

DOCUMENTO DE SEGURIDAD

PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN POSESIÓN DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

A. Manifiesto de resguardo electrónico de bases de datos por la Dirección General de Tecnologías de la Información y Comunicaciones

1. Objetivo

Declarar el alcance de las actividades realizadas por la DGTIC respecto del resguardo electrónico de bases de datos alojadas en la infraestructura tecnológica administrada por la DGTIC, con independencia de que éstas incluyan datos personales.

2. Antecedentes

Con fundamento en las atribuciones establecidas en el Estatuto Orgánico del Instituto Federal de Telecomunicaciones, la DGTIC ha definido, implementado y mantenido diversos mecanismos para preservar la confidencialidad, integridad y disponibilidad de los activos de información. Para la implementación de dichos mecanismos, la DGTIC desarrolló y publicó las:

- Normas para la administración, operación y mantenimiento de soluciones de tecnologías de la información y comunicaciones del Instituto Federal de Telecomunicaciones (Normas TIC) publicadas en febrero de 2016 y actualizadas en junio de 2018, y
- Políticas para el uso de los recursos de tecnologías de la información y comunicaciones del Instituto Federal de Telecomunicaciones publicadas en noviembre de 2014 y actualizadas en octubre de 2015 y de 2017.

Además, en diciembre de 2017, la DGTIC logró las certificaciones ISO/IEC 27001:2013 y NMX-I-27001-NYCE-2015 en materia de seguridad de la información y relacionadas con los procesos de administración de la operación y administración de servicios.

3. Fundamento

- Normas para la administración, operación y mantenimiento de soluciones de tecnologías de la información y comunicaciones del Instituto Federal de Telecomunicaciones
http://www.ift.org.mx/sites/default/files/OPNT/LGTAIP/I/2018/I_18-UA-NormasTIC.pdf
- Políticas para el uso de los recursos de tecnologías de la información y comunicaciones del Instituto Federal de Telecomunicaciones
http://www.conexion.ift.org.mx/intranet/media/k2/attachments/Políticas_Uso_de_Recursos_de_TIC_Accesible_2.pdf
- Sistema de Gestión de Seguridad de la Información (SGSI). Se encuentra clasificado como reservado.

4. Manifiesto

La DGTIC no recaba ni trata datos personales. El alcance de las actividades de la DGTIC respecto de las bases de datos electrónicas que contienen información recabada y tratada por las diversas Unidades Administrativas del Instituto y que se almacenan en infraestructura tecnológica que administra la DGTIC, se limitan a su resguardo mediante mecanismos seguros que permiten mantener la confidencialidad, integridad y disponibilidad de la información.

Con el objetivo de implementar las mejores prácticas en términos de seguridad de la información, la DGTIC aplica las normas y políticas correspondientes y ejecuta los procedimientos de resguardo de información, sin distinción del contenido o ausencia de datos personales.

A la fecha, la DGTIC tiene conocimiento de 6 sistemas de información en los que se almacenan datos personales y que son resguardados en la infraestructura tecnológica administrada por la DGTIC. Dichos sistemas son: Protalento IFT (Khor), Nómina, Soy Usuario, Sistema de Administración Presupuestal y Financiera, Viáticos y Sistemas de Ingresos del IFT. Cabe aclarar que, sin detrimento de lo anterior, la DGTIC no tiene conocimiento de que las Unidades Administrativas almacenen datos personales en otros sistemas.

5. Personal que tiene entre sus funciones la administración de las bases de datos del Instituto

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	
Finalidad del acceso	Coordinar la administración y mantenimiento de las bases de datos para optimizar los recursos tecnológicos en los que operan, así como ejecutar los respaldos y la recuperación de éstos.
Cargo	
Área de adscripción	
Teléfono y extensión	

Correo institucional	
----------------------	--

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	
Finalidad del acceso	Administración y mantenimiento de las bases de datos para optimizar los recursos tecnológicos en los que operan, así como ejecutar los respaldos y la recuperación de éstos.
Cargo	
Área de adscripción	
Teléfono y extensión	
Correo institucional	

