cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

Implementado por:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Guía para la protección y uso ético de la información en poder de las administraciones tributarias.

Administraciones Tributarias de Centro América, Panamá y República Dominicana

En coordinación con:

COSEFIN
Consejo de Ministros de Hacienda o Finanzas de Centroamérica, Panamá y República Dominicana

SICA
Sistema de la Integración Centroamericana

CIAT
CENTRO INTERAMERICANO DE ADMINISTRACIONES TRIBUTARIAS
FUNDADO 1967

Guía para la protección y uso ético de la información en poder de las administraciones tributarias

cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

Implementado por:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

En coordinación con:
COSEFIN
Consejo de Ministros de Hacienda o Finanzas de Centroamérica, Panamá y República Dominicana
SICA
Sistema de la Integración Centroamericana

Guía para la protección y uso ético de la información en poder de las administraciones tributarias. Administraciones Tributarias de Centro América, Panamá y República Dominicana
ISBN: 978-9962-72-64-9

Publicado por:

Centro Interamericano de Administraciones Tributarias – (CIAT)
Avenida Ramón Arias, Ciudad de Panamá, Panamá.
Tel. (+507) 307 CIAT (2428)
www.ciat.org

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Domicilios de la empresa

"Programa Buena Gobernanza Financiera" Agencia de la GIZ Bulevar Orden de Malta,
Casa de la Cooperación Alemana, Urbanización Santa Elena
Antiguo Cuscatlán, La Libertad El Salvador, Centroamérica.
Tel. +503 2121 5100
Giz-el-salvador@giz.de
Zentralamerika - giz.de

Versión

Diciembre (2024)

Por encargo del:

Ministerio Federal de Cooperación Económica y Desarrollo (BMZ) de Alemania

Autores

Alfredo F. Revilak De la Vega
Ana Y. Rodríguez Calderón
A. Gabriela Contreras Delgado
Evelyn Molina Bolaños

Revisión por:

GIZ

Gustavo Ernesto Sánchez Buriticá
Orlando Castellón Tellería
Manfredo Octavio Chocano Alvarado

CIAT

Raul Zambrano
Mónica Alonso
Elizabeth Rodríguez

Contenido

Autores[1]

Alfredo F. Revilak De la Vega, es consultor independiente con más de 30 años de experiencia en los sectores comercial y público, incluyendo cargos en Citibank, BBVA y la Secretaría de Hacienda y Crédito Público de México, específicamente en la Unidad de Inteligencia Financiera y el Servicio de Administración Tributaria. Su experiencia incluye 10 años como evaluador especialista y consultor en protección de información y salvaguarda de datos (OCDE y Banco Mundial) en Administraciones Tributarias, participando en las evaluaciones y apoyo técnico de: Panamá, Costa Rica, Belice, San Cristóbal y Nieves, Trinidad y Tobago, México, Chile, Argentina, Perú, Ecuador, Colombia, Uruguay y Paraguay. Actualmente desempeña la mayor parte de su tiempo como Consultor Senior en Impuestos Internacionales de la Unidad de Política Fiscal y Crecimiento Sostenible de la Práctica Global de Macroeconomía, Comercio e Inversión del Banco Mundial.

Ana Y. Rodríguez Calderón, cuenta con más de 15 años de experiencia en tributación internacional, y ha dedicado su carrera a temas de fiscalidad internacional, cooperación y desarrollo. Trabajó durante 4 años en el Ministerio de Hacienda de Costa Rica, donde desempeñó una serie de puestos, incluyendo la jefatura del Despacho del Ministro, Directora de Asuntos Internacionales y Asesora del Ministro en temas de tributación internacional. Ana laboró más de 7 años en la OCDE como analista de política y posteriormente como asesora coordinando el Programa de Relaciones Globales sobre Fiscalidad (GRP). En la actualidad, Ana es consultora internacional y trabaja principalmente como Consultora Senior en Tributación Internacional para el Banco Mundial y el Banco Asiático de Desarrollo. También ha proporcionado sus servicios al BID, CIAT, IBFD y Naciones Unidas.

A. Gabriela Contreras Delgado, es abogada con especialidad en derecho fiscal. Colaboró en el Servicio de Administración Tributaria de México por 15 años donde participó en la implementación normativa de los acuerdos de intercambio automático de información financiera. Ha sido representante de la delegación mexicana ante la OCDE, el Foro Global y el IRS y fungió como autoridad competente en la negociación y atención de diversos procedimientos amistosos con autoridades competentes de otras jurisdicciones. Actualmente es consultora independiente y ha prestado sus servicios en el sector privado, así como a diversas autoridades fiscales, el Banco Mundial y el CIAT, entre otros.

[1] Los autores quisieran expresar su más sincero agradecimiento a los funcionarios de las administraciones tributarias de Costa Rica, El Salvador, Guatemala, Honduras, República Dominicana y Panamá por su valiosa colaboración en el desarrollo de esta guía.

Evelyn Molina Bolaños, es economista y científica de datos y cuenta con más de 10 años de experiencia en programas regionales de desarrollo digital. Trabajó durante 3 años en el Ministerio de Hacienda de Costa Rica, donde se desempeñó como asesora económica para el ministro. En 2015 Evelyn se incorporó a la División de Innovación al Servicio del Ciudadano del Banco Interamericano de Desarrollo (BID) en Washington DC, en donde lideró y apoyó en programas regionales de gobernanza de datos. En la actualidad Evelyn es consultora independiente y ha proporcionado sus servicios a diferentes agencias de desarrollo, incluido el CIAT y el BID.

1. Introducción

En el marco del acuerdo de cooperación entre el Centro Interamericano de Administraciones Tributarias (CIAT) y la Cooperación alemana para el desarrollo, GIZ, para el fortalecimiento de las capacidades de las Administraciones Tributarias de Centroamérica, Panamá y la República Dominicana, se ha encomendado al CIAT la elaboración de una Guía para la protección de la información en poder de las administraciones tributarias que proporcione recomendaciones sobre cómo abordar una estrategia encaminada a una adecuada protección de datos.

La protección de datos personales juega un papel crucial en las administraciones tributarias al resguardar la integridad y confidencialidad de datos tributarios. La información fiscal, por su naturaleza requiere salvaguardas robustas para evitar accesos no autorizados, alteraciones o divulgaciones indebidas que podrían comprometer la privacidad de los contribuyentes. Además, la confianza del público y la credibilidad de la administración tributaria dependen en gran medida de la seguridad de la información gestionada. La implementación efectiva de medidas de protección no solo resguarda la información tributaria contra amenazas internas y externas, sino que también contribuye a la legitimidad y transparencia de las operaciones tributarias, fortaleciendo así la relación entre la administración tributaria y los contribuyentes.

De esta forma, el principal objetivo de esta guía es brindar a las administraciones tributarias recomendaciones sobre cómo abordar una estrategia encaminada a una adecuada protección de datos, que incluya aspectos procedimentales y los relacionados con la seguridad de la información. Específicamente en los temas de (i) Marco jurídico, (ii) gestión de la protección de la información, (iii) gestión de seguridad de las tecnologías de información, (iv) monitoreo y prevención, (v) generación de datos abiertos en las administraciones tributarias, (vi) gobernanza de datos en las administraciones tributarias y (vii) uso de la nube.

2. Metodología para la elaboración de la guía

Esta guía se desarrolló a partir de un enfoque integral que combinó la revisión de literatura, así como la colaboración de expertos(as) en la materia. A continuación, se detallan los pasos clave de la metodología empleada:

1. **Investigación y revisión documental**: se identificaron las mejores prácticas internacionales y casos de estudio pertinentes a las administraciones tributarias en los temas de protección de datos. Este proceso incluyó una revisión de la legislación existente en el ámbito tributario, así como de manuales, guías normativas y publicaciones de organismos internacionales expertos en la materia.

2. **Recopilación de datos y análisis comparativo**: Se recopilaron y analizaron datos sobre los procedimientos y políticas de protección de datos en las administraciones tributarias de Costa Rica, El Salvador, Guatemala, Honduras, República Dominicana y Panamá. Este análisis comparativo permitió identificar recomendaciones útiles que se adaptarán a los contextos específicos de los países involucrados.

3. **Consultas y entrevistas con expertos:** se consultaron expertos en tecnología, gestión de seguridad de la información, abogados entre otros de las administraciones tributarias de Costa Rica, El Salvador, Guatemala, Honduras, República Dominicana y Panamá. Las entrevistas y consultas proporcionaron perspectivas valiosas sobre las prácticas locales y las necesidades específicas de cada país.

4. **Identificación de casos prácticos:** A partir de la retroalimentación recibida, se incluyeron ejemplos prácticos y casos de estudios relevantes para brindar mayor claridad sobre buenas prácticas.

5. **Revisión y validación:** una vez completado el borrador de la guía, se realizó una revisión con el CIAT y las contrapartes de los países para asegurar la precisión y la coherencia del contenido.

3. Marco jurídico

3.1. Introducción

Los derechos de los contribuyentes son fundamentales en cualquier sociedad democrática y justa. Estos derechos garantizan que los ciudadanos que cumplen con sus obligaciones fiscales sean tratados con equidad y transparencia por parte de las autoridades tributarias. La importancia de estos derechos radica en la preservación de la confianza en el sistema tributario que en consecuencia promueve la participación de los ciudadanos en el financiamiento del Estado.

Así, la transparencia y el acceso a la información constituyen pilares fundamentales de una administración tributaria efectiva y ética. El uso adecuado de la información en poder de las administraciones tributarias facilita la rendición de cuentas, permite combatir la evasión fiscal y promueve una distribución equitativa de la carga impositiva. No obstante, este acceso debe ser regulado para salvaguardar la privacidad y los derechos de los contribuyentes, manteniendo así un balance entre el acceso a la información y la protección de la privacidad y confidencialidad de los datos. Es por ello que el resguardo de la confidencialidad de la información es el tercer principio fundamental de la gestión tributaria que resulta esencial para promover la confianza en el sistema fiscal.

En este contexto, el presente capítulo abordará aspectos relevantes relacionados con los derechos y garantías de los contribuyentes, en cuanto a la información que sobre ellos tiene la administración tributaria, destacando la necesidad de un marco legal que asegure un trato justo y equitativo. Se examinarán las características de las disposiciones legales enfocadas en garantizar la transparencia en la administración fiscal al tiempo que se salvaguardan los derechos individuales y se protege la información sensible. Asimismo, se analizará el marco jurídico necesario para asegurar un equilibrio entre estos elementos tanto a nivel nacional como internacional.

Adicionalmente, se explorarán los mecanismos diseñados para salvaguardar la confidencialidad de los datos e información fiscal, reconociendo la importancia de resguardar la privacidad de los contribuyentes. Finalmente, se estudiarán las principales características del marco normativo sancionador a través del cual las autoridades buscan prevenir, disminuir y disuadir la recurrencia de infracciones relacionadas con cuestiones de confidencialidad y seguridad de la información, uso y divulgación inadecuada de la información y faltas en materia de transparencia.

Para enriquecer este análisis, se incluyen referencias a los marcos normativos de Costa Rica, Guatemala, Honduras, El Salvador, Panamá, República Dominicana, y otras jurisdicciones con el objeto de identificar las diferentes estrategias y enfoques adoptados a nivel global y destacar las medidas y mejores prácticas que favorezcan la protección de datos sin menoscabar la transparencia fiscal, contribuyendo así a fortalecer los sistemas fiscales de manera global.

3.2. Derechos y garantías del contribuyente

Derechos y garantías fundamentales

La Organización de las Naciones Unidas (ONU) define a los **derechos humanos** como aquellos "inherentes a todos los seres humanos, independientemente de su raza, sexo, nacionalidad, etnia, idioma, religión o cualquier otra condición (…) sin discriminación"[2]. Estos derechos incluyen, entre otros, el derecho a la vida, la libertad, al trabajo, a la educación y la libertad de expresión. Se trata de derechos que se califican como universales ya que se refieren a cualquier individuo, son independientes, interrelacionados e indivisibles. Ante ellos, los gobiernos están obligados a actuar de determinada manera o de abstenerse de realizar ciertos actos, con el fin de garantizar su protección y preservación.

Adicionalmente, los **derechos fundamentales** son "aquellos que se encuentran positivados en el sistema jurídico, de tal forma que su fundamento es la norma jurídica, por lo que su fuente es la voluntad de la autoridad competente para crear dichas normas. Producen efectos jurídicos, ya sean derechos u obligaciones e incluso derechos de acción, y tienen todas las consecuencias jurídicas que el sistema jurídico les atribuya. Existen a partir de su otorgamiento por el sistema jurídico, y son asegurados por los medios de control de su ejercicio que el mismo establece como garantía frente a los abusos por parte de la autoridad. Sus límites se encuentran en el propio derecho. (…) Corresponde al derecho constitucional regular la protección de los derechos fundamentales y prever mecanismos especiales de protección."[3]

En general, tanto los derechos humanos como los derechos fundamentales tienen atributos esenciales que los caracterizan; estos son:

---

[2] Organización de las Naciones Unidas. *Derechos Humanos.* https://www.un.org/en/global-issues/human-rights

[3] Huerta, Carla, *Sobre la distinción entre derechos fundamentales.* Corte Interamericana de Derechos Humanos. Artículo disponible en: https://www.corteidh.or.cr/tablas/r28772.pdf

a) **Universalidad:** Se refiere al alcance de la protección que el derecho provee, idealmente se pretende cubrir, si no a la totalidad, a la mayor cantidad de titulares de los derechos y de las condiciones protegidas por éstos.

b) **Interdependencia e Indivisibilidad:** Son interdependientes en tanto establecen vinculación entre ellos y son indivisibles en tanto deben ser observados como un conjunto, la privación de un derecho afecta negativamente al resto de ellos. No pueden tutelarse o salvaguardarse en forma aislada sino como un solo cuerpo jurídico.

c) **Progresividad:** Son progresivos porque concretan las necesidades de la persona en cada momento histórico determinado; no son derechos estáticos, sino que han aumentado gradualmente según el avance o progreso social.

A partir de lo anterior, puede concluirse que los derechos fundamentales se encuentran consignados en una norma o cuerpo legal, lo cual los dota de efectos jurídicos (derechos u obligaciones) y el Estado tiene la obligación de salvaguardarlos haciendo uso de los medios de control con los que cuenta, dentro del ámbito de sus facultades. Los derechos y garantías de los contribuyentes pueden incluirse en esta categoría ya que son derechos que se encuentran consignados en cuerpos normativos respecto de los cuales el Estado tiene la obligación de preservar.

Antecedentes de los derechos de los contribuyentes

Ahora bien, en el contexto fiscal, el primer antecedente formal a nivel internacional donde se tutelaron los derechos fundamentales fue la **Declaración de los Derechos del Hombre y del Ciudadano**[4] que estableció la obligatoriedad de las contribuciones para solventar los gastos del gobierno atendiendo a los *principios de generalidad* y *proporcionalidad*.

Posteriormente, la **Declaración de los Derechos Humanos**[5] también consignó derechos que, aun cuando no son exclusivos de los contribuyentes, constituyen un antecedente de los derechos que actualmente se reconocen en el contexto tributario. Entre los principales derechos ahí consagrados sobresalen: el derecho a la seguridad, a la igualdad ante la ley, a la tutela jurisdiccional, el derecho de audiencia y el derecho y tutela de la propiedad individual y colectiva.

[4] Aprobada por la Asamblea Nacional Constituyente francesa el 26 de agosto de 1789. Documento disponible en https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/espagnol/es_ddhc.pdf

[5] Proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en la resolución 217-A. Información disponible en https://www.un.org/es/about-us/universal-declaration-of-human-rights

Asimismo, la **Convención Americana sobre Derechos Humanos** (conocida coloquialmente como el Pacto de San José[6]) también recogió diversos derechos fundamentales de los instrumentos señalados anteriormente, pero resalta el derecho al debido proceso al interponer recursos ante tribunales independientes e imparciales que les permitan el acceso al amparo contra actos que pudieran violar sus derechos fundamentales. Estos derechos, son los que actualmente se identifican como garantías judiciales que tienen efecto en materia penal, civil, laboral e incluso fiscal con lo que se entiende que la tutela jurisdiccional es extensiva a las obligaciones de carácter tributario.

Derechos y garantías fundamentales de los contribuyentes

En 1990 la OCDE, a través del Comité de Asuntos Fiscales publicó una encuesta[7] que analizaba el estado legal de los derechos y obligaciones de los contribuyentes entre sus países miembros. Dicha encuesta constituye uno de los primeros análisis comparativos en materia de derechos y garantías fundamentales de los ciudadanos en el ámbito fiscal.

Con base en la información recibida en dicha encuesta, la OCDE identificó los derechos, garantías y obligaciones que se presentaban de manera más recurrente en las legislaciones de los países evaluados. Tales resultados se resumen a continuación:

Derechos y garantías de los contribuyentes	Obligaciones de los contribuyentes
Derecho a ser informado, asistido y escuchado.	Obligación de ser honesto al cumplir con las obligaciones fiscales.
Derecho de Apelación	Obligación de cooperar con las autoridades fiscales.
Derecho a no pagar más que la cantidad correcta de impuestos.	
Derecho a la certeza jurídica.	Obligación de proporcionar información y documentos de manera puntual y adecuada.
Derecho a la privacidad.	Obligación de mantener registros, contabilidad y archivos
Derecho a la confidencialidad y secrecía.	Obligación de pagar impuestos en tiempo y forma.

