considerando, al menos, lo siguiente:

a) Contar con herramientas suficientes y adecuadas para recuperar cualquier sistema de un ataque a la infraestructura por medio de códigos maliciosos.

b) Mecanismos de control con el fin de evitar que usuarios y personal de soporte puedan realizar instalaciones no autorizadas de software en la infraestructura que soporta los sistemas del servicio de nube contratado.

c) Contar con herramientas que escaneen contra código malicioso, previo a su uso, cualquier archivo recibido a través de la red u otro medio.

d) Todo activo de información con capacidad de conectarse a los servicios de nube y a la red, deberá contar con herramientas de protección contra código malicioso.

e) Las herramientas deben contar con mecanismos automáticos de actualización con el fin de mantener vigente la protección en contra de cualquier código malicioso.

f) Procedimientos y responsabilidades para acordar protección contra código malicioso sobre los sistemas, así como la debida capacitación sobre su uso, notificación y recuperación posterior a los ataques de estos.

g) Procedimientos de aislamiento de ambientes en el caso que el mismo sea atacado por códigos maliciosos.
h) Procedimiento para las instalaciones y actualizaciones de software de protección de código malicioso, así como para las reparaciones en caso de afectación, lo cual deberá cubrir a su vez:
    - Escanear contra código malicioso, previo a su uso, cualquier archivo recibido a través de la red.
    - Los anexos de correos electrónicos y otros medios, por ejemplo; servidores de correo electrónico y anexos de páginas web.
i) La alineación con los planes de continuidad en relación con la recuperación posterior a los ataques de código malicioso, tanto de datos como de aplicaciones.

2.8 PLAN DE RECUPERACIÓN EN CASO DE DESASTRES

El encargado debe tener definido un plan de recuperación en caso de desastres (*DRP por sus siglas en inglés*) en el cual se considere, al menos, lo siguiente:

a) La descripción de las acciones que se llevarán a cabo para la recuperación ante un fallo.
b) Los planes para responder y recuperarse deben mantener la información segura durante todo el incidente.
c) La ejecución de ejercicios o simulacros para asegurar que la recuperación sea eficiente y es consistente con los requerimientos del responsable.
d) La continua operación de los controles de seguridad; de no ser posible, la adopción de controles de seguridad compensatorios en caso de que los controles establecidos no puedan ser mantenidos durante el incidente.
e) Los mecanismos de comunicación con el responsable.

En caso de que haya ocurrido un desastre natural o humano, el encargado deberá especificar las medidas que tomará para mitigarlo, restaurar el servicio tan rápido como sea posible, así como realizar las mejoras necesarias y mantener en todo momento informado al responsable.

El encargado deberá disponer de un Plan de Continuidad del Negocio (*BCP por sus siglas en inglés*) que establezca las acciones a ejecutar en caso de interrupción de los servicios. Este plan contemplará, al menos, los siguientes aspectos:

a) Identificación de funciones, responsabilidades y actividades a realizar.
b) Análisis de los medios alternativos que se va a seleccionar para poder seguir prestando los servicios.

c) Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los encargados correspondientes.

2.9 ELIMINACIÓN SEGURA DE LOS DATOS PERSONALES

Cuando la relación contractual entre responsable-encargado finalice o cuando el responsable determine eliminar información de la nube, atendiendo al principio de calidad y finalidad de los datos personales, el encargado debe de:

a) Eliminar de manera segura e irrecuperable los datos almacenados y tratados por todos los sistemas que se especifiquen, incluyendo los *backups* que no sean entregados al responsable.
b) Incluir la información almacenada en los archivos temporales de aplicaciones y sistema operativo, la información en memoria virtual y registro de transacciones de base de datos en el borrado seguro de información.
c) Considerar estándares internacionales de borrado seguro, como puede ser: Infosec Security 5 Higher Standar, NIST 800-88[31] Clear o Purge, BSI-2011-VS.
d) Emitir un certificado del borrado seguro.
e) No debe existir un período de retención de los datos si no hubo un previo acuerdo con el responsable.
f) No deben existir respaldos adicionales derivado de redundancias del tipo de almacenamiento.