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	
Finalidad del acceso	Apoyo en la administración y mantenimiento de las bases de datos para optimizar los recursos tecnológicos en los que operan, así como ejecutar los respaldos y la recuperación de éstos.
Cargo	
Área de adscripción	
Teléfono y extensión	
Correo institucional	
Empresa	
Contrato	
Proyecto o Servicio	

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	[REDACTED]
Finalidad del acceso	Apoyo en la administración y mantenimiento de las bases de datos para optimizar los recursos tecnológicos en los que operan, así como ejecutar los respaldos y la recuperación de éstos.
Cargo	[REDACTED]
Área de adscripción	[REDACTED] [REDACTED]
Teléfono y extensión	[REDACTED]
Correo institucional	[REDACTED]
Empresa	[REDACTED]
Contrato	[REDACTED]
Proyecto o Servicio	[REDACTED]

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	[REDACTED]
Finalidad del acceso	Apoyo en la administración y mantenimiento de las bases de datos para optimizar los recursos tecnológicos en los que operan, así como ejecutar los respaldos y la recuperación de éstos.
Cargo	[REDACTED]
Área de adscripción	[REDACTED] [REDACTED]
Teléfono y extensión	[REDACTED]
Correo institucional	[REDACTED]
Empresa	[REDACTED]

Contrato	
Proyecto o Servicio	

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	
Finalidad del acceso	Coordinar la gestión de los portales y sistemas institucionales con la finalidad de garantizar su funcionamiento, disponibilidad, desempeño y resiliencia tecnológica, conforme a las mejores prácticas internacionales de TIC y de acuerdo a lo establecido en la normatividad vigente.
Cargo	
Área de adscripción	
Teléfono y extensión	
Correo institucional	

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	
Finalidad del acceso	Apoyar en la gestión de los portales y sistemas institucionales con la finalidad de garantizar su funcionamiento, disponibilidad, desempeño y resiliencia tecnológica, conforme a las mejores prácticas internacionales de TIC y de acuerdo a lo establecido en la normatividad vigente.
Cargo	
Área de adscripción	
Teléfono y extensión	

Correo institucional	
----------------------	--

Lista de Servidores públicos o personal externo con acceso a los sistemas de tratamiento	
Nombre	
Finalidad del acceso	Apoyo en la operación de la infraestructura institucional que soporta los portales y sistemas institucionales con la finalidad de garantizar su funcionamiento, disponibilidad, desempeño y resiliencia tecnológica, bajo la operación de herramientas de monitoreo conforme a buenas prácticas de gestión de servicios de TI y de acuerdo con la normatividad vigente.
Cargo	
Área de adscripción	
Teléfono y extensión	
Correo institucional	
Empresa	
Contrato	
Proyecto o Servicio	

6. Marco normativo

- *Estatuto Orgánico*

Artículo 61. La Dirección General de Tecnologías de la Información y Comunicaciones tendrá a su cargo el diseño, operación y **administración de la infraestructura** y de los sistemas y servicios informáticos que requieran las áreas del Instituto para el cumplimiento de sus atribuciones; el desarrollo, operación y **administración de** los programas de cómputo, **equipos de procesamiento de datos**, redes de telecomunicaciones de voz y datos, y **bases de datos**

del Instituto, así como la coordinación del soporte técnico que se proporcione a los usuarios de los mismos, además de la administración del portal de Internet del Instituto. Corresponde a esta Dirección General el ejercicio de las atribuciones siguientes:

...

- III. Desarrollar, operar y **administrar** los sistemas de informática, programas de cómputo, equipos de procesamiento de datos, redes de telecomunicaciones de voz y datos, y **bases de datos del Instituto**, así como coordinar el soporte técnico que se proporcione a los usuarios de los mismos;

...