Fuente: Derechos, garantías y obligaciones de los contribuyentes – Encuesta OCDE 1990

[6] Suscrita el 22 de noviembre de 1969. Documento completo disponible en https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

[7] OECD, *Taxpayer's Rights and Obligations – Practice Note.* Documento completo disponible en: https://www.oecd.org/tax/administration/Taxpayers'_Rights_and_Obligations-Practice_Note.pdf

Adicionalmente, el estudio de la OCDE identificó los distintos enfoques adoptados por las jurisdicciones para plasmar tales derechos y garantías en su normativa:

a) **Carta/Declaración de derechos de los contribuyentes:** Algunas jurisdicciones concentraron las medidas adoptadas para proteger a los contribuyentes en una carta o declaración general de principios generales que debe regir la relación entre las autoridades tributarias y el contribuyente. Tal es el caso de Estados Unidos[8] o Canadá[9] que cuentan con una Carta de Derechos del Contribuyente. En otros países, estos documentos proporcionan una guía más detallada de los derechos de los contribuyentes enfocada en alguna de las fases del proceso de evaluación, como la Carta de Derechos del Contribuyente Auditado[10], en el caso de México, o de Honduras y la carta de Derechos y Obligaciones del OT en Actuaciones de Fiscalización[11].

b) **Inclusión en declaraciones de la administración tributaria:** Donde algunas jurisdicciones optaron por incluir señalamientos sobre los comportamientos esperados de los funcionarios y contribuyentes como parte de la misión de las administraciones tributarias. Tal es el caso del Reino Unido[12], que en el documento conocido como *HMRC Charter* (Carta HMRC) se define el servicio y el estándar de comportamiento que los clientes deben esperar al interactuar con la administración tributaria de dicha jurisdicción.

c) **Reconocimiento tácito a través de otras disposiciones fiscales:** Algunas jurisdicciones no cuentan con una declaración expresa que señale los derechos de los contribuyentes, sin embargo, en sus disposiciones fiscales existe un reconocimiento por parte de la autoridad tributaria respecto de derechos similares o equiparables a los derechos y garantías de los contribuyentes. Un ejemplo de este enfoque se encuentra en la legislación de Costa Rica, que en su Código de Normas y Procedimientos Tributarios[13] incluye un capítulo enfocado en los derechos y garantías del contribuyente.

   Aun cuando el estudio de la OCDE antes referido no lo señala expresamente, es conveniente agregar una categoría adicional a las previamente indicadas:

---

8 Documento disponible en https://www.irs.gov/es/taxpayer-bill-of-rights

9 Documento disponible en https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/taxpayer-bill-rights.html

10 Documento disponible en http://omawww.sat.gob.mx/informacion_fiscal/derechos_contribuyentes/Documents/Carta_Contr_Aud_072014.pdf

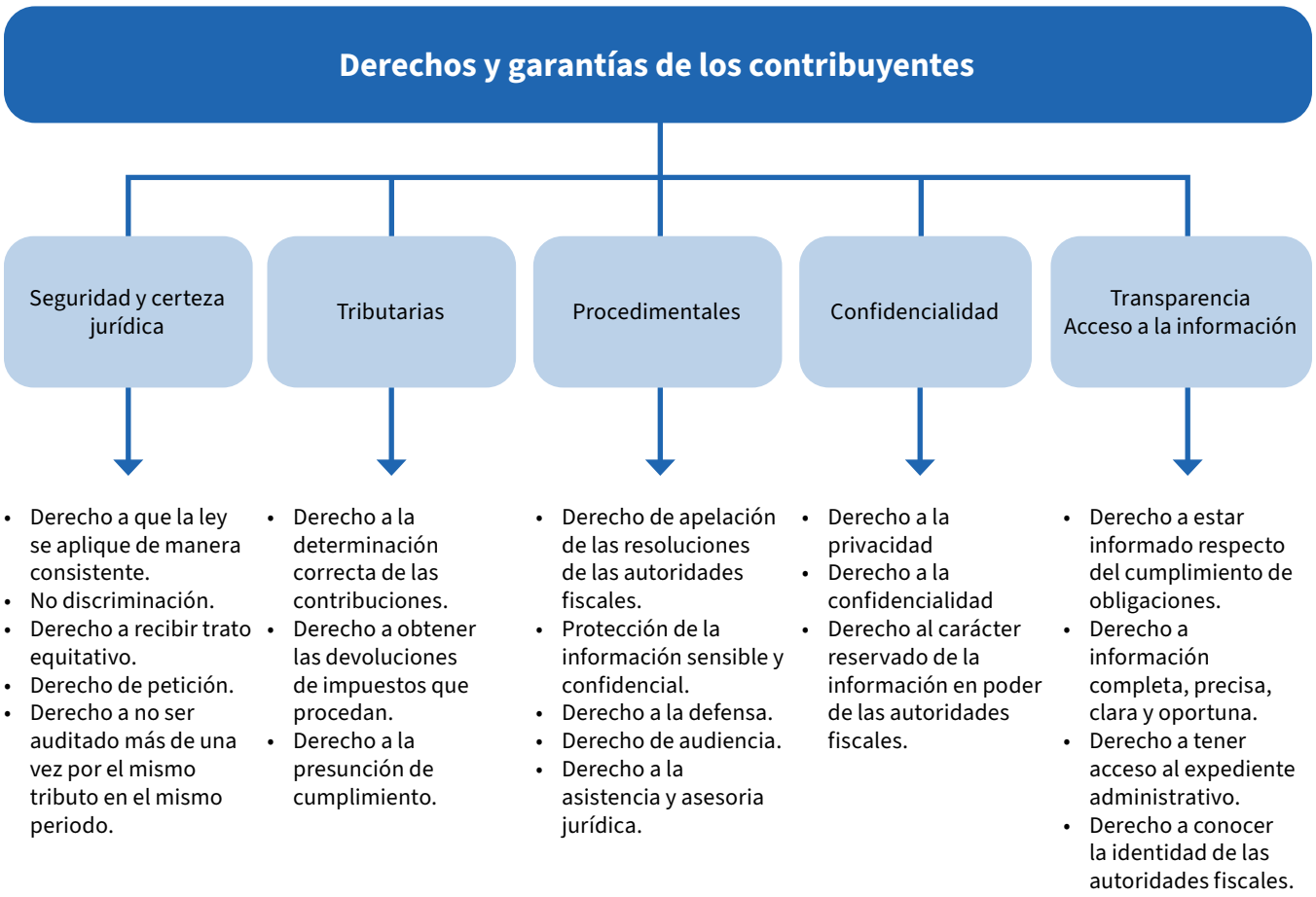
11 Documento disponible en https://www.sar.gob.hn/derechos-y-obligaciones/

12 Información complementaria disponible en https://www.gov.uk/government/publications/hmrc-charter/the-hmrc-charter

13 Texto completo disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_articulo.aspx?param1=NRA&nValor1=1&nValor2=73336&nValor3=89973&nValor5=3

d) Elevación a rango de ley: Existen jurisdicciones en las que el reconocimiento de los derechos y garantías básicas del contribuyente en su relación con las autoridades fiscales se encuentra consignado en una Ley con el fin de garantizar la protección y seguridad jurídica al más alto nivel normativo posible; tal enfoque es el adoptado por México con la Ley Federal de Derechos del Contribuyente[14] .

Con independencia del enfoque adoptado, es válido señalar que los principales derechos y garantías fundamentales de los contribuyentes podrían clasificarse en las siguientes categorías atendiendo al bien tutelado o protegido o al ámbito de aplicación:



Fuente: Clasificación de los derechos y garantías de los contribuyentes

Tomando como punto de partida lo señalado en esta sección, a continuación se analizarán con mayor detalle diversos aspectos normativos relevantes relacionados con la confidencialidad y protección de la información en poder de las autoridades tributarias, la transparencia, así como el acceso y uso adecuado de la información con el objeto de proporcionar elementos suficientes para fomentar el uso ético de la información mientras

[14] Texto completo disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFDC.pdf

salvaguardan las garantías fundamentales del contribuyente, asegurando así un equilibrio adecuado entre la transparencia fiscal y la protección de los derechos individuales.

3.3. Confidencialidad de la información y protección de datos

Como ya se indicó anteriormente, uno de los derechos fundamentales de los contribuyentes es el derecho a la privacidad y la confidencialidad de la información en poder de las autoridades fiscales. La confidencialidad de la información fiscal es un pilar fundamental en la relación entre los contribuyentes y las administraciones tributarias. La protección de los datos financieros, fiscales y personales de los ciudadanos es esencial para fomentar la confianza en el sistema tributario y garantizar el respeto a los derechos individuales. La protección de la información no solo implica evitar su divulgación no autorizada, sino también asegurar su uso adecuado y resguardar ante cualquier vulnerabilidad que pueda comprometer su seguridad. En este sentido, los marcos normativos juegan un rol crucial en la preservación de la confidencialidad de los datos fiscales, promoviendo así la integridad y la equidad en la gestión financiera.

A partir de lo anterior, se determina que el marco normativo de cada jurisdicción requiere de disposiciones enfocadas en la protección de la información en general -y en lo particular, de la confidencialidad- que sean lo suficientemente precisas, claras y detalladas y expresamente delimiten las circunstancias bajo las cuales esta información podrá revelarse y utilizarse.

En el contexto fiscal, la preservación de la confidencialidad de la información o el secreto fiscal como comúnmente se le conoce constituye “un instrumento de protección al contribuyente, consistente en la obligación de reserva por parte de las autoridades fiscales en todo lo relativo a su información tributaria como lo son sus declaraciones y datos suministrados por el propio contribuyente o por terceros, así como los que obtenga la autoridad en el ejercicio de sus facultades de comprobación”[15] Lo anterior, implica que “este derecho del contribuyente es correlativo a la obligación de no hacer impuesta a la autoridad fiscal consistente en la no revelación de la mencionada información”.[16]

Existen diversos principios básicos que rigen la protección de la confidencialidad de la información; estos principios son los que dan forma y consistencia a las leyes y normas que deberán incorporarse al marco jurídico.

---

[15] Prodecon. Transparencia, Secreto Fiscal y Uso Indebido de Comprobantes, 2014, p. 2. Documento disponible en https://portal.prodecon.gob.mx/Documentos/analisis-sistemicos/estudios-tecnicos/secreto-fiscal/mobile/index.html#p=1

[16] Idem.

Al respecto, la Organización de Estados Americanos publicó un listado de los principios actualizados[17] en materia de privacidad y protección de datos personales que cubren de manera integral todos los aspectos que las jurisdicciones deberán considerar al momento de diseñar normas, procesos y procedimientos. Tales principios son:

a) **Finalidades legítimas y legalidad:** Los datos personales deberán ser recopilados solamente para finalidades legítimas y por medios legales y legítimos.

b) **Transparencia y consentimiento**: Debe indicarse la finalidad específica que justifique su recopilación, el fundamento jurídico que lo sustenta, los sujetos a los que se les comunicará y los derechos de su titular.

c) **Pertinencia y necesidad:** Solo se recabarán los datos que resulten adecuados, pertinentes y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior.

d) **Tratamiento y conservación limitados:** Los datos deberán ser tratados y conservados de manera legítima compatible con la finalidad para la cual se recabó; su conservación no debe exceder del tiempo necesario para cumplir tal finalidad.

e) **Confidencialidad:** Los datos no deberán divulgarse, ponerse a disposición de terceros ni utilizarse para fines distintos de aquellos para los que fueron recopilados, excepto por mandato legal o consentimiento expreso del titular.

f) **Seguridad de los datos:** la confidencialidad, integridad y disponibilidad de los datos deberían ser protegidas mediante salvaguardas de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos.

g) **Exactitud de los datos:** Los datos deben mantenerse exactos, completos, y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad.

h) **Acceso, rectificación, cancelación, oposición y portabilidad**. Las jurisdicciones deben contar con métodos y mecanismos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados, puedan solicitar el acceso, rectificación y cancelación de estos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales.

i) **Datos personales sensibles:** Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas domésticas.

[17] OEA, *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales,* 2021. Texto completo disponible en https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

j) **Responsabilidad:** Deberán adoptarse e implementarse medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar que se cumplen con las normativas en materia de protección de datos. Estas medidas serán objeto de auditoría y actualización periódicas.

k) **Flujo transfronterizo de datos y responsabilidad:** (aplicable solo en el contexto de los miembros de la OEA) referido a la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción sean efectivamente responsables por el cumplimiento de estos Principios.

l) **Excepciones:** Cualquier excepción deberá estar prevista de manera expresa y específica en la legislación nacional, ser hecha del conocimiento de los ciudadanos y limitarse a casos específicos (seguridad nacional, orden público, interés público, entre otros).

m) **Autoridades de protección de datos:** Establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos.

Estos principios necesariamente deberán estar presentes en las normativas de las jurisdicciones a efecto de considerar que se cuenta con un marco jurídico que efectivamente garantiza la preservación de la confidencialidad de la información y la protección de los datos en su poder.

Finalmente, en relación con el cuerpo normativo donde deberán incorporarse a la normatividad vigente, la OCDE ha señalado que las normas de protección de la confidencialidad pueden encontrarse en "leyes, regulaciones secundarias o ejecutivas o guías administrativas. Sea cual sea el instrumento legal utilizado, estos deben ser jurídicamente vinculantes y aplicables"[18]. A partir de lo anterior, es válido concluir que las jurisdicciones pueden incluir disposiciones relativas a la confidencialidad de la información en el cuerpo legal que les resulte más adecuado o conveniente siempre y cuando éste goce de validez jurídica y sea susceptible de aplicarse y tener efectos jurídicos plenos. En el mismo tenor, no existen limitantes respecto del enfoque que dicha normatividad tenga, es decir, las normas de protección de la confidencialidad "pueden estar recogidas en leyes tributarias o en leyes de índole más general (por ejemplo, las disposiciones legales sobre la función pública o sobre las obligaciones de los funcionarios del servicio civil), en leyes sobre protección de la esfera privada y los datos personales u otras leyes"[19].

[18] OECD, *Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información*, OECD Publishing, 2021. p. 11

[19] Ídem.

3.4. Acceso a la información pública y transparencia

De acuerdo con la UNESCO, el acceso a la información puede definirse como el "derecho a buscar, recibir y difundir información en poder de los organismos públicos"[20]. Es uno de los derechos fundamentales reconocidos por la Declaración Universal de los Derechos Humanos, como parte integrante del derecho a la libertad de expresión. Como tal, el acceso a la información es entonces una prerrogativa que tiene su origen en el derecho a la información.

Por su parte, la transparencia podría definirse como el "conjunto de decisiones y acciones del gobierno que tienen por objeto dotar a los ciudadanos de información clara, precisa, accesible y abundante sobre dimensiones diversas del desempeño gubernamental".

No obstante, con la evolución de las políticas de datos abiertos, el concepto de transparencia se ha modificado también, por lo que ahora es factible hablar de dos *niveles o generaciones de transparencia*. Esto es, la noción convencional de transparencia (identificada como de primera generación) es la que se regula a través de las leyes de acceso a la información gubernamental, su objetivo es amplio y abstracto ya que busca la promoción del derecho a la información en general mientras que la segunda generación, llamada *transparencia focalizada* consiste en la "divulgación, por parte de entidades públicas o privadas, de información pública dirigida a una audiencia determinada[21]"; es decir, las autoridades adicionalmente ponen a disposición de sujetos específicos, datos e información específica o especializada.

En conjunto, el derecho al acceso a la información y la transparencia resultan esenciales para promover la democracia ya que garantiza que la ciudadanía contará con la información suficiente para participar plenamente en los asuntos de interés público. Esta interacción promueve la rendición de cuentas, obliga a los servidores públicos a actuar de manera responsable lo que resulta en una mayor confianza en las instituciones públicas y el gobierno en general.

Las políticas de datos abiertos y su gobernanza se han convertido en una tendencia que busca transformar la gestión pública promoviendo la transparencia y participación ciudadana. El concepto gira en torno a la noción de que la información generada por las instituciones públicas deberá estar disponible para cualquier persona, en formatos accesibles, abiertos y gratuitos que faciliten su uso e interpretación.

Este tema se abordará con mayor detalle en la sección relativa a la Gobernanza de Datos en las Administraciones Tributarias.

---

[20] https://www.unesco.org/en/access-information-laws

[21] Organización de Estados Americanos, *El Acceso a la Información Pública, un Derecho para ejercer otros Derechos.* 2013, pp 17-18.

3.5. Marco sancionador

Una de las potestades más importantes con que cuenta el Estado se refiere a su acción punitiva, definida como "la posibilidad jurídica de la imposición de sanciones a los particulares y aún a los funcionarios que infringen sus disposiciones, o a sus servidores que, en el ejercicio de sus funciones, transgreden sus mandatos o desconocen sus prohibiciones"[22].

De lo anterior se desprende que el Estado, encarnado en las autoridades administrativas cuenta con facultades para aplicar sanciones a aquellos sujetos que infrinjan los ordenamientos jurídicos. Los sujetos susceptibles de ser sancionados abarcan desde los particulares hasta los funcionarios y servidores públicos que incumplan las normas o cometan conductas ilícitas.

En el contexto de presente documento, la existencia de procedimientos administrativos sancionatorios contribuye a asegurar la transparencia y la protección de los derechos de los particulares disminuyendo el riesgo de la aplicación de medidas desproporcionadas, evitando la arbitrariedad en el ejercicio del poder estatal, mientras se preserva el orden y la legalidad.

Así, el procedimiento administrativo sancionador garantizará la transparencia y el acceso a la información siempre que se encuentre respaldado por un marco legal claramente definido que asegure que las acciones de las autoridades administrativas están sujetas a disposiciones legales específicas.

En ese sentido, deberá existir un balance entre el acceso a la información y la protección de los derechos de los contribuyentes; por lo tanto, resulta crucial garantizar que, la divulgación y el acceso público a la información en poder de las autoridades se lleve a cabo de manera compatible con la protección de los derechos de los contribuyentes y la confidencialidad de la información sensible.

En virtud de lo anterior, las jurisdicciones deben contar con mecanismos y protocolos adecuados para proteger la confidencialidad de la información y los derechos del contribuyente mientras se concede el acceso a la información pública sin identificar de manera individual a los contribuyentes, salvo los casos en que la ley expresamente lo requiera.

En esta sección se abordarán los principios y aspectos más relevantes que deberán tomarse en consideración al revisar o en su caso, diseñar las disposiciones normativas que constituyen el marco sancionador en materia de confidencialidad, transparencia y acceso a la información.