Para este punto, **deberá atender lo establecido en Acuerdo INE-CT-ACG-PDP-003-2018 para el bloqueo y supresión de los datos personales**, con base en el Artículo 12 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos personales.

2.10 ACTUALIZACIONES DE LA APLICACIÓN CLIENTE

El encargado, debe asegurarse que para las aplicaciones cliente se disponga de:

a) Actualizaciones automáticas del software.
b) Registro de eventos de instalación y desinstalación.
c) Compatibilidad operativa de las actualizaciones de las aplicaciones cliente.
d) Licenciamiento apropiado para las aplicaciones cliente.

[31] Para mayor información del estándar. Consultar https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

2.11 SEGURIDAD FÍSICA

Se recomienda que los responsables busquen encargados que se ajusten a las normas ISO/IEC 27002:2013, ISO/IEC 24762: 2008 (E)[32], TIA942[33] con referencia a:

a) Protección de la infraestructura física e instalaciones en áreas seguras.
b) Protección contra amenazas externas y ambientales.
c) Control del personal que labora en las instalaciones.
d) Controles de seguridad del equipo.
e) Controles para suministro de gas, agua, luz, etc.
f) Controles para la seguridad del cableado.
g) Mantenimiento adecuado del equipo.
h) Control de eliminación de activos.
i) Planes de respaldo redundancia y continuidad.

2.12 NIVELES DE SERVICIO (SLA)

Los acuerdos contractuales entre el encargado y el responsable deberán definir los servicios y componentes de seguridad, considerando, al menos, lo siguiente[34]:

a) **Protección contra desastres:** contar con protección contra desastres adecuada, por ejemplo, *backup y cloud bursting* (intercambio de los centros de datos internos cuando estos no pueden encargarse del procesamiento de las cargas).
b) **Redundancia:** contar con redundancia suficiente entre los sistemas del proveedor de servicios de nube.
c) **Mantenimiento:** la disponibilidad de los servicios cuando existan mantenimientos en la infraestructura de nube que permita acordar si, durante el mantenimiento, los servicios no estarán disponibles, es decir, se tendrá disponibilidad, pero se impactará su rendimiento y si se tendrá la oportunidad de comparar la operación y rendimiento de las aplicaciones con el servicio actualizado después de un mantenimiento.
d) **Ubicación de los datos:** el almacenamiento de distintos tipos de datos en ubicaciones físicas determinadas. Si el encargado puede responder a los requisitos con la garantía de que los datos del responsable serán almacenados solamente en las ubicaciones requeridas por este.

[32] Para mayor información del estándar. Consultar https://www.iso.org/obp/ui/#iso:std:iso-iec:24762:ed-1:v1:en
[33] Para mayor información del estándar. Consultar: https://www.tic.ir/Content/media/article/TIA%20942%20-A(2012)_0.PDF
[34] Para mayor información. Consultar: https://www.ibm.com/developerworks/ssa/cloud/library/cl-rev2sla.html

e) **Embargo de datos:** si por cumplimiento de alguna ley o mandato jurídico de las autoridades competentes en el espacio geográfico donde se encuentran los servidores del encargado, se realizan embargos para capturar los datos y las aplicaciones que pertenecen otro cliente del encargado, evaluar qué sucedería si esos equipos contienen datos del responsable.
f) **Error del proveedor:** contar con acuerdos en caso de fallas en el servicio para que se tengan planes de contingencia.
g) **Jurisdicción:** las leyes locales que apliquen al encargado y, de igual manera, las leyes locales que apliquen al proveedor.
h) **Terceros involucrados:** si el encargado subcontrata el servicio en la nube que presta al responsable, considerar que debe comprender las políticas de su proveedor.
i) **Disponibilidad del servicio:** definir el *uptime* del servicio.
j) **Cifrado de datos:** el cifrado de los datos en tránsito y reposo, acordando los algoritmos de cifrado.
k) **Eliminación de dispositivos:** la retirada y/o destrucción de los dispositivos por el encargado asegurando que ningún dato del responsable pueda ser recuperado de ellos.
l) **Auditoria:** la auditoria de los sistemas del encargado por parte del proveedor para revisar el cumplimiento de los acuerdos, dejando claro cómo y cuándo se ejecutarán dichas auditorias.
m) **Soporte de expertos:** disponibilidad de personal especializado del encargado para dar soporte al proveedor.
n) **Certificación:** las certificaciones requeridas al encargado y su responsabilidad por mantenerlas.
o) **Incidentes de seguridad:** la notificación al responsable por parte del encargado en caso de ocurrencia de algún incidente de seguridad que afecte los datos del responsable y los servicios que el encargado le provee.