- VIII. Definir e implementar la estrategia para garantizar el debido resguardo, confidencialidad y seguridad de la información y las comunicaciones, redes, plataformas digitales y archivos del Instituto;

- *Normas para la administración, operación y mantenimiento de soluciones de tecnologías de la información y comunicaciones del Instituto Federal de Telecomunicaciones (Normas TIC)*

Título sexto *Normas específicas y documentos asociados a las soluciones tecnológicas*

Capítulo I *Normas específicas aplicables a las soluciones tecnológicas*

Artículo 48 Son de aplicación obligatoria a las soluciones tecnológicas las siguientes normas específicas:

...

II Clasificación de la Información. *La UA solicitante deberá identificar y comunicar al proveedor que le atenderá, el tipo de información que se gestionará a través de la solución tecnológica, clasificándola de conformidad a la normativa en las materias de transparencia, acceso a la información pública y protección de datos personales.*

En caso de que el sistema maneje datos personales, es de suma importancia que le sea comunicado a la DGTIC, con la finalidad de prever las acciones necesarias para asegurar la información y cumplir con la normatividad aplicable.

...

VII Arquitectura de la solución tecnológica. Se deberá considerar como parte de la arquitectura de la solución tecnológica, la conceptualización de al menos una capa de presentación (servidores de presentación), una capa de negocio (servidor de aplicaciones web, servidores de contenido

o servidor de reglas de negocio) y una capa de datos (almacenamiento en base de datos), tal y como se ilustra en el diagrama anexo. <Diagrama>. La distribución de los componentes a nivel red, así como el número de servidores que formarán parte de la **arquitectura tecnológica** deberá acordarse entre el administrador del proyecto, el líder técnico y la DGTIC.

...

IX Ambientes independientes: desarrollo, pruebas y producción. **Deberán existir ambientes independientes de producción, pruebas y desarrollo de software**, de tal forma que no compartan recursos tecnológicos entre sí. Las versiones de sistema operativo, base de datos y servidores de aplicación deberán ser idénticos en todos los ambientes que formen parte de la solución tecnológica.

...

Los ambientes de pruebas y producción deberán ser instalados y configurados en los Centros de Datos del IFT, **siendo la DGTIC la responsable de proveer los servidores y sistema operativo acordes a la arquitectura definida**.

...

XIII Cifrado y comunicación segura. **El intercambio de información sensible** (cuentas de usuario, contraseñas, **datos personales**, información confidencial, información reservada, etc.) entre la solución tecnológica y los usuarios, **deberá realizarse a través de medios seguros** utilizando mecanismos de cifrado basados en los protocolos SSL/TLS de al menos 128 bits, con algoritmo de firma SHA-256 y longitud de llaves de 2048 bits. Los certificados deberán ser expedidos por una autoridad certificadora de confianza y tener una vigencia no mayor a 825 días naturales.

...

XXIII Administración de usuarios. La solución tecnológica deberá contener un módulo de **administración de usuarios** (alta, baja, cambios) **que permita validar la identidad de los usuarios a través de un mecanismo de autenticación basado en contraseñas**.

...

El módulo de administración de usuarios deberá configurarse de manera que permita cumplir con los siguientes requisitos para la administración de contraseñas:

- **Reglas configurables para asignar la complejidad de las contraseñas** (longitud mínima de caracteres, uso de mayúsculas, minúsculas, números y símbolos).
- **Cambio periódico de contraseñas.**
- **Bloqueo automático del acceso a la cuenta** de usuario después de un número determinado de intentos fallidos.
- **Reinicio de contraseñas** por parte del administrador del sistema a solicitud de un usuario.
- **Almacenamiento seguro de contraseñas a través de los algoritmos de cifrado SHA2 o AES 128 o 256 bits.**

XXIV Autenticación de usuarios. Para aplicaciones donde su acceso está limitado a los usuarios conectados a las redes internas del Instituto, se deberá utilizar el Directorio Activo Institucional, como medio de autenticación a las mismas.

Para el caso de aplicaciones que se encuentren publicadas en Internet, **se deberán utilizar mecanismos de autenticación basados en usuario y contraseña**, considerando lo establecido en los requisitos para la administración de contraseñas citadas en la norma anterior.

Adicionalmente, con la finalidad de proteger de abusos a las aplicaciones, se deberán implementar mecanismos tipo CAPTCHA de nueva generación que **minimicen los riesgos** de ataque de diccionario por sistemas automatizados o robots.