---

[22] Ossa Arbeláez, Jaime, *Derecho Administrativo Sancionador. Hacia una teoría general y una aproximación para su autonomía,* Colombia, Legis, 2000, p. 126 – citado en: *Estudios en Homenaje a Héctor Fix Zamudio – El reconocimiento del Derecho Administrativo Sancionador en la Jurisprudencia Constitucional Mexicana,* Góngora Pimentel, Genaro David, IIJ – UNAM, p. 257.

Un sistema legal robusto necesariamente debe contar con normas y procedimientos cuyo objetivo sea garantizar el cumplimiento de las obligaciones y disposiciones legales. Las sanciones tienen como propósito castigar las conductas infractoras y procurar que los sujetos infractores no vuelvan a incurrir en su incumplimiento. Es decir, son medidas disuasivas y represivas enfocadas en evitar la reincidencia de los infractores.

Ley especial contra delitos informáticos y conexos. El Salvador.

La legislación penal de El Salvador vigente desde el año 1998, marginalmente hacía referencia a delitos efectuados mediante el uso de las tecnologías de la información y la comunicación; no fue sino hasta 2016 que se promulgó la Ley Especial contra Delitos Informáticos y Conexos que establece el tratamiento legal específico que se le deberá dar a las conductas indebidas o ilícitas que se lleven a cabo haciendo uso de Tecnologías de la Información y la Comunicación.

Al respecto, resalta el hecho de que esta Ley establece que se considerarán como agravantes aquellos delitos que recaigan en programas o sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público, o destinados a la prestación de servicios financieros o bien, si los delitos comprendidos en la legislación son cometidos por funcionarios, empleados públicos y municipales, autoridad pública o agentes de autoridad, en cuyo caso serán sancionados con la pena máxima correspondiente, aumentada hasta en una tercera parte del máximo establecido de la pena y la inhabilitación del ejercicio de su profesión durante el tiempo que dure la condena.

Este caso ejemplifica de manera notable la interacción entre disposiciones administrativas y penales con el fin de establecer marco jurídico integral y robusto enfocado en la confidencialidad de la información, velando por su uso adecuado y previniendo su divulgación inadecuada.

En ese sentido, existen diversos tipos de sanciones susceptibles de imponerse ante circunstancias específicas que pueden individualizarse atendiendo a la naturaleza de la conducta infractora, la gravedad de ésta, la calidad del sujeto infractor y la repetición o reincidencia en la conducta.

En el contexto de la presente guía se requiere que las administraciones fiscales tengan la potestad de aplicar sanciones efectivas ante casos de uso o divulgación indebida de la información, violaciones de la confidencialidad, faltas a las obligaciones de transparencia, etc.

Atendiendo a lo anterior, las sanciones, según su naturaleza, se dividen en:

a) **Disciplinarias o administrativas:** Por ejemplo, la amonestación, suspensión, destitución o inhabilitación de servidores públicos infractores.

b) **Patrimoniales o pecuniarias:** Referidas a obligaciones de pago de cantidades de dinero por la comisión de una infracción, como las multas.

c) **Penales:** Se aplican cuando la infracción cometida configura un delito y pueden ser privativas de la libertad o los derechos del infractor.

Ahora bien, de manera general, las infracciones y sanciones relativas a las violaciones a la confidencialidad, al uso o divulgación indebida de la información o, incluso, las faltas a las obligaciones de transparencia deben alinearse con diversos principios, tales como el principio de legalidad, proporcionalidad, irretroactividad y prescripción.

a) **Principio de legalidad.** Implica que la descripción genérica de las infracciones necesariamente debe estar contenida en un cuerpo legal. Esto significa que, si bien "*las sanciones pueden estar contenidas en la legislación tributaria, de administración pública o penal, o en una combinación de todas ellas (…), lo importante es que se tengan debidamente en cuenta multas o sanciones administrativas, civiles y/o penales, que cubran una amplia gama de violaciones de la confidencialidad o uso indebido de la información*"[23] de transparencia y acceso a la información. Esto significa que independientemente del cuerpo legal que las contenga o de la naturaleza que se les atribuya, lo esencial es que dichas infracciones, multas y/o sanciones estén formuladas de manera clara y precisa y sean lo suficientemente contundentes como para disuadir cualquier infracción o violación a la normatividad.

   El principio de legalidad se refiere también al instrumento administrativo o judicial en el cual se resuelva o determine la aplicación de la sanción al infractor con el fin de dotar de certeza y seguridad jurídica a las partes involucradas.

b) **Principio de proporcionalidad.** Se debe concretar también en dos niveles, inicialmente al momento de identificar la infracción y atribuir una sanción donde el legislador deberá mantener un equilibrio entre la falta y la sanción que corresponda.

   El segundo nivel debe observarse al momento de la aplicación de la sanción, donde deberá indicarse el alcance de esta atendiendo a las circunstancias específicas del caso (gravedad, reincidencia, daño causado por la violación, etc.)

[23] OECD, *Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información*, OECD Publishing, 2021. p. 95.

c) **Principio de irretroactividad.** Este principio salvaguarda las garantías de legalidad y seguridad jurídica ya que solo podrá aplicarse la normatividad vigente en el momento en que se producen los hechos para determinar si éstos efectivamente constituyen una infracción. En consecuencia, solo podrán aplicarse las sanciones que expresamente estén contempladas en la normatividad vigente al momento de su realización.

d) **Principio de prescripción**. se refiere a que, por lo general, el transcurso del tiempo dará lugar a la extinción de las infracciones y sanciones administrativas. Sin embargo, debe aclararse que en el plazo de cómputo para dicha prescripción se suspende una vez que se inicia el proceso administrativo sancionador.

Tratándose de infracciones relacionadas con cuestiones de confidencialidad y seguridad de la información, uso y divulgación inadecuado de la información y faltas en materia de transparencia deben tomarse en consideración diversas cuestiones tales como la calidad de los sujetos que cometen la infracción (servidores públicos -incluyendo trabajadores fijos, eventuales o temporales, o incluso trabajadores retirados, trabajadores externos) y la gravedad de la infracción (a partir valoración del daño causado por la infracción), entre otras.

Lo anterior es así, toda vez que la evaluación de la gravedad de una infracción relacionada con cuestiones de confidencialidad y seguridad de la información o bien respecto del uso y divulgación inadecuado de la información debe considerar no solo la naturaleza y sensibilidad de la información comprometida, sino también el contexto y las circunstancias bajo las cuales se cometió dicha infracción.

Ejemplo de clasificación de la gravedad de las infracciones. Costa Rica

Un ejemplo de la distinción de la gravedad de las infracciones se encuentra en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales – Ley No. 8968 publicada el 05 de septiembre de 2011.

Esta normativa, en sus artículos 29, 30 y 31, clasifica las faltas como leves, graves y gravísimas describiendo claramente los supuestos concretos que corresponden a cada categoría y estableciendo sanciones específicas para cada caso.

Faltas Leves: Recolectar datos personales sin que se le otorgue suficiente información al interesado; recolectar, almacenar y transmitir datos personales de terceros por medio de mecanismos inseguros o que no garanticen la seguridad e inalterabilidad de los datos.

En este caso, la sanción aplicable es una multa hasta de cinco salarios base.

Faltas Graves: Entre otras, recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular; emplear datos personales para una finalidad distinta de la autorizada por el titular; negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases o bien, negarse a modificar, corregir o eliminar tales datos si así lo solicita el titular.

La sanción establecida es una multa que va de los cinco a los veinte salarios base.

Faltas Gravísimas: Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos sensibles; obtener datos personales de una persona mediante engaño, violencia o amenaza, revelar información cuyo secreto esté obligado a guardar conforme a la ley o transferir, a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus titulares, entre otros Aplica multa de entre quince y treinta salarios base y suspensión de hasta seis meses.

Esto significa que aquellas violaciones que involucren datos clasificados como altamente confidenciales o críticos requerirán una sanción más enérgica y efectiva que aquellas infracciones que afecten información menos sensible. Al respecto, la OCDE ha señalado que aun cuando "la violación de la confidencialidad del contribuyente puede proceder de un acto involuntario, deficiencias en los sistemas y procedimientos que protegen la confidencialidad de la información, o puede ser consecuencia de acciones intencionadas en beneficio personal por parte de una o más personas (por ejemplo, en caso de corrupción). (…) cualquier violación de la confidencialidad debe tomarse en serio y abordarse de inmediato (y) deben adoptarse medidas adecuadas en función de las circunstancias de la infracción."[24]

En adición a lo anterior, resulta fundamental tomar en cuenta los protocolos y normativas que las jurisdicciones hayan establecido en materia de protección de datos y transparencia, asegurando que las sanciones sean proporcionales a la magnitud de la infracción con el fin de promover una cultura de responsabilidad y cumplimiento en todas las instancias gubernamentales y organizaciones involucradas.

En virtud de ello, es crucial para las jurisdicciones el establecer mecanismos efectivos de monitoreo y supervisión para prevenir futuras infracciones y garantizar la integridad y confianza en los sistemas de manejo de información. Esto implica que, además del marco normativo adecuado, debe considerarse la implementación de controles adecuados, capacitación constante del personal y una respuesta rápida y contundente ante cualquier violación detectada, con el fin de salvaguardar los derechos de los

[24] Ídem.

contribuyentes. Este tema en particular se abordará en el capítulo relativo al marco de Gestión de Seguridad de la Información (GSI).

Los aspectos más relevantes que deberán considerarse al momento de implementar el marco sancionatorio son los siguientes:

a) Identificación de los sujetos que la legislación considerará como sujetos obligados a los que se les fincará responsabilidad por las violaciones a las obligaciones de confidencialidad, transparencia y acceso a la información.

b) Descripción detallada de las conductas que se considerarán faltas, infracciones y delitos en materia de confidencialidad, protección de datos y transparencia. Las conductas deberán encontrarse expresamente definidas en la legislación; no deberá permitirse la aplicación de analogías con el fin de dar certeza y seguridad jurídica a los sujetos obligados.

c) Los tipos de violaciones podrán clasificarse atendiendo a su gravedad o al grado de daño que se cause con su comisión.

d) Identificar los supuestos que se considerarán agravantes o atenuantes de las conductas. Estas condiciones serán tomadas en cuenta al momento de imponer la sanción y pueden referirse a cuestiones tales como la reincidencia, el carácter intencional de la infracción, el tipo de información que fue vulnerada, entre otros.

e) Establecer claramente el procedimiento para la imposición de sanciones, indicando de manera precisa las etapas del procedimiento y la forma en la que se desahogará cada fase.

A partir de lo anterior, se puede concluir que independientemente de las diferencias en los enfoques y el tratamiento que cada país decida aplicar, lo crucial es contar con un marco normativo que cuente con los elementos requeridos para proteger los derechos fundamentales de los contribuyentes en este ámbito, donde cada jurisdicción ha establecido disposiciones específicas para abordar las diversas infracciones que pueden cometerse, desde el acceso indebido a información confidencial hasta la divulgación inapropiada de datos sensibles. Las sanciones previstas incluyen multas, suspensiones temporales de funciones o inhabilitación de los servidores públicos o incluso, acciones penales, asegurando así una respuesta proporcional y efectiva ante las violaciones de las disposiciones en materia de transparencia, protección de datos y confidencialidad de la información.

País	Tipo de sanción	Ejemplos de infracciones	Sanción
Costa Rica	Administrativas	• No entrega de información pública • Violación de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.	• Multas • Advertencias o amonestaciones
	Penales	• Revelación de datos confidenciales sin autorización.	• Prisión • Multas
	Patrimoniales	• Uso indebido de información personal.	• Indemnización por daños
El Salvador	Administrativas	• Negativa a proporcionar información pública.	• Multas • Suspensión de funciones
	Penales	• Ocultamiento de información pública.	• Prisión • Multas
	Patrimoniales	• Uso indebido de fondos públicos.	• Indemnización o reembolso de daños
Guatemala	Administrativas	• No cumplimiento de solicitudes de acceso a la información.	• Multas • Inhabilitación
	Penales	• Revelación de información confidencial.	• Prisión • Multas
	Patrimoniales	• Uso indebido de recursos públicos.	• Indemnización
Honduras	Administrativas	• No proporcionar información solicitada.	• Multas • Advertencias
	Penales	• Revelación de datos sin autorización.	• Prisión • Multas
	Patrimoniales	• Daños a la imagen pública.	• Indemnizaciones
Panamá	Administrativas	• Negativa a entregar información pública	• Multas • Sanciones administrativas
	Penales	• Obstrucción a la información pública	• Prisión • Multas
	Patrimoniales	• Uso indebido de información pública	• Indemnizaciones
República Dominicana	Administrativas	• Falta de entrega de información pública	• Multas • Suspensión
	Penales	• Revelación indebida de información	• Prisión • Multas
	Patrimoniales	• Uso indebido de fondos públicos	• Indemnizaciones

Ámbito internacional

En general, las disposiciones contenidas en los instrumentos internacionales en materia fiscal, tales como la Convención sobre Asistencia Administrativa Mutua en Materia Fiscal, los Modelos Convenio sobre la Renta, así como los convenios y acuerdos que se basan en dichos modelos establecen distintos lineamientos que aplican respecto de la **confidencialidad y protección de la información**.

Entre los aspectos más relevantes previstos en tales instrumentos sobresalen:

a) La información que las autoridades de una jurisdicción reciban -a través del intercambio de información- deberá ser tratada como secreta aplicando las mismas reglas y criterios que aplicarían para la información obtenida bajo las leyes nacionales de dicha jurisdicción.

b) La información solo podrá utilizarse para objetivos y fines específicos y siempre deberá guardar relación con los impuestos materia del instrumento de que se trate.

c) La información solo podrá divulgarse a personas o autoridades específicas, incluyendo tribunales y organismos administrativos encargados de la evaluación, recaudación, aplicación, procedimientos judiciales y determinación de recursos.

Las jurisdicciones deben garantizar que preservarán la confidencialidad de la información intercambiada en los mismos términos aplicables a la información obtenida en virtud de su legislación nacional.

Lo anterior implica que las jurisdicciones están obligadas a preservar el secreto o la confidencialidad de la información intercambiada con base en instrumentos internacionales utilizando los **mismos criterios** que aplican a la información recabada en virtud de su legislación nacional. Es por ello que resulta crucial que las jurisdicciones cuenten con normatividad interna adecuada para identificar conductas indebidas o ilícitas y sancionarlas de manera apropiada con el fin de disuadir su realización y, en consecuencia, proteger la confidencialidad y el uso adecuado de la información.

Disposiciones de confidencialidad contenidas en los Modelos Convenio y otros Instrumentos Internacionales.

Convención sobre Asistencia Administrativa Mutua en Materia Fiscal

Artículo 22. Secrecía

1. *Cualquier información obtenida por una Parte de conformidad con esta Convención deberá mantenerse como secreta y deberá protegerse de la misma manera que la información obtenida con base en la legislación interna de esa Parte y, en la medida en que se requiera para asegurar el nivel necesario de protección de datos personales, de conformidad con las salvaguardas que puedan especificarse por la Parte que proporciona la información, según lo requiera su legislación interna.*

2. *Dicha información, en cualquier caso, podrá ser revelada únicamente a las personas o autoridades (incluidos los tribunales y órganos administrativos o de supervisión) encargadas de la determinación, recaudación o cobro de los impuestos de esa Parte, de los procedimientos declarativos o ejecutivos relativos a dichos impuestos o de la resolución de los recursos relativos a los mismos o de la supervisión de lo anterior. Únicamente estas personas o autoridades podrán utilizar la información, y sólo para los fines señalados. No obstante, lo dispuesto en el párrafo 1, dichas personas o autoridades podrán revelar la información en las audiencias públicas de los tribunales o en las sentencias judiciales relacionadas con dichos impuestos.*

3. *Si una Parte formula una reserva de conformidad con el inciso a del párrafo 1 del Artículo 30, cualquier otra Parte que obtenga información de la Parte mencionada en primer lugar no utilizará dicha información en relación con un impuesto que se encuentre en una categoría que esté sujeta a reserva. De igual forma, la Parte que formule dicha reserva no utilizará la información obtenida de conformidad con esta Convención en relación con un impuesto de una categoría que esté sujeta a reserva.*

4. *Sin perjuicio de lo dispuesto en los párrafos 1, 2 y 3 la información que reciba una Parte podrá ser utilizada para otros efectos cuando ello sea factible de conformidad con la legislación de la Parte que otorgue la información y la autoridad competente de esa Parte autorice dicho uso. La información que una Parte otorgue a otra Parte puede transmitirse por esta última a una tercera Parte, previa autorización de la autoridad competente de la Parte mencionada en primer lugar.*

Un ejemplo de lo anterior se encuentra en el *Estándar para el Intercambio Automático de Información sobre Cuentas Financieras en Materia Fiscal* [25] que indica, en los Comentarios al Modelo de Acuerdo entre Autoridades Competentes, específicamente en relación con la aplicación de penas y sanciones, lo siguiente:

Modelo OCDE – Convenio Tributario sobre la Renta y sobre el Patrimonio
Artículo 26 – segundo párrafo

2. Cualquier información, del tipo recogido en el párrafo 1 y recibida por un Estado contratante será mantenida tan en secreto como la información obtenida de conformidad con la legislación nacional de dicho Estado y únicamente se revelará a las personas o autoridades (incluidos tribunales y organismos administrativos) que participen en labores de evaluación o recaudación de los impuestos indicados en el párrafo 1, en los procedimientos declarativos o ejecutivos relativos a dichos impuestos, o en la resolución de los recursos relativos a los mismos, o también en la supervisión de lo anterior. Dichas personas o autoridades solo utilizarán la información para dichos fines. Podrán revelar la información en audiencias públicas ante los tribunales o en las sentencias judiciales.