ANEXO I. CHECKLIST CUMPLIMIENTO

No.	Acción	Cumple		Justificación
		Sí	No	
Contratación del servicio				
Características del encargado				
1	Políticas de protección de datos compatibles.			
2	Aviso de privacidad con información sobre la protección de datos personales			
Certificaciones				
3	ISO/IEC 27018			
	ISO/IEC 27001			
	SOC 1			
	SOC 2			
	SOC 3			
	PCI DSS			
Relación Jurídica Responsable-Encargado				
4	Procedimiento en caso de vulneración de los datos.			
5	Convenios de confidencialidad con las personas involucradas en el tratamiento de los datos.			
6	Servicio de nube privada.			
7	Existencia de un responsable para temas contractuales.			
Seguridad				

No.	Acción	Cumple		Justificación
		Sí	No	
8	Clasificación del nivel de seguridad con el que cuenta el servicio			
9	Medidas que se tienen para el control de acceso			
11	Cuenta con asignación de roles y responsabilidades			
12	Los accesos autorizados de los usuarios corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones			
13	Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados			
14	Existe una relación de usuarios, especifica qué datos y recursos tiene autorizados para cada uno de ellos y se encuentra actualizada			
15	Si existen procedimientos de identificación y autenticación para el proceso de acceso, ¿Garantiza la correcta identificación del usuario?			
16	¿El mecanismo de acceso y verificación de autorización de los usuarios identifica de forma inequívoca y personalizada?			
17	Si existe un procedimiento de asignación, distribución y almacenamiento de contraseñas, ¿Garantiza su confidencialidad e integridad?			
18	¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?			
19	¿Se limita el intento reiterado de acceso no autorizado al sistema?,			
20	¿Se anotan estos intentos en el registro de incidencias?			

ANEXO II. EMPRESAS DE CÓMPUTO EN LA NUBE

En el año de 2017, la revista Forbes nombró a las cien mejores empresas en el mundo que presta el servicio de cómputo en la nube, derivado de dicha lista a continuación se enuncian

las primeras diez empresas, asimismo se señalan los escudos de privacidad y las certificaciones con las que cuentan. [35]

Empresas Americanas de Computo en la Nube		
Cons.	**Empresa**	**Escudo de Privacidad**
1	Stripe	Unión Europea y Suiza
2	Dropbox	Unión Europea y Suiza
3	Slack	Unión Europea y Suiza
4	Qualtrics	Unión Europea y Suiza
5	Medallia	Unión Europea y Suiza
6	Tatium	No cuenta con escudo
7	Mailchimp	Unión Europea y Suiza
8	Squarespace	Unión Europea y Suiza
9	Cloudflare	Unión Europea y Suiza
10	SurveyMonkey	Unión Europea y Suiza

ANEXO III. SUPRESIÓN DE LOS DATOS PERSONALES

A continuación, se incluyen el procedimiento para la supresión de datos personales elaborado por la Unidad de Transparencia y aprobado por el Comité de Transparencia.

Documento	Archivo
Procedimientos y plazos de conservación para el bloqueo en su caso y supresión de los datos personales que obran en posesión del Instituto Nacional Electoral (Anexo Único del Acuerdo INE-CT-ACG-PDP-003-2018)	INE-CT-ACG-PDP-003 -2018-PROCEDIMIENT

[35] Forbes Cloud 100, revista Forbes, disponible en *www.forbes.com>cloud100>list,* (Fecha de consulta 18 de enero de 2018).