XXV. Matriz de roles y privilegios. El módulo de **administración de usuarios** de la solución tecnológica deberá contar con un mecanismo de autorización basado en roles o perfiles, que permita al sistema verificar qué roles tienen permisos sobre qué recursos; qué opciones de menú configurar; o **qué información mostrar en tiempo de ejecución.**

...

XXVII **Manejo de datos personales.** En caso de que la solución tecnológica recolecte o gestione información clasificada como datos personales, **la UA deberá definir el aviso de privacidad relativo**, de acuerdo con la normativa en las materias de transparencia, acceso a la información pública y protección de datos personales, y deberá asegurarse que el

proveedor o líder técnico del IFT lo integre a la interfaz gráfica de la solución tecnológica.

XXIX Manejo de sesiones. La solución tecnológica deberá ser capaz de **limitar a una, el número de sesiones** concurrentes de un mismo usuario.

...

XXX **Validación de datos de entrada.** La validación de los datos de entrada deberá realizarse y parametrizarse en los diferentes módulos que conformen la solución tecnológica, de tal forma que se **mitiguen ataques tales como: inyección de código** (SQL, LDAP o XPath), así como ataques de sitios cruzados (XSS).

Ataque por sistemas automatizados o robots. Con la finalidad de **evitar la inserción de datos** inválidos provenientes de sistemas automatizados o robots, cualquier formulario expuesto a Internet deberá contener una prueba de validación Captcha.

...

XLIII Ambiente de pruebas. El proveedor deberá realizar una primera implementación de la solución tecnológica en el ambiente de pruebas, de tal forma que se valide el manual de instalación y configuración. Siendo este el ambiente en el que **se deberán ejecutar todas las pruebas** de la UA solicitante, el área de calidad y aquellas **de seguridad necesarias** acorde a la naturaleza de la solución tecnológica.

...

XLV **Pruebas funcionales de seguridad.** La DGTIC será la responsable de **realizar pruebas funcionales de seguridad** sobre la solución tecnológica desarrollada, con la finalidad de verificar la **correcta implementación de las recomendaciones de seguridad** establecidas y acordadas por la DSI y el proveedor de la solución. Será responsabilidad de la DGTIC reportar los hallazgos encontrados, anexando la evidencia del incumplimiento detectado.

...

XLVIII **Análisis de vulnerabilidades.** Antes de que la solución tecnológica sea implementada en un ambiente productivo, se deberá **realizar un análisis que permita identificar las vulnerabilidades de la solución** y el nivel de riesgo que estas representan para los activos de información del IFT.

Será responsabilidad de la DGTIC la ejecución del análisis de vulnerabilidades sobre la aplicación e infraestructura, asimismo clasificarlas de acuerdo a su posibilidad de explotación e impacto a los activos de información del IFT; estas pueden ser: Críticas, Altas, Medias, Bajas o Informativas.

...

LVI Política de respaldos. Con la finalidad de garantizar la disponibilidad de la información y la continuidad de la operación de la solución tecnológica, la UA solicitante y el líder técnico del IFT deberán acordar obligatoriamente los respaldos necesarios, así como los periodos de retención de los mismos.

A su vez, el proveedor o líder técnico del IFT solicitará a la DIT, a través del documento de Políticas de respaldo correspondiente, los componentes (instancias de bases de datos, archivos ejecutables, carpetas de sistemas operativos, rutas o directorios etcétera) de la solución tecnológica que deberán respaldarse de forma periódica con la finalidad de:

- Permitir la restauración de información a un punto anterior.
- Garantizar su recuperación y/o replicación en un nuevo ambiente completamente independiente.

LVII Documento de Mantenimiento de la Base de Datos. Consiste en el conjunto de actividades de mantenimiento y optimización recomendadas para su aplicación en la Base de Datos, con el propósito de mejorar el rendimiento y garantizar la integridad y resguardo de los datos que, entre otros, incluye:

- Optimización / reconstrucción de índices
- Revisión de integridad de la Base de Datos
- Respaldos
- Generación de estadísticas
- Organización de datos históricos
- Especificación de Jobs de la Base de Datos

El proveedor deberá documentar el mantenimiento a la Base de Datos alineado a los "Estándares de Base de Datos" definidos por el Instituto.