Modelo ONU – Convenio Tributario sobre la Renta y sobre el Patrimonio
Artículo 26 – segundo párrafo

2. La información recibida por un Estado Contratante en virtud del apartado 1 se considerará secreta, de la misma forma que la información obtenida de conformidad con la legislación interna de ese Estado, y solo será revelada a las personas o autoridades (incluidos los órganos jurisdiccionales y administrativos) encargadas de la liquidación o recaudación de los impuestos a los que hace referencia el apartado 1, de su aplicación efectiva o enjuiciamiento por el incumplimiento relativo a los mismos, de la resolución de los recursos referentes a tales impuestos, o de la supervisión de las funciones antes mencionadas. Dichas personas o autoridades solo utilizarán la información para los mencionados fines y podrán revelar la información en las audiencias públicas de los tribunales o en las sentencias judiciales. No obstante, lo anterior, la información recibida por un Estado Contratante podrá utilizarse para otros fines cuando, conforme a las leyes de ambos Estados, pueda utilizarse para esos otros fines y la autoridad competente del Estado que suministra la información autorice dicho uso.

3.1. Penas y Sanciones

35. La legislación interna deberá imponer multas o sanciones por la divulgación o el uso indebido de la información de un contribuyente, al tiempo que las administraciones tributarias deberán, por su parte, imponer de facto esas multas y sanciones al personal que infrinja las políticas y procedimientos en

[25] OECD, *Estándar para el Intercambio Automático de Información sobre Cuentas Financieras,* OECD Publishing, 2017, p. 95.

materia de seguridad, con el fin de disuadir a otros de verse involucrados en infracciones similares. Para garantizar su aplicación, dicha legislación interna deberá reforzarse mediante recursos y procedimientos administrativos adecuados. Las administraciones tributarias deberán implementar un procedimiento sancionador formal aplicable al personal y proveedores externos de servicios que incumplan las políticas y procedimientos de seguridad en la información establecidos. Esas políticas deberán abarcar tanto sanciones civiles como penales aplicables en caso de inspección o divulgación no autorizadas.

Con base en lo señalado en este capítulo, se puede concluir que un marco jurídico adecuado debe garantizar una protección integral de los derechos fundamentales del contribuyente tanto en el ámbito doméstico como en el ámbito internacional. Es importante encontrar un equilibrio adecuado entre el acceso a la información y la transparencia respecto de la protección de la confidencialidad y la integridad de los datos. Por lo tanto, las leyes y políticas relacionadas con la confidencialidad deben establecerse con claridad y ser objeto de supervisión adecuada para evitar abusos y garantizar que se respeten los principios de transparencia y acceso a la información en la medida de lo posible.

Es fundamental establecer mecanismos efectivos de rendición de cuentas para asegurar que la información confidencial se maneje de manera responsable y se utilice solo en los términos expresamente previstos por la legislación. Esto puede implicar la implementación de salvaguardas internas, como protocolos de acceso restringido y sistemas de supervisión, así como la rendición de cuentas externa a través de auditorías independientes y la revisión por parte de organismos reguladores y de control. Estos temas serán abordados con mayor detalle en los siguientes capítulos.

4. Gestión de la seguridad y protección de la información

La digitalización de la economía y, en consecuencia, de las operaciones fiscales han transformado el horizonte de la seguridad tecnológica para las administraciones tributarias a nivel global. Esto ha resultado en nuevos desafíos y requerimientos en términos de protección de datos, infraestructura segura y cumplimiento normativo. Para hacer frente a estos desafíos, es crucial que las autoridades fiscales adopten medidas de seguridad cibernética efectivas y estén preparadas para adaptarse a un entorno digital en constante evolución.

Así, la gestión eficiente de la protección de la información tributaria se ha convertido en un aspecto esencial para las administraciones; la gradual y continua transición hacia la digitalización de los procesos y procedimientos fiscales genera, en consecuencia, una cantidad masiva de datos sensibles que requieren una protección sólida contra amenazas a su seguridad.

En este contexto, la implementación de un marco GSI adecuado es fundamental para salvaguardar la integridad, confidencialidad y disponibilidad de la información tributaria. Es por ello que la implementación de un marco GSI efectivo debe involucrar a todos los niveles de la organización en la protección de la información tributaria, fortaleciendo en general la seguridad cibernética de la administración mientras reduce el riesgo de incidentes de seguridad causados por errores humanos o negligencia.

Atendiendo a lo antes señalado, se considera que la implementación de un marco GSI proporciona a las administraciones tributarias las herramientas y los procesos necesarios para proteger la integridad, confidencialidad y disponibilidad de la información tributaria, asegurando así la confianza de los contribuyentes y fortaleciendo el cumplimiento de sus obligaciones fiscales.

En esta sección se abordarán los puntos estratégicos que las administraciones tributarias deberán tomar en consideración al momento de implementar un marco GSI que efectivamente establezca controles y procedimientos para proteger la información tributaria contra amenazas cibernéticas y riesgos tales como el acceso no autorizado, la manipulación de datos y el robo de información. Esto incluye la implementación de controles de acceso, cifrado de datos, monitoreo de eventos de seguridad y políticas de gestión de contraseñas, entre otros.

4.1. Seguridad de la información

La seguridad de la información puede definirse como "el proceso de mantener la confidencialidad, integridad y disponibilidad de los datos de una organización de manera coherente con su propia estrategia de riesgo"[26]. Este proceso se realiza a través de la implementación de medidas de protección, conocidas como salvaguardas, diseñadas para satisfacer los requerimientos de seguridad de un sistema informático, limitando su acceso y el manejo de la información. En adición a la protección de la confidencialidad, integridad y disponibilidad de la información, también es importante que se implementen medidas enfocadas en preservar la autenticidad, confiabilidad, trazabilidad y no repudio[27] de la información.

Los principales objetivos de la seguridad de la información en poder de las autoridades fiscales, para efectos de la presente guía, se pueden concentrar en tres grandes rubros:

a) Preservar la **privacidad** de los datos del contribuyente, restringiendo su acceso y divulgación.

b) Proteger la **integridad** de la información previniendo su modificación o destrucción indebida.

c) Mantener la **disponibilidad** y en su caso, procurar la recuperación de la información en tiempo y forma.

En el ámbito de la seguridad de la información se encuentra también la **ciberseguridad,** que es una rama especializada en la protección de los sistemas informáticos y las redes contra accesos no autorizados, actividades maliciosas y daños, es decir, se centra específicamente en la protección de las tecnologías diseñadas para facilitar el acceso y manejo de la información.

Aun cuando ambas ramas tienen como objetivo común la protección de la información confidencial, la principal diferencia entre ambas es que mientras que la ciberseguridad protege los dispositivos, sistemas y tecnologías conectados a Internet, la seguridad de la información también extiende su protección a cualquier información fuera de línea (i.e. datos, registros físicos y digitales, propiedad intelectual, entre otros).

Considerando lo anterior, las autoridades fiscales requieren diseñar e implementar estrictos protocolos de seguridad integrales, es decir, que abarquen tanto los sistemas tecnológicos como aspectos operativos y administrativos con el fin de disuadir, detener y evitar accesos no autorizados, manipulación de datos o pérdidas de información sensible. Esto incluye la adopción de medidas avanzadas de encriptación, sistemas de detección de intrusiones y la capacitación constante del personal en prácticas seguras de gestión de datos.

---

[26] Según lo define el *National Institute of Standards and Technology.* https://www.nccoe.nist.gov/data-security

[27] Este atributo permite probar la participación de las partes en una comunicación, es decir, da la certeza de que una parte no podrá negar posteriormente los datos originados.

En virtud de lo antes expuesto, puede señalarse que el marco GSI se centra en asegurar todos los activos de información de la administración fiscal, incluyendo datos confidenciales, información fiscal, información financiera, etc. El objetivo primordial de este marco es garantizar la confidencialidad, integridad y disponibilidad de la información a lo largo de su ciclo de vida, desde la creación hasta su eliminación.

A continuación, se abordarán algunas cuestiones relevantes que las autoridades fiscales deben tomar en consideración al momento de diseñar e implementar sus estrategias de seguridad de la información.

4.2. Estándares internacionales en materia de seguridad de la información

Los estándares internacionales en seguridad informática son conjuntos de mejores prácticas, directrices y requisitos técnicos diseñados para promover la seguridad y protección de la información en organizaciones y sistemas a nivel global. El objetivo primordial de estos estándares es apoyar en el establecimiento e implementación de prácticas sólidas de seguridad informática, proteger los datos confidenciales, gestionar riesgos y cumplir con las regulaciones aplicables en diferentes jurisdicciones a nivel mundial.

En relación con lo anterior, la Organización Internacional de Normalización[28] (ISO, por sus siglas en inglés) es una organización internacional no gubernamental creada en 1947 que engloba diferentes comités técnicos integrados por grupos de expertos en materias diversas cuyo objetivo es diseñar normas estandarizadas internacionales. Actualmente cuenta con 171 países adheridos cuyos expertos han elaborado más de 20,000 normas internacionales y documentos relacionados.

Una de las normas más importantes diseñadas por la ISO es la serie **ISO/IEC-27000**[29] enfocada en la gestión de seguridad de la información. Esta norma engloba más de una docena de estándares más específicos enfocados en la gestión de la seguridad de la información y los sistemas GSI. Estos estándares, en conjunto, proporcionan un marco integral para establecer, implementar, mantener y mejorar la seguridad de la información dentro de la organización.

La serie ISO/IEC-27000 fue elaborada inicialmente en 2016, en 2018 fue sustituida por la norma que actualmente está vigente y se espera que en los próximos años sea reemplazada por la serie ISO/IEC WD – 27000.

[28] https://www.iso.org/es/home

[29] Esta serie fue elaborada por un Comité Técnico Conjunto integrado por expertos de la Organización Internacional de Normalización y de la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés), de ahí que se le identifique como serie ISO/IEC 27000.

El estándar ISO 27000 consta de varias normas, siendo las más conocidas y utilizadas:

a) **Norma ISO-27001.** Es la norma principal de la serie y establece los requisitos fundamentales para la implementación adecuada de un sistema de GSI. Esta norma establece el marco operativo, tecnológico e incluso normativo – regulatorio requerido para la implementación sistemática y consistente de medidas de seguridad informática.

b) **Norma ISO-27002.** Establece directrices y recomendaciones relativas a la implementación de controles de seguridad, acceso a la información y mantenimiento de sistemas tecnológicos.

c) **Norma ISO-27005.** Concentra las principales directrices en materia de gestión de riesgos de seguridad (identificación, evaluación y tratamiento).

d) **Normas complementarias.** (i.e. ISO-27003, ISO-27004, ISO-27006) Enfocadas en temas relativos a mediciones y métricas aplicables, certificación de sistemas de GSI, entre otras cuestiones.

Es necesario aclarar que no existe un único estándar GSI por lo que las administraciones fiscales podrán aplicar el que consideren más adecuado o acorde a sus necesidades y circunstancias[30]; sin embargo, tomando en consideración que la serie ISO/IEC-27000 es reconocida internacionalmente como la norma que engloba los estándares y mejores prácticas más comúnmente aplicadas en materia de seguridad de la información es que se tomará como referencia en el presente trabajo.

Ahora bien, con independencia de la norma que las administraciones fiscales utilicen como sustento para la implementación del marco GSI, dicha adopción traerá múltiples ventajas para la autoridad tributaria, tales como:

a) La autoridad fiscal estará en posibilidades de reaccionar de manera ágil para abordar incidentes y eventos de seguridad al aplicar controles físicos, administrativos y tecnológicos diseñados específicamente para gestionar aspectos tales como accesos (tanto de personal interno como externo), hardware, software, operaciones y comunicaciones.

b) La protección de la seguridad de la información abarcará todo tipo de información en poder de la autoridad fiscal: impresa o escrita en papel, almacenada electrónicamente, transmitida por medios electrónicos e incluso verbalmente.

[30] Entre los estándares en materia de seguridad de la información también se encuentra el *NIST Cybersecurity Framework* desarrollado por el *National Institute of Standards and Technology* de los Estados Unidos o bien, la normativa desarrollada por la Unión Europea conocida como *General Data Protection Regulation* o GDPR

c) La autoridad podrá valorar adecuadamente los riesgos a los que está potencialmente expuesta con base en un procedimiento y contará con los elementos suficientes para crear el plan óptimo para su atención y tratamiento.

d) La administración tributaria establecerá, paralelamente, los mecanismos para el cumplimiento legal y normativo relativos al uso y manejo adecuado de la información en poder de la autoridad fiscal.

e) Como consecuencia de la implementación del marco GSI, aumentará la confianza de los contribuyentes, otras dependencias al interior del gobierno, otras autoridades fiscales y la sociedad en general

Lo anterior corrobora los beneficios que conlleva el que las administraciones fiscales establezcan procesos y mecanismos dirigidos a proteger la información mediante la preservación de su confidencialidad, integridad y disponibilidad.

4.3. Implementación de la serie ISO/IEC-27000

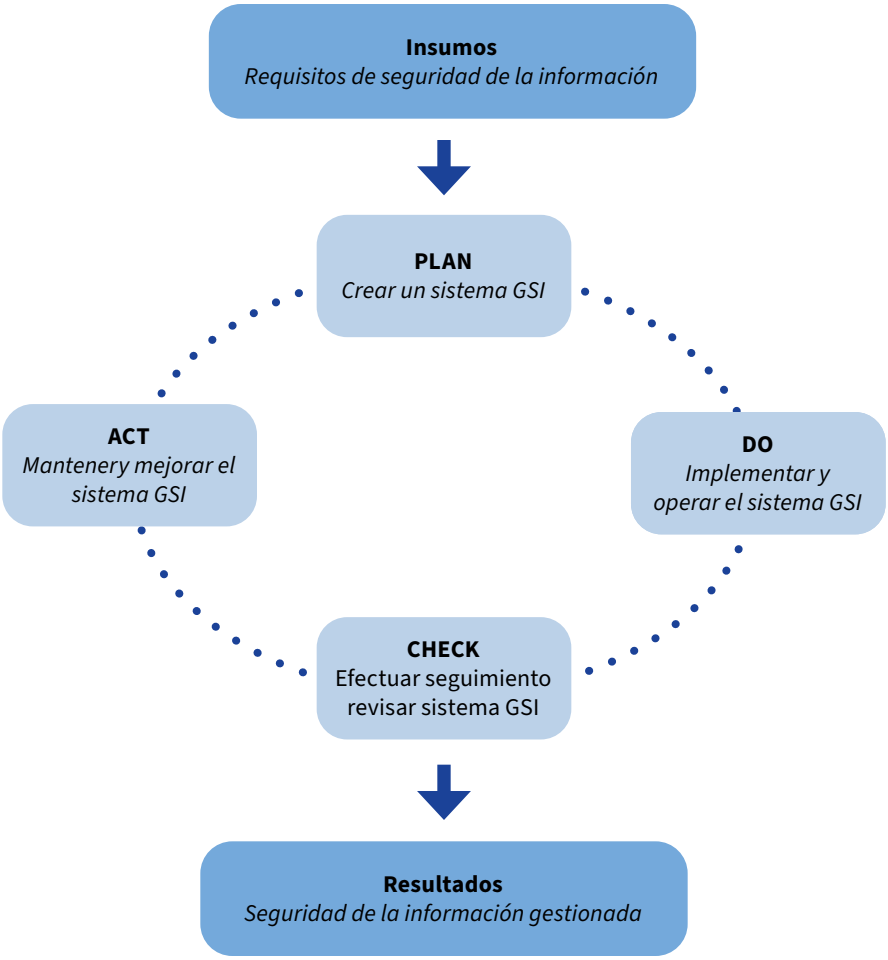
La serie 27000 se basa en el Ciclo de Deming, que fue diseñado como un método de mejora continua de procesos que se implementa en diferentes etapas o fases. Comúnmente, al ciclo de Deming también se le conoce como el Ciclo PDCA (*Plan, Do, Check, Act*¸ por su acrónimo en inglés).

En el contexto de las administraciones tributarias, la serie ISO/IEC-27000 se puede adaptar implementando controles de acceso específicos para los sistemas de gestión fiscal, monitoreo de redes y auditorías periódicas para garantizar la protección de los datos de los contribuyentes.

De manera general, puede señalarse que el Ciclo PDCA, aplicado al contexto de la seguridad de la información, implica “desarrollar e implementar un marco y un plan de seguridad de la información, aplicar los mecanismos de control de la seguridad según lo planeado, verificar que el plan funciona debidamente y mejorar continuamente el plan y los controles, reforzando las actividades que funcionan debidamente y modificando las que no lo hacen”[31]

En relación con lo anterior, el Foro Global ha esquematizado el ciclo de la siguiente manera:

[31] OECD, Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información, Op Cit., pág. 14.



Fuente: El ciclo PDCA en la Gestión de la Seguridad de la Información

Como ha quedado ejemplificado, el Ciclo PDCA constituye una metodología esencial para la gestión de la seguridad de los datos en poder de las administraciones fiscales. Su enfoque cíclico permite que las autoridades tributarias estén en posibilidades de implementar y optimizar sus prácticas de seguridad de manera continua. Aunado a ello, la adopción del Ciclo PDCA garantiza que la administración tributaria contará con medidas de seguridad efectivas pero que, a largo plazo, pueda adaptarse con facilidad a las nuevas amenazas y riesgos en materia de seguridad que pudieran surgir.

De manera general, el Ciclo PCDA se explica de la siguiente forma:

a) La primera fase corresponde a la etapa de **Planeación (PLAN),** mediante la cual las administraciones tributarias deberán identificar y evaluar los potenciales riesgos a los que se expone la seguridad de la información en poder de la autoridad. Este análisis incluye también la revisión de la normatividad aplicable, la evaluación de posibles vulnerabilidades de los sistemas para que, posteriormente, se

establezcan políticas y procedimientos encaminados a garantizar el cumplimiento normativo y la protección de datos e información fiscal.

b) En la segunda etapa, identificada como la fase de **Hacer (DO)**, la autoridad fiscal implementará las medidas de seguridad establecidas en la etapa de planeación; esto es, llevará a cabo la instalación de controles de acceso físico y lógico, sistemas de detección, capacitación del personal en prácticas seguras de manejo de la información fiscal. Esta etapa resulta fundamental en el ciclo ya que permite mitigar riesgos y fortalecer la seguridad de la administración.

c) La fase de **Verificar (CHECK)** se centra en monitorear y evaluar el desempeño de las medidas de seguridad implementadas. Dicho monitoreo se lleva a cabo mediante la ejecución de auditorías internas y externas, pruebas de penetración, análisis de registros y reportes de incidentes de seguridad. Los resultados de tales evaluaciones permiten identificar posibles áreas de mejora y ajustar las estrategias de seguridad para asegurar su efectividad continua.