ANEXO IV. CATEGORIZACIÓN DE DATOS PERSONALES

Categorización de datos personales de acuerdo con su tipo		
Categoría	**Tipo de datos personales** *(con ejemplos)*	**Riesgo inherente**
Estándar	**Identificación y contacto, laborales y académicos**. Como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, domicilio, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.	**BAJO**
Sensible	**De Ubicación física de la persona,** la relativa al tránsito de las personas dentro y fuera del país (geolocalización) y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más (dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.).	**MEDIO**
	De patrimonio. Todos aquellos que permitan inferir el patrimonio de una persona, incluye entre otros, saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados, número de tarjeta bancaria de crédito y/o débito.	**MEDIO**
	De autenticación. Información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.	**MEDIO**

Categorización de datos personales de acuerdo con su tipo		
Categoría	**Tipo de datos personales** *(con ejemplos)*	**Riesgo inherente**
	Jurídicos, como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.	**MEDIO**
Sensible	Todos aquellos que afecten la esfera más íntima de su titular, es decir, los que puedan dar origen a discriminación o conlleven un riesgo grave a la integridad del titular, como revelar aspectos del origen racial o étnico, estado de salud, pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales, entre otros, según el caso en concreto.	**ALTO**
Especial	Son todos los datos que pueden causar daño directo a los titulares, debido a su naturaleza o bien, debido a un cambio excepcional en el contexto de las operaciones usuales, como: • información adicional de la tarjeta bancaria -número de tarjeta de crédito o débito más cualquier otro dato relacionado o contenido en la misma (fecha de vencimiento, código de seguridad, datos de la banda magnética, número de identificación personal PIN • Conjunto de varios tipos de datos personales en una base de datos.	**REFORZADO**

REFERENCIAS

Agencia Europea de Seguridad de las Redes y de la Información (ENISA) . (1 de Noviembre de 2009). *European Union Agency for Network and Information Security (ENISA.* Obtenido de Cómputo en la nube.: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

Association, T. I. (08 de 2012). *Telecommunications Infrastructure Standards for Data Centers*. Obtenido de TIA-942-A: https://www.tic.ir/Content/media/article/TIA%20942%20-A(2012)_0.PDF

Cella, J. (- de - de 2014). *ISACA*. Obtenido de Seguridad y Privacidad en la nube : http://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014-%20Seguridad%20y%20Privacidad%20en%20la%20Nube.pdf

Centro Criptológico Nacional. (- de Abril de 2017). *Centro Criptológico Nacional.* Obtenido de Criptología de empleo en el ENS: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

CN-CERT. (8 de Enero de 2010). *CN-CERT.* Obtenido de ENS - Esquema Nacional de Seguridad: https://www.ccn-cert.cni.es/publico/ens/ens/1093.htm#!-alone

Council, S. S. (- de - de 2019). *PCI Security Standards Council*. Obtenido de https://www.pcisecuritystandards.org/pci_security/

CPAs, A. I. (- de - de 2019). *AICPA*. Obtenido de https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html

División Consultoría de EvaluandoCloud.com. (17 de Mayo de 2016). *Evaluando Cloud.com*. Obtenido de Guardar datos en la nube, seguridad : http://evaluandocloud.com/guardar-datos-la-nube-aspectos-seguridad/

Electoral, I. N. (28 de 10 de 2013). *Reglamento para el uso y operación de la firma electrónica avanzada en el Instituto Federal Electoral*. Obtenido de https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/86280/CGex201310-28_ap_8_x1.pdf?sequence=2&isAllowed=y

Forbes. (18 de Enero de 2018). *Forbes*. Obtenido de Forbes Cloud 100: https://www.forbes.com/

GLORIA CARRALES, J. A. (8 de Noviembre de 2013). *Instituto Veracruzano de acceso a la información y protección de datos personales* . Obtenido de Datos personales: https://colaboracion.uv.mx/rept/files/pdp/Guia-Medidas-Seguridad.pdf