- *Políticas para el uso de los recursos de tecnologías de la información y comunicaciones del Instituto Federal de Telecomunicaciones*

Artículo 15. El Instituto podrá proporcionar a las Unidades Administrativas, previa solicitud, un servicio de Sitios Colaborativos con el fin de apoyar al ejercicio de sus funciones, el cual está

soportado en la plataforma Microsoft SharePoint. Es responsabilidad de todo Usuario considerar las siguientes directrices con respecto a dicho servicio:

...

- III. A cada Sitio Colaborativo deberá asignarse **un administrador** por Sitio o Sub-sitio (dependiendo de la estructura del mismo), quien **será responsable de realizar las altas, bajas o cambios de accesos, permisos o bien de solicitar cambios** a la estructura del Sitio. Dicho administrador deberá indicarse en el formato a través del cual se solicita el servicio (FODGTIC-13);
- IV. **Los Usuarios que requieran de acceso** a Sitios Colaborativos ya existentes, **deberán solicitarlo al administrador del Sitio**, quien validará las solicitudes así como los privilegios asignados;
- V. **Los Usuarios** que tienen acceso a los Sitios Colaborativos **son responsables de la Información** contenida en estos, así como de las acciones que ejecuten acorde a los privilegios que tienen asignados

...

Artículo 16.- El Instituto podrá proporcionar a las Unidades Administrativas, previa solicitud, un servicio de Carpetas Compartidas con el fin de apoyar al ejercicio de sus funciones. Es responsabilidad de todo Usuario considerar las siguientes directrices con respecto a dicho servicio:

...

- III. Por cada Carpeta Compartida **deberá asignarse un responsable de las solicitudes de altas, bajas o cambios de accesos o bien de los permisos de la Carpeta**. Dicho responsable deberá indicarse en su solicitud vía Portal de Autoservicio o mediante el formato a través del cual se solicita el servicio (FO-DGTIC-01) y deberá tener por lo menos un nivel de Subdirector de área;
- IV. **Los Usuarios que requieran de acceso** a Carpetas Compartidas ya existentes, **deberán solicitarlo a través del responsable** de la misma;
- V. **Los Usuarios** que tienen acceso a Carpetas Compartidas **son responsables de la Información** contenida en éstas, así como de las acciones que ejecuten acorde a los privilegios que tienen asignados;
- VI. El responsable de la Carpeta Compartida, deberá validar las solicitudes de altas o bajas de accesos, así como los privilegios asignados y canalizarlas a la DGTIC para su aplicación;
- ...
- IX. **El responsable** de la Carpeta Compartida, deberá evaluar periódicamente, **en conjunto con los dueños de la Información**, la pertinencia de **mantener la Información** dentro de la misma, con el fin de optimizar los recursos e infraestructura tecnológica

del Instituto, asegurando que la Información contenida en ésta, es con el fin de almacenamiento y no para colaboración grupal.

Artículo 22. Todo Usuario será provisto de las cuentas de acceso y contraseñas necesarias para el uso de los sistemas de Información y recursos relacionados con las Tecnologías de la Información y Comunicaciones del IFT, de acuerdo con sus funciones de su puesto, para lo cual, deberá observar lo siguiente:

...

- I. Las cuentas de acceso son personales e intransferibles y es responsabilidad del Usuario garantizar que es el único que conoce las contraseñas de acceso, por lo que toda actividad registrada con dichas cuentas, es responsabilidad del Usuario al que pertenecen;
- II. Las contraseñas provistas por la DGTIC para el acceso a los sistemas y recursos de Información, son de carácter temporal, por lo que el Usuario deberá cambiarlas en su primer inicio de sesión;
- III. Con el fin de crear contraseñas seguras, el Usuario deberá apegarse a los criterios de seguridad siguientes:

...