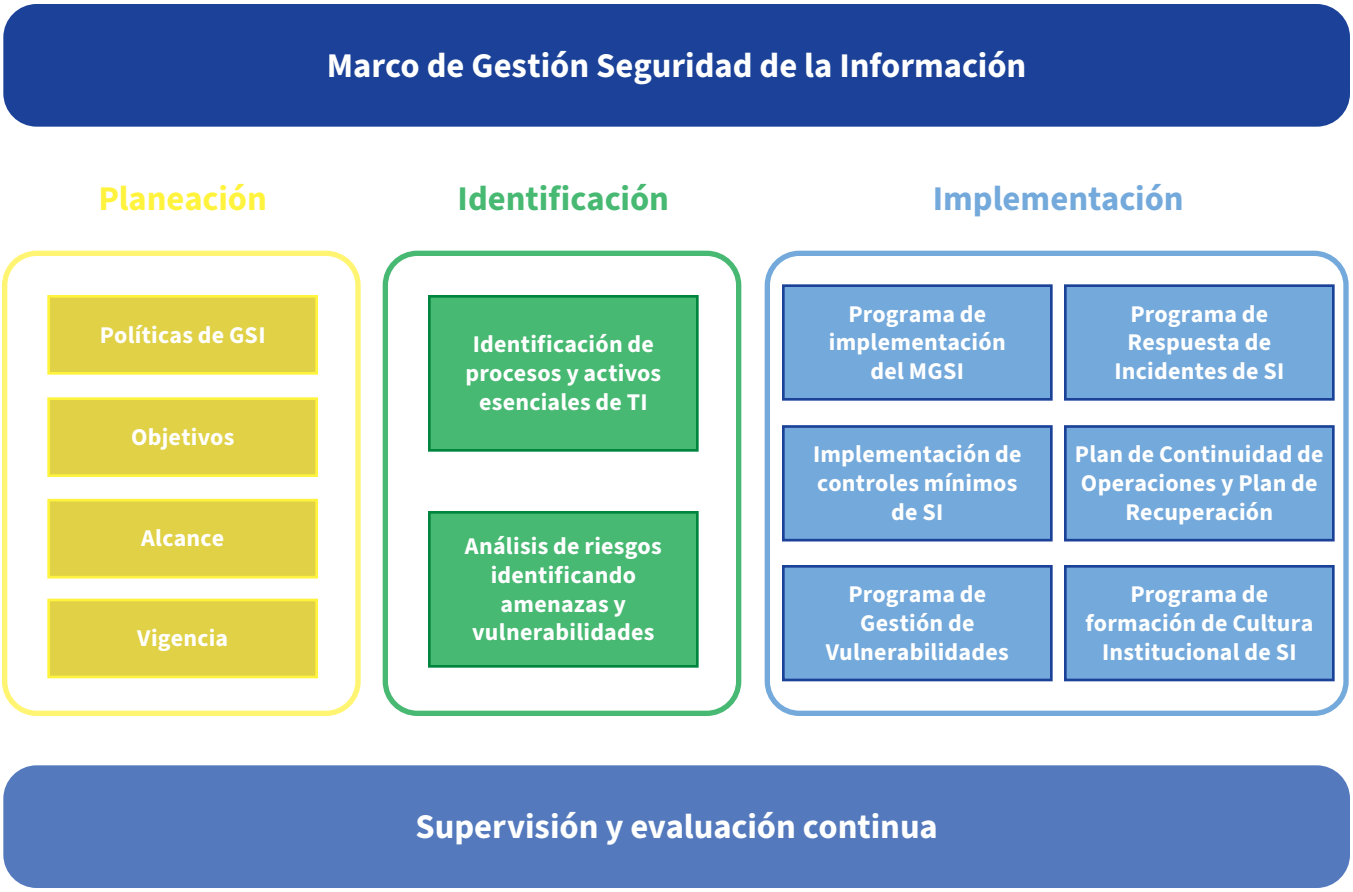
d) Finalmente, en la fase de **Actuar (ACT)**, se llevan a cabo las acciones correctivas y preventivas necesarias en respuesta a los hallazgos y recomendaciones derivadas de la fase anterior. Esto puede implicar la actualización de políticas y procedimientos, la implementación de nuevos controles de seguridad o la mejora de la capacitación del personal.

Con base en lo anteriormente señalado, la OCDE recomienda una ruta integrada por seis pasos[32] fundamentales para que las autoridades fiscales lleven a cabo la implementación del marco GSI. Cabe señalar que esta ruta está diseñada para su implementación en el marco del intercambio de información, por lo que, para efectos del presente documento, se ha adecuado para aplicarse a la totalidad de las actividades de la administración tributaria y -de ser el caso- hacerlo extensivo al intercambio de información, en cualquiera de sus modalidades.

Paso 1. Delimitar el alcance del Marco GSI

La implementación de un Marco GSI para las administraciones tributarias se refiere a la adopción de un conjunto de estrategias, políticas, procedimientos, controles y prácticas para garantizar la protección adecuada de la información fiscal. Este marco proporciona una guía estructurada y sistemática para gestionar los riesgos de seguridad de la información y proteger los activos de datos contra las amenazas internas y externas que pudieran suscitarse.

[32] OECD, Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información, Op Cit., pág. 15.



Fuente: Ejemplo de diseño de Marco GSI

Generalmente, el punto de partida para el diseño del marco GSI es el **ciclo de vida de la información** ya que el conocimiento del ciclo de vida de la información permite gestionar los datos desde que se generan o *entran* en la esfera de competencia de la autoridad hasta su destrucción, una vez que han sido utilizados.

En ese tenor, el ciclo de vida de la información se divide en cinco fases:

a) **Creación de los datos:** Referido a la recopilación de la información que lleva a cabo la autoridad. Dicha información procede de diversas fuentes y puede presentarse en distintos formatos. Idealmente, la autoridad deberá evaluar la calidad y relevancia de la información para determinar su utilidad en el futuro.

b) **Almacenamiento de los datos:** La autoridad deberá considerar la forma en la que los datos están estructurados con el fin de determinar el tipo de almacenamiento que se requerirá. Adicionalmente,

la autoridad evaluará la infraestructura en busca de vulnerabilidades de seguridad y los datos pueden someterse a diferentes tipos de procesamiento (i.e. cifrado y/o transformación de los datos) como medida de protección ante eventualidades y maliciosos. Con ello también se garantiza que se cumplirán los requerimientos normativos en materia de confidencialidad y privacidad de la información.

c) **Uso de la información:** La información se pondrá a disposición de los sujetos autorizados. La administración tributaria deberá establecer normativas y regulaciones para definir los parámetros específicos bajo los cuales se podrá acceder a la información. Este aspecto resulta fundamental ya que deberán indicarse expresamente los supuestos bajo los cuales podrá concederse acceso a otras autoridades (incluso extranjeras, tratándose del intercambio de información) y el público en general. Desde el punto de vista operativo y tecnológico deberán desarrollarse políticas y procedimientos enfocados en garantizar la accesibilidad y disponibilidad de datos limpios y útiles, permitiendo su manejo de manera eficiente y segura.

d) **Archivo de la información:** Las administraciones tributarias deberán garantizar que una vez que los datos han sido utilizados se archivarán de manera adecuada, permitiendo su acceso y restauración en caso de ser requerido (ej. en caso de litigios o investigaciones penales). Las autoridades fiscales, paralelamente, deberán establecer lineamientos que definirán claramente los plazos y términos bajo los cuales se archivará la información.

e) **Eliminación de la información:** Se refiere a la destrucción de manera segura de la información una vez que hayan transcurrido los plazos de retención señalados en el inciso anterior.

Paso 2. Establecimiento de políticas de GSI

Las autoridades fiscales deberán consignar en un documento de política de GSI los lineamientos relativos al marco global de seguridad. De manera general, el marco GSI deberá contar con **objetivos** claramente definidos[33], una política integral que defina el alcance del sistema de GSI y los objetivos generales y refleje el compromiso de la autoridad en la consecución de éstos.

Se considera que una política es *integral* cuando cubre los siguientes ámbitos generales de seguridad: recursos humanos, gestión del acceso, seguridad de las tecnologías de la información, protección de la información y gestión de las operaciones.

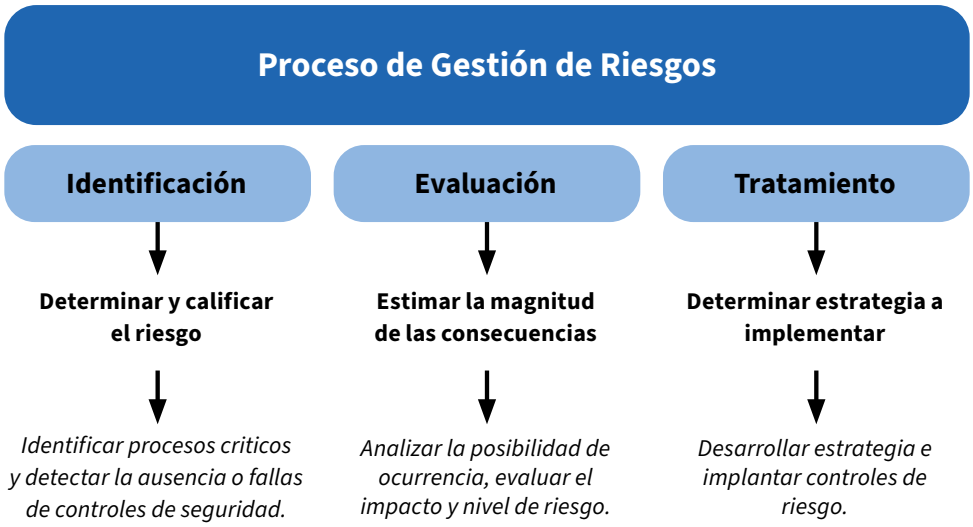
[33] Por ejemplo, proteger la información sensible de conformidad con las normas de confidencialidad y seguridad de la información, mitigar riesgos mediante controles de seguridad, etc.

Adicionalmente, el marco GSI deberá consignar los criterios relativos a seguridad de las tecnologías de la información, seguridad física, seguridad en materia de recursos humanos y continuidad de operaciones, así como delimitar claramente las funciones y responsabilidades del personal a cargo de la seguridad de la información.

En relación con lo anterior, la autoridad fiscal deberá de implementar medidas operativas adecuadas e integradas con las operaciones de negocio. Idealmente, estas medidas se consignarán en un manual o documento similar que compilará las políticas, procesos, procedimientos y controles diseñados para mitigar y/o eliminar los posibles riesgos para la seguridad de la información.

Paso 3. Identificación y gestión de riesgos de seguridad

Es obligatorio que las administraciones tributarias gestionen sistemáticamente los riesgos de la información a que se exponen a través de un proceso riguroso y exhaustivo de gestión de riesgo. Podrá desarrollarse una metodología específica para la gestión del riesgo dentro del sistema de GSI o bien, adecuar la metodología integral de la administración y alinearla a los objetivos GSI y los criterios de seguridad de la información.



Aunado a lo anterior, deberán considerarse seguimientos y revisiones periódicas, criterios de valoración de riesgo (generalmente, medido a través de la evaluación del posible impacto en caso de que se manifieste dicho riesgo), controles de riesgo, opciones de tratamiento, reporte de hallazgos y resultados, etc.

Disposiciones relativas a la gestión de riesgo contenidas en las Políticas GSI. España.

Un ejemplo de cómo pueden incorporarse las políticas generales relativas a la gestión de riesgos se encuentra en la Resolución de 8 de noviembre de 2012 por la que se aprueba la política de seguridad de la información de la Agencia Estatal de Administración Tributaria. En este documento se consignan las políticas generales de GSI que posteriormente se reflejan en manuales, guías y demás documentos internos para aplicación del personal de la Administración Tributaria.

Gestión de riesgos

1. *La gestión de riesgos debe realizarse de manera continua sobre el sistema de información y contemplar un análisis de riesgos avanzado que evalúe los riesgos residuales y proponga tratamientos adecuados.*
2. *La gestión de riesgos sobre el sistema de información estará alineada con la gestión de riesgos establecida en la Agencia Tributaria, centrada en el Mapa de Riesgos de la organización.*
3. *La Comisión de Seguridad y Control de Informática Tributaria, en el ejercicio de sus funciones, se encargará de analizar y evaluar los riesgos de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas.*
4. *Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y en especial las guías elaboradas por el Centro Criptológico Nacional.*

Paso 4. Establecer políticas, procesos y procedimientos específicos para garantizar la continuidad de las operaciones.

Una vez realizados los análisis de riesgos y seleccionados los controles adecuados para su tratamiento, es imperativo que la administración tributaria formalice y documente estos controles en sus políticas, procesos y procedimientos. Este enfoque sistemático asegura que todos los aspectos relacionados con la gestión de riesgos se integren de manera coherente en el marco normativo de la entidad. La documentación debe incluir descripciones claras de los controles aplicables, así como sus objetivos, responsables y la metodología de implementación, garantizando así la trazabilidad y la transparencia en la gestión tributaria.

Asimismo, las administraciones fiscales deberán contar con medidas específicamente diseñadas para gestionar y mantener la continuidad de las operaciones ante la presencia de eventos que alteren su

funcionamiento. Estas medidas garantizan la disponibilidad continua de servicios y aseguran que la autoridad contará con medios suficientes para actuar ante posibles interrupciones causadas no solo por ataques cibernéticos o fallas técnicas sino también por fenómenos naturales o incluso, cuestiones sociales.

Al igual que con la evaluación de riesgos, las autoridades deberán conducir una evaluación para determinar las condiciones en las que se encuentra la administración tributaria para identificar los requerimientos de seguridad que requieren implementarse, adecuarse, modificarse o sustituirse.

Así, el proceso de gestión inicia con la identificación de los posibles escenarios que podrían afectar o alterar operaciones de la administración tributaria, posteriormente se evaluará y documentará el posible impacto de cada escenario. Con base en dicha evaluación, se diseñará un **Plan de Continuidad de Operaciones (PCO)** que incluya criterios de prueba y revisión del plan y la capacitación correspondiente.

El PCO deberá indicar los procesos y procedimientos detallados que deberán ejecutarse para garantizar que la administración tributaria estará en posibilidades de operar correctamente o incluso recuperar o reestablecer su funcionamiento en caso de que se presente la contingencia o perturbación.

Aspectos Relevantes del Plan de Continuidad de Acción del Servicio de Rentas Internas (IRS) de Estados Unidos.

En 2020, el IRS actualizó el Manual de Recaudación Tributaria para incluir nuevas medidas destinadas a hacer frente a los retos derivados de la pandemia de COVID-19.

Algunas de las disposiciones más relevantes son:

- *El IRS debe ser capaz de continuar con el desempeño de sus actividades esenciales durante cualquier emergencia por un período de hasta 30 días o hasta que se puedan reanudar las operaciones normales.*
- *El IRS debe tener la capacidad de estar completamente operativo en sus instalaciones de continuidad tan pronto como sea posible después de la ocurrencia de una emergencia, pero a más tardar 12 horas después de la activación de las operaciones de continuidad.*
- *El IRS debe salvaguardar sus recursos, instalaciones y registros vitales, y proporcionar acceso oficial a ellos. El IRS debe tomar medidas para la contratación y/o asignación del personal y los recursos necesarios para las operaciones de continuidad en caso de emergencia.*
- *El IRS debe tomar medidas para la disponibilidad y redundancia de las capacidades de comunicaciones críticas en los sitios de continuidad con el fin de apoyar la conectividad entre*

el liderazgo clave del gobierno, los elementos organizativos del IRS, otros departamentos y agencias ejecutivas, los socios críticos y el público, así como para la identificación, capacitación y preparación del personal del IRS capaz de reubicarse en las instalaciones designadas como aptas durante la contingencia

- *El IRS debe tomar disposiciones para las capacidades de reconstitución que permitan la recuperación de una emergencia catastrófica y la reanudación de las operaciones normales.*

Un PCO adecuado deberá, por lo menos, contener provisiones relativas a cuestiones tales como: (i) sistemas clave y orden prioritario de funcionamiento, (ii) actividades y servicios esenciales y no esenciales[34], (iii) elaboración de copia(s) de seguridad, (iv) personal esencial para el funcionamiento *básico* de la administración, (v) información crítica (considerando también su formato y la forma de almacenamiento y traslado, de ser el caso), (vi) medidas para el restablecimiento (incluso si éste deberá ser gradual o total, según el tipo de incidente).

La última fase del proceso de gestión de la continuidad de las operaciones se enfoca en la verificación de la efectividad del PCO y la revisión continua a la que deberá someterse. Para tales efectos, pueden realizarse simulacros para evaluar la preparación de la administración fiscal ante las posibles amenazas y contingencias a las que está expuesta.

Paso 5. Formación y capacitación del personal

La formación del personal en GSI es un pilar fundamental para la efectividad de las políticas y procedimientos diseñados para gestionar los riesgos de seguridad. Es crucial que cada miembro de la administración fiscal comprenda a cabalidad no solo las normativas vigentes, sino también la importancia de su aplicación. Esta capacitación debe ser integral y continua, adaptándose a las actualizaciones de las políticas y a las nuevas amenazas que puedan surgir.