Gobernación, S. d. (23 de 01 de 2018). *Diario Oficial de la Federación*. Obtenido de http://www.dof.gob.mx/index.php?year=2018&month=01&day=23

IBM. (- de - de -). *IBM*. Obtenido de ¿Qué es una nube privada?: https://www.ibm.com/cloud-computing/mx-es/learn-more/what-is-private-cloud/

IBM, D. c. (03 de 02 de 2011). *Revisión y resumen de acuerdos del nivel de servicio en nube*. Obtenido de https://www.ibm.com/developerworks/ssa/cloud/library/cl-rev2sla.html

Incibe- Instituto NAcional de Ciberseguridad. (0 de Enero de 2011). *Incibe- Instituto NAcional de Ciberseguridad.* Obtenido de Seguridad y resistencia en las nubes de administración pública: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/es_governmental_clouds_enisa.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (4 de Junio de 2016). *INAI.* Obtenido de Guía para el Borrado Seguro de Datos Personales: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

Internet Society . (- de - de -). *Internet Society .* Obtenido de TLS Basic : https://www.internetsociety.org/deploy360/tls/basics/

J.Pomeyrol. (22 de Enero de 2014). *Muy seguridad.net.* Obtenido de Almacenamiento en la nube: ¿cifrado en cliente o cifrado en servidor?: https://www.muyseguridad.net/2014/01/22/nube-cifrado-cliente-servidor/

Ltd., C. (2016). *Transmission Confidentiality and Integrity (SC-8)*. Obtenido de https://cyuber.co.uk/security-controls/system-communications-protection-sc/transmission-confidentiality-integrity-sc-8/

Master Magazine. (- de - de 2018). *Sistemas* . Obtenido de Cliente / Servidor: https://sistemas.com/cliente-servidor.php

Osores, M. (10 de Enero de 2014). *TechTarget*. Obtenido de ¿Qué modelo de nube le conviene a mi empresa?: https://searchdatacenter.techtarget.com/es/noticias/2240211902/Que-modelo-de-nube-le-conviene-a-mi-empresa

Program, T. F. (2018). *FedRAMP*. Obtenido de https://www.fedramp.gov/

Publication, F. I. (12 de 03 de 2002). *Security Requirements for Cryptographic Modules*. Obtenido de https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Red Iris . (15 de 07 de 2002). *Res Iris .* Obtenido de Criptología : https://www.rediris.es/cert/doc/unixsec/node29.html

Sistemas . (- de - de -). Obtenido de Definición de Cliente / Servidor: https://sistemas.com/cliente-servidor.php

Standarization, I. O. (2008). *Guidelines for information and communications technology disaster recovery services*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:24762:ed-1:v1:en

Standarization, I. O. (08 de 2015). *Security techniques -- Network Security - Part 1: Overview and concepts*. Obtenido de https://www.iso.org/standard/63461.html

Standarization, I. O. (- de - de 2019). *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Obtenido de https://www.iso.org/standard/43757.html

Standarization, I. O. (01 de 2019). *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. Obtenido de https://www.iso.org/standard/76559.html

Standarization, I. O. (- de - de 2019). *Information Security Management Systems*. Obtenido de https://www.iso.org/isoiec-27001-information-security.html

Team, C. C.-N. (25 de 03 de 2019). *Defensa frente a las ciberamenazas*. Obtenido de https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/guias-de-acceso-publico-ccn-stic.html

Technology, N. I. (09 de 2006). *Guidelines for Media Sanitization*. Obtenido de https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

Technology, N. I. (- de 04 de 2013). *Security Controls and Assessment Procedures for Federal Informatión Systems and Organizations*. Obtenido de https://nvd.nist.gov/800-53/Rev4/control/SC-8

Technology, N. I. (04 de 2014). *Guidelines for the Selection, Congiguration, and Use of Transport Layer Security (TLS) Implementations*. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Technology, N. I. (10 de 10 de 2018). *Cryptographic Standards and Guidelines*. Obtenido de https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

Technology, N. I. (2019). *National Vulnerability Database*. Obtenido de SC-7 Boundary Protection: https://nvd.nist.gov/800-53/Rev4/control/SC-7