[34] La OCDE, en la publicación titulada *Respuesta de las Administraciones Tributarias al COVID-19: Consideraciones acerca dela continuidad de actividades y servicios* define a las actividades *esenciales* como *aquellas funciones en las que el tiempo es un factor crítico cuya indisponibilidad o malfuncionamiento, incluso durante horas, afectaría a los sistemas de continuidad de la actividad de la administración, a personas, edificios y proveedores, dando lugar a un nivel inaceptable de desorganización en su labor e interrupción de sus actividades, al deterioro del servicio a clientes o a daños reputacionales.* Documento disponible en: https://read.oecd-ilibrary.org/view/?ref=133_133006-nruwv5tdpl&title=Respuesta-de-las-administraciones-tributarias-al-COVID-19-Consideraciones-acerca-de-la-continuidad-de-actividades-y-servicios

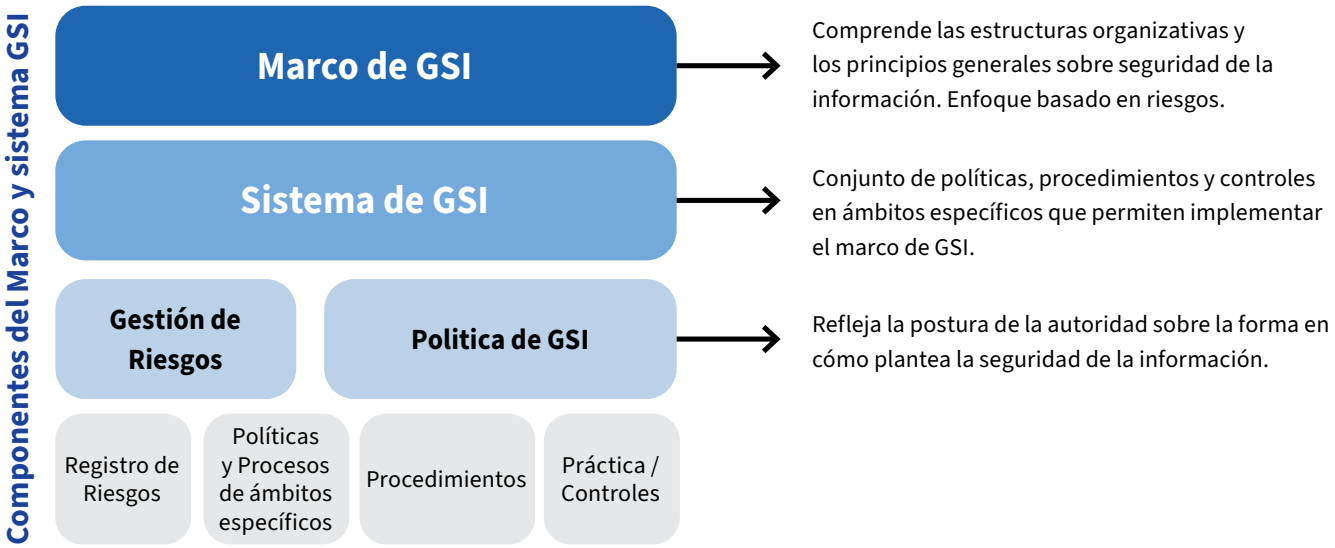
Asimismo, la evaluación constante de la capacitación recibida es fundamental para asegurar su efectividad; por lo tanto, la implementación de mecanismos de retroalimentación y revisión periódica permite identificar áreas de mejora y adaptar el contenido de la capacitación a las necesidades específicas del personal y a las tendencias emergentes en seguridad. Este enfoque dinámico no solo contribuye al desarrollo profesional del equipo, sino que también garantiza que la autoridad fiscal esté, en la medida de lo posible, a la vanguardia en la protección contra riesgos y amenazas tecnológicas, manteniendo un entorno seguro y eficiente.

Paso 6. Verificación de la adopción efectiva del sistema GSI

La administración tributaria debe establecer un programa de verificación periódica que evalúe la efectividad de la aplicación del sistema GSI por parte de su personal. Este programa debe incluir auditorías internas y revisiones de cumplimiento que permitan identificar si las políticas, procesos y procedimientos definidos están siendo implementados de manera uniforme y alineada a las provisiones del propio marco GSI. La sistematización de estas evaluaciones permitirá recoger datos relevantes sobre la adherencia al sistema, facilitando la toma de decisiones informadas para la mejora continua.

Asimismo, deben establecerse mecanismos para dar a conocer los resultados de las auditorías y las acciones correctivas derivadas de estas evaluaciones, con el fin no solo de optimizar la implementación del marco GSI, sino que también reforzar el compromiso institucional con la seguridad y la protección de datos sensibles.

Con base en lo anteriormente descrito, se tiene que el Marco de GSI deberá estar integrado por los siguientes elementos:



En el siguiente capítulo se abordarán diversos aspectos relacionados con la gestión de seguridad de las TIs con el fin de proporcionar a las administraciones tributarias de elementos suficientes para llevar a cabo una implementación eficaz del marco GSI adecuado a sus necesidades y requerimientos.

5. Gestión de seguridad de las tecnologías de información

El marco de gestión de la seguridad de tecnologías de la información (GSTI) se enfoca en la protección de los sistemas de tecnologías de la información que soportan y gestionan la información crítica de la organización; es decir, protege las redes, servidores, aplicaciones y dispositivos que procesan, almacenan y transmiten datos. El objetivo principal del marco STI es asegurar que estos sistemas estén protegidos contra amenazas cibernéticas y operen de manera segura y eficiente.

Como se indicó en el capítulo anterior, el marco GSI se enfoca en asegurar la confidencialidad, integridad y disponibilidad de todos los activos de información críticos de la organización, mientras que el marco GSTI se centra en proteger los sistemas y tecnologías que soportan y gestionan esa información. Esto significa que ambos marcos son complementarios y deben trabajar en conjunto para garantizar una protección integral de los activos de la organización.

Ahora bien, el marco GSTI no se limita únicamente a la mera aplicación de controles técnicos ni a cuestiones exclusivamente de carácter tecnológico. El ámbito de aplicación del marco GSTI se extiende también a los ámbitos organizacionales de la administración tributaria; es decir, la alta dirección debe fomentar y promover una cultura organizacional que dé prioridad a la seguridad a través de la sensibilización y capacitación continua del personal, la asignación de roles y responsabilidades claras y bien definidas y que integre las prácticas y políticas de seguridad a lo largo del ciclo de vida de la información.

De lo anterior se desprende que las administraciones tributarias que requieran implementar un sistema integral de seguridad al interior de su organización deberán establecer un enfoque integral que, además de incorporar las políticas y medidas de protección de la información, implemente controles técnicos y operativos en combinación con la creación de un ambiente cultural que fomente y priorice la seguridad.

¿Cuáles son los requisitos de un Director de Seguridad?

El director de seguridad (Chief Security Officer, CSO por sus siglas en inglés) debe estar altamente cualificado y contar con experiencia específica para desarrollar la estrategia e iniciativas asociadas a la seguridad para proteger los activos, datos e infraestructura de la empresa. Esta persona no solo desarrollará e implementará estrategias de seguridad integrales, Si no que debe tener capacidad para trabajar con equipos interdisciplinarios y así poder identificar riesgos, idear medidas preventivas y asegurar el cumplimiento de las normativas relacionadas con infraestructura y ciberseguridad.

Objetivos de quien desempeñe este rol

- *Desarrollar e implementar un marco de seguridad integral para proteger los activos e infraestructura de la administración tributaria.*
- *Diseñar e implementar políticas, procedimientos y protocolos de seguridad para mitigar riesgos y mantener un entorno seguro.*
- *Investigar y supervisar las actividades de respuesta a incidentes, incluyendo investigaciones, análisis de causas raíz y desarrollo de acciones correctivas.*
- *Colaborar con equipos interdisciplinarios para evaluar riesgos, identificar vulnerabilidades e idear medidas preventivas.*
- *Establecer y mantener relaciones sólidas con partes interesadas externas, como organismos reguladores, agencias de aplicación de la ley y asociaciones de la industria.*
- *Liderar programas de concienciación sobre seguridad e iniciativas de capacitación para educar a los empleados sobre las mejores prácticas y amenazas potenciales.*

Principales tareas

- *Realizar auditorías de seguridad y evaluaciones de riesgos regularmente para identificar vulnerabilidades y asegurar el cumplimiento de las normativas relevantes.*
- *Implementar y gestionar tecnologías de seguridad, como cortafuegos, sistemas de detección de intrusiones y controles de acceso.*
- *Asegurar el cumplimiento de la organización con las leyes, regulaciones y estándares de seguridad aplicables a nivel mundial.*
- *Monitorear sistemas y redes de seguridad en busca de amenazas potenciales, investigando y mitigando incidentes de seguridad de manera oportuna.*
- *Supervisar la gestión de medidas de seguridad física, incluyendo controles de acceso, sistemas de CCTV y personal de seguridad.*

- *Desarrollar y mantener planes de respuesta a incidentes, asegurando respuestas oportunas y efectivas a las violaciones de seguridad.*
- *Gestionar registros, documentación e informes para demostrar el cumplimiento y facilitar auditorías.*
- *Colaborar con equipos internos para integrar consideraciones de seguridad en el desarrollo de nuevos productos y servicios.*
- *Mantenerse actualizado con las últimas tendencias, tecnologías y cambios regulatorios en seguridad, asegurando la mejora continua de la función de seguridad.*

Habilidades y calificaciones esperadas

- *Título universitario en informática, seguridad de la información o un campo relacionado. Máster en ciberseguridad, garantía de la información o un campo relacionado.*
- *Certificaciones relevantes como Certified Information Systems Security Professionals (CISSP), Certified information security manager (CISM) o Certified in Risk and Information Systems Control (CRISC).*
- *Más de 7 años de experiencia en un rol de gestión de seguridad senior, con un historial demostrable en el desarrollo e implementación de estrategias y marcos de seguridad.*
- *Excelente conocimiento de las leyes, regulaciones y estándares de la industria relacionados con la seguridad de infraestructura en una organización.*
- *Profundo entendimiento de ciberseguridad, regulaciones de protección de datos y mejores prácticas de la industria.*
- *Fuertes habilidades de liderazgo y comunicación, con la capacidad de colaborar eficazmente con equipos interdisciplinarios y alta dirección. Capacidad para impulsar el cambio cultural e integrar una cultura consciente de la seguridad dentro de la organización.*
- *Mentalidad analítica y sólidas habilidades de resolución de problemas para evaluar riesgos, analizar problemas complejos de seguridad y desarrollar soluciones adecuadas.*
- *Conocimiento actualizado de amenazas emergentes, tendencias y tecnologías de seguridad.*
- *Experiencia en la realización de auditorías de seguridad, evaluaciones de riesgos y gestión de procesos de respuesta a incidentes.*
- *Dominio del idioma inglés*

En este capítulo se abordarán las principales medidas y mejores prácticas relativas a la implementación efectiva del marco GSTI de manera integral con el objetivo de establecer una infraestructura segura a la par de un clima organizacional confiable al interior de las administraciones tributarias.

5.1. Gestión integral del capital humano

El primer elemento por considerar como parte de la implementación del marco GSTI se refiere a la gestión de los trabajadores y así como de los demás individuos que interactúan con la administración tributaria ya sea a través de un contrato laboral, de suministro o de prestación de servicios.

A partir de lo anterior, resulta relevante distinguir entre los conceptos de *recursos humanos* y *capital humano* y señalar las principales diferencias entre ellos ya que frecuentemente son empleados de manera indistinta como sinónimos.

Los **recursos humanos** pueden definirse como el conjunto de prácticas y procesos y procedimientos administrativos que tienen como objetivo gestionar el recurso humano dentro de una organización. Esto incluye funciones como la contratación, la gestión del desempeño, la administración de compensaciones y beneficios, la formación y desarrollo, entre otros.

En contraste, el **capital humano**, de acuerdo con la OCDE, se define como "la mezcla de aptitudes y habilidades innatas a las personas, así como la calificación y el aprendizaje que adquieren en la educación y la capacitación"[35]. Esta noción resalta, prioritariamente, las capacidades, conocimientos y habilidades de los trabajadores de una organización, lo que implica elevar la noción tradicional de los recursos humanos al integrar todas las funciones relacionadas con el personal en una estrategia cohesiva.

Así, una visión integral del elemento humano como parte de una institución comprende tanto el aspecto netamente personal o individual y el manejo estratégico en función de los objetivos y enfoques de la propia institución. A tales efectos, entonces, la gestión integral del capital humano abarca, en primera instancia, la administración general del personal que labora en la organización, el desarrollo personal (junto con la inversión que ello conlleva) en conjunción con la filosofía o políticas que rijan la gestión específica de la administración y la aportación que el personal realiza al manejo estratégico general de la organización.[36]

---

[35] OECD, *Perspectivas de la OCDE. Capital Humano: Cómo moldea tu vida lo que sabes. Resumen en español.,* OECD Publishing, Paris, 2007. Pág. 2. Documento disponible en https://www.oecd-ilibrary.org/docserver/9789264029095-sum-es.pdf?expires=1721158015&id=id&accname=guest&checksum=0B33A3E116BBA88CA0AA16B137FEB6E9

[36] Rüdiger Pieper (editor), *Human Resource Management: An international comparison.*, Ed. De Gruyter, Berlín, 1990. Publicación disponible en: Human Resource Management: An International Comparison – Google Libros

En línea con lo anterior, es válido señalar que la gestión del capital humano implica cuestiones que van más allá de la asignación de roles y responsabilidades, ya que considera a los empleados como elementos fundamentales para la consecución de los objetivos de la organización y, por lo tanto, resulta esencial incorporar mecanismos que favorezcan y estimulen el crecimiento de sus competencias.

Así, la Gestión de Recursos Humanos (GRH) consiste en el "diseño e implementación de tareas tales como el reclutamiento y la selección del personal, la gestión de la compensación, la gestión del desempeño y la capacitación"[37]. Mediante dicha gestión, se establecerán los parámetros que la organización requiere para garantizar la eficiencia operativa y salvaguardar la información confidencial en poder de las administraciones tributarias.

Ahora bien, en el caso de las administraciones tributarias, la gestión efectiva del capital humano cobra mayor relevancia en el contexto de la implementación efectiva del marco GSTI debido a la naturaleza técnica y altamente especializada de las funciones que sus empleados desempeñan. Los funcionarios públicos no solo deben poseer conocimientos sólidos en normativa fiscal sino también en tecnologías y seguridad de la información y el uso ético de la información que obra en su poder. Atendiendo a ello, la selección y capacitación de los empleados y la implementación de medidas de control y seguridad durante todo el ciclo de vida del personal son elementos esenciales que garantizan la efectividad operativa de la administración tributaria.

Adicionalmente, las administraciones tributarias deberán hacer extensivas ciertas medidas de seguridad y control a individuos que tengan una relación laboral o contractual distinta de aquella de los empleados *regulares* o *permanentes,* tal es el caso de los empleados temporales o de los contratistas externos.

En las siguientes secciones se abordarán de manera específica las reglas y medios de control más apropiados para implementar de manera eficaz el marco GSTI.

El ciclo de vida del personal

De manera general, el ciclo de vida laboral se refiere al conjunto de etapas o fases por las que atraviesa un empleado desde su reclutamiento y contratación hasta su salida de la organización. Este ciclo puede variar en detalle según las políticas y prácticas específicas de cada organización o abarcar distintas etapas de la relación laboral.

[37] OECD, *Panorama de las Administraciones Públicas América Latina y el Caribe 2020*, OECD Publishing, Paris, 2020, pág. 110. Documento disponible en: https://doi.org/10.1787/1256b68d-es

Sin embargo, puede establecerse que el ciclo de vida laboral se divide -de manera general- en tres grandes fases:

a) **Reclutamiento y Contratación:** Implica la búsqueda proactiva de talento para incorporar a la organización una vez que éstos acreditan tener los conocimientos y habilidades necesarios para cubrir una vacante. Como parte del proceso, se aplicarán distintos filtros, tales como entrevistas, evaluaciones, revisión de antecedentes, entre otros. La fase finaliza una vez que la oferta de empleo es aceptada por el candidato y se formaliza con la firma del contrato laboral.

b) **Capacitación y Desarrollo Profesional:** Inicia con la fase de inducción, en la cual el empleado recibirá capacitación con el fin de que adquiera los conocimientos necesarios para integrarse adecuadamente a la organización. La capacitación es la fase posterior en la cual se dota al empleado de conocimientos técnicos, teóricos y prácticos con el objetivo de optimizar su desempeño al mejorar e incrementar sus competencias y habilidades.

c) **Desvinculación Laboral:** Se da cuando la relación laboral se extingue de forma voluntaria por el empleado, el empleador o ambos (ya sea por renuncia o jubilación, por ejemplo) o bien, de forma involuntaria (a través de un despido, destitución, etc.). Esta desvinculación requiere llevarse a cabo de manera estructurada a través de un proceso que contemple medidas enfocadas en salvaguardar la seguridad y confidencialidad de la información ante la salida de un empleado.

Desde la contratación hasta la terminación de la relación laboral, cada fase requiere que las administraciones tributarias establezcan medidas rigurosas para mitigar los riesgos asociados con las potenciales violaciones de datos y las infracciones que los funcionarios pudieran cometer. Al implementar protocolos de seguridad sólidos y adherirse a requisitos regulatorios estrictos, las administraciones tributarias pueden mantener la confianza pública y cumplir su papel vital en la gobernanza fiscal.

Implementación de controles de capital humano

De manera general, los controles de los recursos humanos se definen como las “políticas y procedimientos jurídicos y administrativos aplicables a la gestión de los recursos humanos de la administración tributaria (por lo general, personal propio y contratistas), con vistas a garantizar que respetan y protegen la confidencialidad de la información tributaria”[38].

En esta sección se abordarán brevemente las medidas de control que se recomienda implementar en cada fase del ciclo de vida laboral.

[38] OECD, *Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información,* Op Cit., pág. 29.

Controles durante la fase de contratación

Específicamente, estos controles se refieren a las verificaciones y pruebas que efectuará la administración fiscal tendientes a garantizar la confidencialidad de los candidatos (y potenciales empleados) respecto del manejo de la información confidencial. Tales medidas incluyen la transmisión al candidato de información relativa a la importancia de la seguridad y la confidencialidad de la información (regularmente durante el momento de la entrevista), la aplicación de procesos de verificación de antecedentes penales, financieros y cualquier otro tipo de investigación más profunda que la administración fiscal requiera ejecutar atendiendo al tipo de puesto que se esté ofertando.

Cabe resaltar que estas verificaciones deberán actualizarse o reaplicarse periódicamente a lo largo de la relación laboral; tratándose de contratistas externos y proveedores la administración fiscal deberá realizar también dichas comprobaciones y verificaciones adecuándolas a la naturaleza de las funciones, actividades o labores que desempeñarán tales contratistas y proveedores.

En cualquier caso, las administraciones fiscales están obligadas a informar a los candidatos, empleados recién contratados, contratistas y proveedores respecto de las funciones, obligaciones, responsabilidades y sanciones aplicables en materia de confidencialidad y seguridad de la información.

Controles relativos a la relación de trabajo

Se recomienda que la administración fiscal implemente campañas continuas de formación y sensibilización a los trabajadores en materia de seguridad y confidencialidad de la información. La *formación* se refiere a la adquisición y desarrollo de conocimientos, capacidades y competencias para incorporar la confidencialidad y seguridad a los procesos tributarios, mientras que la *sensibilización* comunica al personal sobre los riesgos y amenazas en materia de seguridad.[39]

Controles relativos al término de la relación de trabajo

Se refieren a las políticas y procesos aplicables cuando se concluye la relación laboral con el fin de proteger la información sensible. El objetivo es garantizar que la confidencialidad de la información se mantendrá aún después de la extinción de la relación laboral.

[39] Ibidem, pág. 35.

Entre las medidas de control aplicables más importantes se encuentran:

a) *Recuperación de bienes oficiales:* El empleado deberá devolver las identificaciones, equipo informático, telefónico y cualquier otro dispositivo similar que se le hubiera proporcionado al trabajador para el desempeño de sus funciones.

b) *Supresión de derechos:* Con el fin de preservar la seguridad y confidencialidad de la información, se deberán revocar todos los permisos de acceso (físicos y lógicos) que se le hayan concedido al trabajador. Este punto se abordará con mayor detalle en el siguiente apartado.

5.2. Control de acceso

El principio fundamental que rige las políticas de control de acceso enfocadas específicamente en la seguridad y la confidencialidad de la información es el **principio de necesidad de saber.** Este principio implica que solo los usuarios que tengan una razón legítima[40] para acceder a la información en poder de las autoridades fiscales. En estrecha conexión con ello, el **principio de mínimo privilegio**. La diferencia entre ambos radica en que el primero de éstos se dirige a las personas a las que se les autorizará ver cierta información confidencial, mientras que el segundo se refiere a los derechos de acceso privilegiado de los usuarios y las cuentas respectivas. La adopción de estos principios requerirá forzosamente la aplicación de controles de los derechos de acceso de los usuarios y la gestión de las cuentas asignadas a éstos.

Atendiendo a lo anterior, es necesario que la administración tributaria defina claramente los roles y responsabilidades, así como los tipos de usuarios a los que se les concederán los derechos mínimos de acceso a los datos.

En ese contexto, el tipo de usuarios a los que, potencialmente, se le concederá acceso a la información en posesión de las autoridades fiscales atiende al rol y nivel de acceso a la información que se otorgará. En tal virtud, los tipos de usuarios generalmente incluyen usuarios finales, administradores de sistemas y personal de auditoría. Los usuarios finales son aquellos que interactúan directamente con los sistemas de información en sus actividades diarias, mientras que los administradores de sistemas son responsables de la configuración, mantenimiento y seguridad de las plataformas tecnológicas. Por otro lado, el personal de auditoría se encarga de evaluar el cumplimiento de las políticas de seguridad y la efectividad de los controles establecidos.

[40] Generalmente, la razón legítima está directamente vinculada al rol y responsabilidades que la función laboral requiera y específique.

Diseño e Implementación de Políticas Generales de Seguridad de la Información. México.

El Servicio de Administración Tributaria (SAT) publicó el documento que concentra los requerimientos para la adecuada implementación de las políticas de seguridad de la información.

Política General de Seguridad de la Información.

Objetivo: *Asegurar que todo el personal de la organización y terceros, actúen y tomen decisiones en apego a los criterios y definiciones de la organización respecto a seguridad de información, además de asegurar el compromiso íntegro y participación activa de la alta dirección con la seguridad de la información.*

Diseño:

1. *Debe existir una Política General de Seguridad de la Información formalmente documentada.*
2. *Debe estar firmada de manera autógrafa o mediante e-firma, por la dirección general, representante o apoderado legal.*
3. *Debe incluir un apartado que describa el compromiso y participación activa de la dirección general con respecto a la seguridad de la información.*
4. *Debe incluir la definición de la seguridad de la información, es decir, como la organización concibe el concepto de la seguridad de la información.*
5. *Debe incluir referencias a la normatividad, legislación vigente y marcos de trabajo aplicables a la organización respecto a la seguridad de la información.*
6. *Debe incluir los objetivos de seguridad de la información de la organización.*

   (a) Deben estar alineados con la estrategia de la organización (b) Deben considerar la protección de datos personales e información de los contribuyentes y, (c) Deben considerar el cumplimiento normativo y regulatorio.
7. *Debe incluir los roles y responsabilidades de la seguridad de la información y elementos tales como:*

   (a) Matriz de asignación de responsabilidades RACI u (b) Organigrama con descripción de funciones o, (c) Perfiles de puestos con detalle de actividades, y (d) Medidas disciplinarias, sanciones y/o penalizaciones, en caso de incumplimientos a la política.
8. *Debe incluir lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información tanto para personal interno como para personal ajeno a la organización.*
9. *Debe tener una sección para control de cambios y versiones de la política con fecha, participantes y control de cambios.*
10. *Debe definir una periodicidad de revisión de la política, al menos cada 12 meses.*

Ahora bien, las medidas de control que las administraciones tributarias deberán implementar para proteger la integridad, confidencialidad y disponibilidad de la información sensible que manejan pueden clasificarse en dos categorías: controles de acceso físico y de acceso lógico, ambas categorías se explican más adelante.

Para efectos del diseño e implementación de las políticas que rigen la asignación de controles de acceso físico y lógico, las autoridades fiscales deberán llevar a cabo, cuando menos, una **evaluación de riesgos y amenazas** mediante la cual la autoridad analice de manera exhaustiva respecto de los riesgos y amenazas a los que se enfrenta, ello incluye identificar los activos críticos que necesitan protección, como instalaciones, centros de datos, servidores, equipos de red, sistemas y aplicativos, entre otros recursos. La evaluación de riesgos ayudará a la autoridad a priorizar cuáles y en qué términos se implementarán los controles de seguridad.

A tales efectos, la administración fiscal deberá establecer diversos **criterios de asignación, modificación y revocación de derechos de acceso.** La autoridad deberá -en primera instancia- determinar si los derechos y controles de acceso se otorgarán con base en los roles de cada usuario o bien si se otorgarán de manera discrecional.

Un enfoque que puede resultar de utilidad al momento de definir los criterios con base en los cuales podrán otorgarse los accesos a la información es el presentado por el CIAT en el documento titulado “Las TIC como Herramienta Estratégica para Potenciar la Eficiencia de las Administraciones Tributarias”[41] en el cual se recomienda la implementación de tres niveles de seguridad:

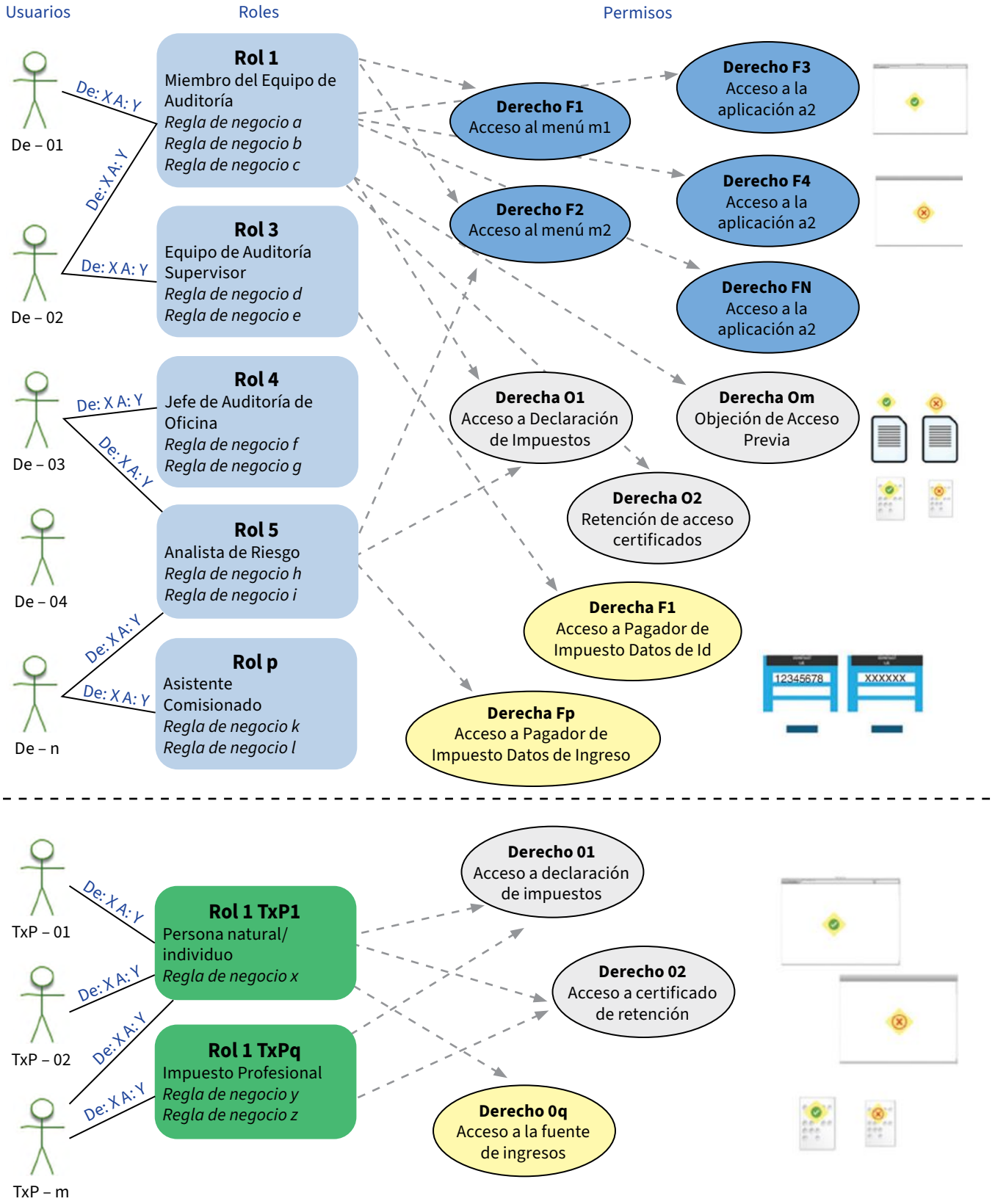
a) **Nivel funcional:** Este permiso otorgaría acceso a las partes funcionales del sistema, limitando el acceso solo a determinados usuarios.

b) **Nivel de los objetos:** Tipo de acceso limitado exclusivamente a cierto tipo de objetos por un tiempo determinado o para la realización de una tarea específica, como por ejemplo una auditoría.

c) **Nivel de campo:** Permite el acceso a campos específicos de un objeto.

En el siguiente esquema se ejemplifica un marco de seguridad dentro de un sistema de información en el cual los accesos se otorgan permisos en atención a roles específicos y por periodos de tiempo limitados.

[41] CIAT, *Las TIC como Herramienta Estratégica para Potenciar la Eficiencia de las Administraciones Tributarias,* Panamá, 2020, págs. 352-353. Documento completo disponible en: https://www.ciat.org/Biblioteca/Estudios/2020_TIC-CIAT-FBMG.pdf



Fuente: CIAT (2020)

Posteriormente, deberán diseñarse políticas específicas que establezcan los criterios básicos aplicables para supuestos tales como la contratación de nuevo personal, cambio, aumento o reducción de funciones, retiro provisional o definitivo de los empleados, accesos temporales o reducidos, privilegios y restricciones, bloqueos, eliminación de accesos, entre otros.

Adicionalmente, la administración deberá establecer procesos para la revisión y comprobación de la vigencia de los controles asignados; esto significa que deberán ejecutarse donde se compruebe, periódicamente que los titulares de los derechos de acceso son efectivamente usuarios legítimos y actuales por lo que resulta indispensable o necesario que continúe teniendo derecho de contar con tales accesos.

Controles de acceso físico

Se refieren a las medidas diseñadas para proteger el acceso físico a las instalaciones, equipos y recursos de la administración tributaria. Estas medidas deben "articularse a través de una o varias políticas de seguridad física avaladas por la alta dirección. Estas políticas deben incluir un conjunto estructurado de controles de seguridad física que deben aplicarse dentro de la administración tributaria. Para garantizar que estos controles cumplan los estándares de buenas prácticas, deben estar basados en riesgos y vinculados a prácticas, deben estar basados en riesgos y vinculados a las consideraciones de diseño físico y requerimientos de los usuarios"[42].

Ahora bien, entre las medidas más frecuentemente implementadas por las administraciones tributarias se encuentran:

a) **Restricción física** del ingreso a áreas específicas al interior de las instalaciones de la administración fiscal mediante la utilización de cerraduras electrónicas o físicas en puertas y accesos.

b) Incorporación de carnés o tarjetas de identificación, **tarjetas de acceso** o dispositivos electrónicos similares que permitirán el acceso a áreas restringidas al personal expresamente autorizado.

c) Instalación de **sistemas de seguridad y videovigilancia** para monitorear áreas sensibles y detectar intrusiones.

d) **Accesos biométricos** (lectores de huellas digitales, reconocimiento facial u otros) como medida de verificación de la identidad de los individuos antes de permitirles el acceso físico a las instalaciones de la administración tributaria.

[42] OECD, Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información, Op Cit., págs. 40-41.

Controles de acceso lógico

Al igual que los controles de acceso físico, los controles de acceso lógico están sustentados en los principios de necesidad de saber y de mínimo privilegio. Sin embargo, estos controles se basan en la implementación de medidas de seguridad diseñadas para proteger los sistemas informáticos, aplicaciones y datos electrónicos contra el acceso no autorizado. El otorgamiento efectivo de acceso permitirá que el personal de la administración tributaria adquiera oportunamente los derechos legítimos que necesitan para desempeñar sus tareas.

Tomando en consideración que los datos podrán resguardarse en diferentes lugares (centros de datos en las instalaciones físicas de la administración tributaria o en áreas externas o en la nube o incluso en entornos fuera del ambiente laboral) los controles de acceso lógico deberán adecuarse a dichas circunstancias.

La administración deberá, además, implementar procedimientos relativos a:

a) **Identificación de usuarios:** Medidas enfocadas en corroborar cuáles son los usuarios que legítima y válidamente disponen de un derecho de acceso.

b) **Autenticación:** Confirmación irrefutable de la identidad del usuario una vez que accede a los sistemas informáticos de la administración tributaria.

c) **Autorización:** Después de la autenticación, el usuario estará autorizado a acceder a los recursos, bajo las limitantes previstas por los principios de necesidad de saber y mínimo privilegio.

d) **Gestiones secundarias:** gestión de contraseñas, sesiones, identificación de cuentas activas e inactivas, entre otras.

5.3. Seguridad de la infraestructura tecnológica

Esta etapa del marco GSTI se refiere a la integración de la seguridad en la TI y la alineación de ésta al negocio; para ello se requiere, en primer lugar, que la administración tributaria establezca una unidad o departamento enfocado en la gestión de las TI's y su correcta integración a los procesos de la administración tributaria.

A tales efectos, las administraciones tributarias deberán implementar medidas enfocadas en integrar la seguridad como parte de la prestación de servicios a través de la implantación de controles adecuados de seguridad y la gestión efectiva de sus activos de TI y la prestación de servicios por parte de sus proveedores y garanticen la continuidad de servicios de TI y su resiliencia ante fallos.

Implementación normativa de la Unidad de Gestión de Tecnologías de la Información en la Administración Tributaria. Costa Rica.

Estructura Organizacional de la Dirección de Tecnología de Información y Comunicación No. 37859-H

Artículo 4º – *Para el cumplimiento de su objetivo la Dirección de Tecnologías de Información y Comunicación, queda conformad por:*

Dirección, que incluye la Dirección, la Subdirección y un Pool Secretarial.
Departamento de Infraestructura de TIC.
Departamento de Sistemas de Información.
Departamento de Servicios de TIC.
Departamento de Control y Aseguramiento de TIC.
Unidad de Estrategia de TIC.
Unidad de Administración de Proyectos de TIC.

Artículo 7º – *Para cumplir sus funciones, el Departamento de Infraestructura TIC estará conformado por cinco unidades:*

Gestión de Redes y Comunicaciones
Administración de Servidores
Administración de Micros
Gestión de Operaciones de TIC.
Administración de Base de Datos.

Artículo 8º- *Objetivo: Brindar una plataforma tecnológica actualizada y robusta, que permita garantizar la eficiencia, disponibilidad y continuidad de los servicios de Tecnologías de Información y Comunicación.*

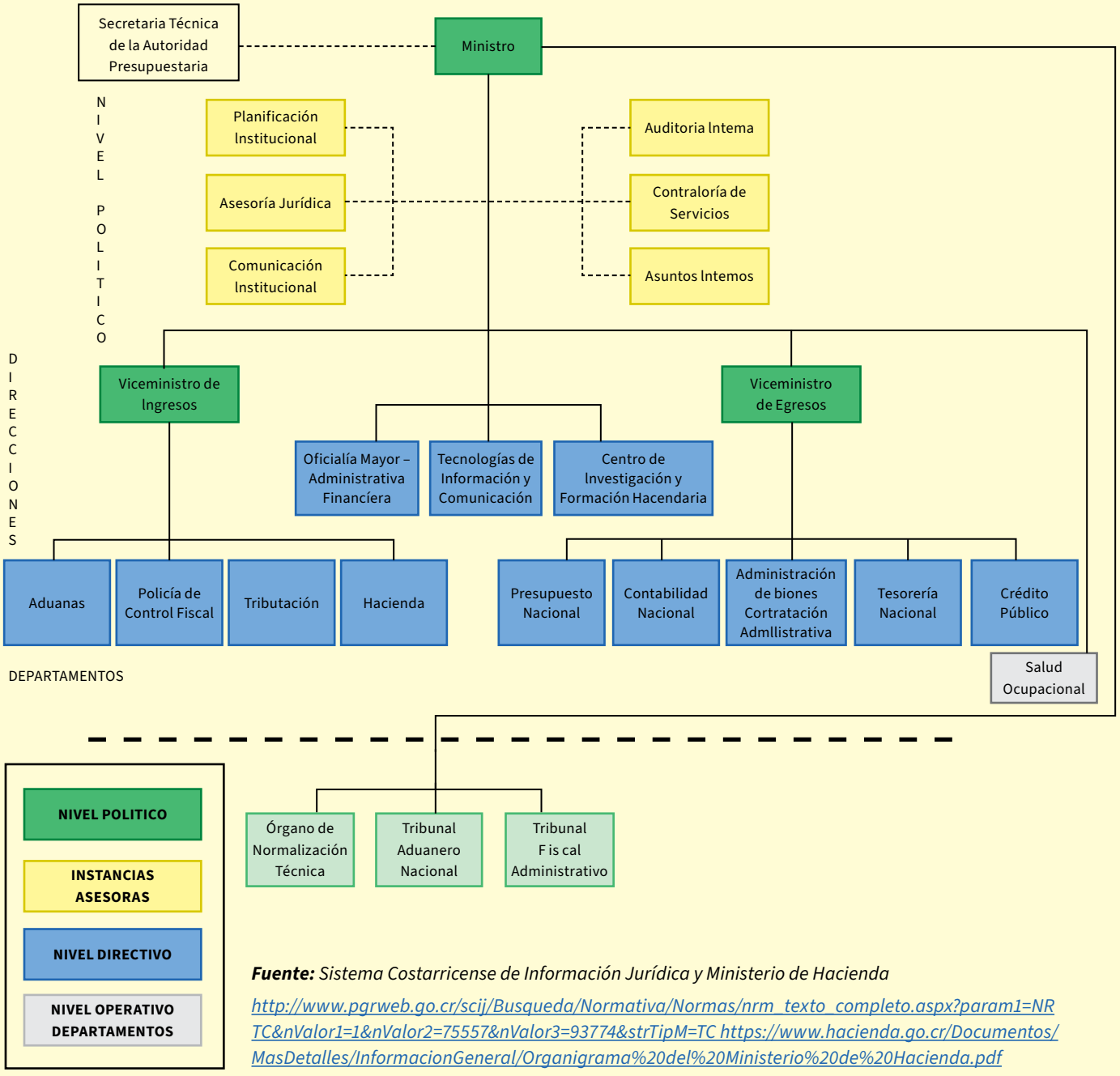
Artículo 9º – *Para el cumplimiento de su objetivo el Departamento de Infraestructura de TIC tendrá las siguientes funciones:*

Proponer a la dirección las políticas, procedimientos y métodos relacionados a la administración de la infraestructura.
Garantizar una plataforma tecnología actualizada y robusta, que soporte la disponibilidad y continuidad de los servicios de TIC.
Realizar estudios e investigaciones en materia de infraestructura, para la implementación de nuevas soluciones que fortalezcan la misma.
Asesorar a las distintas instancias a nivel interno y externo de la Institución, sobre aspectos de infraestructura tecnológica.
Suministrar los insumos para crear y mantener un modelo de información de TIC, por medio de una arquitectura de TIC sólida y actualizada.

Remitir informes a la Dirección según su ámbito de competencia.

Cumplir con las disposiciones de Control Interno establecidas por la Dirección de Tecnología de Información y Comunicaciones.

A continuación, se muestra el organigrama del Ministerio de Hacienda de Costa Rica



Fuente: *Sistema Costarricense de Información Jurídica y Ministerio de Hacienda*

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=75557&nValor3=93774&strTipM=TC https://www.hacienda.go.cr/Documentos/MasDetalles/InformacionGeneral/Organigrama%20del%20Ministerio%20de%20Hacienda.pdf

Implementación de controles de seguridad

Ahora bien, en relación con la implantación de controles adecuados de seguridad, es necesario que la administración lleve a cabo una evaluación de riesgos en la que se determinen los riesgos específicos a los que se enfrenta la administración y se identifiquen, igualmente, los riesgos residuales de la administración.

Con base en los resultados de las evaluaciones antes mencionadas, la administración determinará el tipo de controles que requerirá implementar; estos se clasifican en tres categorías (básicos, adicionales y reforzados) y pueden implementarse a través de medida administrativas (políticas, procesos), físicas (vallas, sistemas de iluminación) o técnicas (firewalls, software), como se describe a continuación:

Controles de Seguridad de TI[43]		
Controles Básicos	**Controles Adicionales**	**Controles Reforzados**
Controles mínimos indispensables aplicados como consecuencia de la identificación de riesgos específicos que lleve a cabo la administración fiscal, **independientemente de su gravedad**.	Medidas adicionales a los controles básicos implantadas para mitigar los riesgos identificados, con base en el nivel de gravedad que se les asigne. El tipo de medida de control que se adopte se determinará **en función de la tolerancia al** **riesgo** que la administración tributaria posea.	Controles que ayudan a hacer **frente a amenazas avanzadas**, tales como tecnologías para detectar y prevenir la exfiltración de datos.
Antivirus, registros, CCTV, políticas de contraseñas.	Autenticación multifactorial, trampas, políticas de formación y sensibilización.	Sistemas de prevención de pérdida de datos, centros de datos, políticas de cifrado.

Una vez implementados los controles adecuados, es recomendable que la administración tributaria lleve a cabo pruebas para medir su eficacia y detectar oportunamente los ajustes y modificaciones que se requieran con el fin de preservar la seguridad de sus procesos. Entre las medidas que pueden adoptarse para evaluar la eficacia de los controles se encuentran los indicadores clave de rendimiento, las pruebas de penetración, las evaluaciones de las vulnerabilidades o las pruebas con conjuntos de datos.

[43] Ibidem, págs. 51-52.

Gestiones secundarias

a) Gestión de activos y servicios: Se refiere al seguimiento y control de todos los activos de TI (hardware/ software) con el objeto de optimizar su uso garantizando su disponibilidad y seguridad.

En cuanto a los servicios, el objetivo es alinearlos con los objetivos del Gobierno, mejorar la eficiencia y efectividad de los servicios que realiza la administración.

Con la implementación adecuada de este marco de gestión se reducirán potencialmente los costos al eficientar el uso de licencias y otros activos, aumentar la transparencia y control, optimizar y eficientar los servicios de TI.

b) **Gestión del nivel de servicio:** "Se refiere a las relaciones globales entre las divisiones del negocio tributario que requieren servicios de TI y las entidades con la responsabilidad general de prestar dichos servicios de TI"[44].

La gestión del nivel de servicio comprende dos tipos de instrumentos:

- *Acuerdos de nivel operativo:* acuerdos internos aplicables cuando el servicio depende de otro departamento para funcionar correctamente.
- *Contratos Marco:* Aplicable en caso de que los servicios de TI dependan de los servicios prestados por un contratista.

c) Gestión de la prestación del servicio por el proveedor: Aplicable con el objeto de garantizar la seguridad de los procesos de la administración con el uso de la subcontratación y cadenas de suministro con sus proveedores.

Entre las medidas recomendadas se encuentran la evaluación y selección cuidadosa de los proveedores, aplicación de cláusulas sobre seguridad apropiadas, implementación de mecanismos de monitoreo y auditoría periódica para supervisar las prácticas de seguridad de los proveedores, evaluación y medición de capacidad de respuesta y la resiliencia ante posibles amenazas, etc.

5.4. Protección de la información

Esta etapa se refiere a la implementación de diversas medidas enfocadas en proteger la información en poder de las administraciones fiscales; generalmente se aplicarán controles específicos atendiendo a la fase del ciclo de la información en que ésta se encuentre y la clasificación que la autoridad le asigne.

[44] Ibidem, pág. 56.

Con base en lo anterior, la administración tributaria deberá identificar los tipos de información que tienen en su poder y a partir de ello aplicarán medidas de control y gestión materializadas en políticas.

Una clasificación comúnmente utilizada es la siguiente:

Criterios aplicables relativos al ciclo de vida de la información[45]	
Identificación y clasificación de la información	**Ejemplos de clasificación:** • *Sensibilidad:* Información pública, interna, reservada y confidencial. • *Restricción:* Principio de necesidad de saber enfocado en el tipo de usuario al que se le concederá el acceso. • *Impacto de la información:* En caso de que se vulnerara la seguridad, se evaluará el impacto que dicha violación tendría en la administración tributaria.
Controles durante el uso de la información	**Tipo de información:** • *Tipo de Información:* Física (impresa) o digital. • *Uso:* En reposo (almacenada) o en uso. **Restricciones aplicables:** • Restricciones al acceso, cifrado de la información, restricciones a la impresión, a la transmisión y al almacenaje.
Controles aplicables para información que ya no es necesaria	Destrucción como medida de seguridad ante amenazas. Establecimiento de periodos precisos de retención y conservación y diseño de políticas específicas.

El conocimiento del ciclo de vida de la información permite a la autoridad fiscal identificar los riesgos y amenazas específicas a que se expone la información. A partir de ello es que se pueden implementar controles adecuados a cada etapa del ciclo de vida previniendo o mitigando riesgos tales como filtraciones, accesos no autorizados y evitando brechas que resulten en la pérdida de información o afectación a la privacidad y seguridad de la información en poder de la autoridad fiscal.

[45] Ibidem, págs. 51-52.

5.5. Gestión de las operaciones

Esta fase del ciclo se centra en los acuerdos operativos que las administraciones tributarias utilizan para verificar que el sistema GSI y sus controles están funcionando. Para tales efectos, se requiere implementar controles adicionales aplicables en distintos ámbitos de la gestión operativa. Entre los más importantes se encuentran:

Gestión de registros

Un punto medular en la implementación del marco GSI es la adopción de medidas, prácticas y políticas enfocadas en asegurar que la información y los sistemas están adecuadamente protegidos a lo largo de todo su ciclo de vida.

En este sentido, la implementación de procedimientos para la creación, almacenamiento, acceso y eliminación de registros de acuerdo con las normas de seguridad y confidencialidad deberá en todo momento estar alineada con las políticas integrales de la administración tributaria y, además, requiere la aplicación de tecnologías y herramientas que permitan la automatización de la gestión de tales registros, incluyendo la captura, clasificación, almacenamiento y recuperación de información.

Asimismo, es necesario que la administración tributaria implemente sistemas de gestión de registros que sean interoperables con otras herramientas y los sistemas de seguridad de la información que ya existan al interior de la organización.

Los registros pueden clasificarse en tres grandes categorías:

a) **Registros de seguridad**: Estos registros son esenciales para la auditoría y análisis de eventos relacionados con la seguridad de la información. Documentan actividades relacionadas con mecanismos de autenticación, control de acceso y eventos de seguridad potenciales. Su propósito es facilitar la identificación de intentos de acceso no autorizado, patrones inusuales de comportamiento del usuario y posibles incidentes de seguridad, permitiendo la detección y respuesta oportuna ante amenazas y vulnerabilidades.

b) **Registros de aplicaciones:** Diseñados para capturar eventos y actividades específicas a nivel de aplicación. Incluyen información detallada sobre interacciones de los usuarios, errores, advertencias y métricas de rendimiento. Estos registros son fundamentales para la resolución de problemas y el diagnóstico de anomalías operativas dentro de las aplicaciones, proporcionando datos críticos para la optimización del rendimiento y la identificación de fallos funcionales.

c) **Registros del Sistema:** Proporcionan una visión detallada de la operación del sistema operativo y sus componentes subyacentes. Incluyen datos sobre configuraciones del sistema, utilización de recursos y eventos de hardware. Estos registros son cruciales para el monitoreo continuo de la salud y el rendimiento de los sistemas de la administración tributaria, permitiendo la detección proactiva de problemas de infraestructura y facilitando la gestión eficiente de los recursos del sistema.

De manera general, la gestión de registros resulta un componente importante en la implementación del marco GSI ya que resultan útiles para coadyuvar en la identificación de incidentes de seguridad, infracciones de políticas, actividades fraudulentas y para proporcionar información que pudiera resultar trascendente para la atención oportuna de incidencias.

Asimismo, los registros también proporcionarán información que será útil para realizar auditorías y análisis forenses, apoyando las investigaciones internas de la administración, establecer líneas de base e identificar tendencias operativas y problemas a largo plazo.

Gestión de vulnerabilidades

La gestión de vulnerabilidades es una práctica fundamental para garantizar la seguridad de los sistemas, herramientas y aplicativos de la administración tributaria que implica la identificación, evaluación, tratamiento y monitoreo constante de vulnerabilidades que pueden ser aprovechadas por amenazas externas o internas y su objetivo es reducir los riesgos asociados a estas vulnerabilidades, asegurando la protección de los activos de información de la organización.

La gestión de vulnerabilidades debe ser un proceso continuo e intrínsecamente integrado en la cultura organizacional. Esto implica la repetición sistemática del proceso para garantizar que se adapte a las dinámicas cambiantes del entorno de TI que asegura una postura proactiva en la protección de sus sistemas y datos contra potenciales ataques y exposiciones, facilitando una adaptación ágil a las amenazas y mitigaciones emergentes.

Una de las medidas más comúnmente implementadas como integrantes del marco de gestión de vulnerabilidades es la **prueba de penetración** (*pentest*) que consiste, a grandes rasgos, en la aplicación de pruebas de seguridad que lanzan ataques cibernéticos simulados con el único objetivo de encontrar vulnerabilidades en los sistemas de la administración tributaria.

Una vez ejecutadas estas pruebas, la autoridad fiscal deberá documentar las vulnerabilidades explotables que afecten la seguridad y confidencialidad de la información para efectuar una investigación y análisis que le permita, posteriormente, emitir recomendaciones para mitigación, sugerir procedimientos que ayuden a

minimizar el impacto o definir acciones correctivas que eliminen las fallas detectadas y finalmente, se verifique su efectividad al repetir la prueba de penetración o mediante la ejecución de medidas de seguimiento.

Gestión de incidentes

La administración tributaria deberá diseñar e implementar procesos de gestión de identificación y atención de incidentes que se ejecute de manera regular y eficaz. Lo anterior implica que se desarrollen políticas, procesos y procedimientos dirigidos exclusivamente a la detección, atención y solución oportuna de eventos o violaciones de seguridad y confidencialidad.

De manera general, el proceso de gestión de incidentes inicia con la **detección o identificación** del incidente (ya sea vulneración de seguridad, violación de confidencialidad o cualquier otro suceso similar que pueda afectar la seguridad de la información en poder de la autoridad fiscal).

Una vez identificado, el incidente se someterá a una evaluación en la cual será analizado, categorizado, priorizado y preparado para su atención mientras que, por otra parte, la administración deberá llevar a cabo una **investigación** sobre el incidente para determinar y evaluar su impacto. Una vez concluido dicho análisis, deberán tomarse **acciones específicas** para responder o atender el referido incidente hasta su **solución definitiva**.

Gestión de cambios

Se refiere a “la gestión controlada del desarrollo de nuevos sistemas y servicios, así como la realización de cambios importantes sobre los ya existentes. Comprende el diseño de soluciones sólidas, las pruebas y el control de lanzamientos, y es el medio por el cual se garantiza que la seguridad informática se incorpora a los cambios en los sistemas”[46].

El punto medular de la ejecución del proceso de gestión de cambios es que se trata de una medida que se considera de alto riesgo ya que, si se realizan de forma incontrolada existen altas posibilidades de que la confidencialidad, la integridad y la disponibilidad de los sistemas de la administración tributaria se pongan en peligro.

Las administraciones tributarias deben implementar el método de gestión de cambios que mejor se ajuste a sus requerimientos, circunstancias y necesidades y mantenerlo, en todo momento, alineado con las políticas integrales en materia de seguridad y confidencialidad de la información.

[46] Ibidem, pág. 89.

6. Monitoreo y prevención

Las prácticas relacionadas con el monitoreo y prevención son esenciales para las administraciones tributarias ya que permiten detectar y responder de manera oportuna y proactiva a posibles amenazas, disminuir potenciales brechas de seguridad y minimizar el impacto de los ataques que pudieran suscitarse.

Una de las medidas más efectivas para monitorear y prevenir las vulneraciones en materia de ciberseguridad es la revisión constante de controles en los sistemas tecnológicos, procesos y procedimientos. La evaluación periódica de estos controles fortalece las defensas de la administración tributaria ante amenazas externas e internas y garantiza la eficacia de las medidas implementadas.

La implementación de medidas de monitoreo y prevención ayuda a proteger la infraestructura de TI de las administraciones tributarias contra ataques maliciosos. Estas medidas actúan como una barrera adicional contra amenazas externas.

Así, medidas como el establecimiento de parámetros claros, la revisión continua de controles, la ejecución de pruebas y evaluaciones y generación de reportes detallados y la realización de auditorías internas o externas permitirá a la autoridad fiscal la implementación de acciones de mejora, contribuyendo así a la adopción de una estrategia de seguridad efectiva que garantizará no solo la protección de datos sensibles, sino también el cumplimiento de las normativas y la confianza en la integridad de los sistemas de administración tributaria.

6.1. Definición de parámetros

La fase de monitoreo y prevención inicia con la definición clara de los parámetros de seguridad, es decir, la administración tributaria deberá establecer y especificar criterios, límites o directrices que guían la implementación y el funcionamiento de los controles de seguridad. Estos parámetros son fundamentales para asegurar que las medidas de seguridad sean efectivas y consistentes dentro de la administración y en todo momento deberán estar alineados con las normativas nacionales e internacionales aplicables a la seguridad de la información en materia fiscal.

A tales efectos, es identificar cuáles serán los sistemas y aplicativos que serán objeto de monitoreo y posteriormente se establecerán umbrales específicos para fijar alertas de seguridad (volumen de

transacciones, accesos fallidos a aplicativos, etc.), finalmente, como parte del protocolo, se deberán definir políticas claras relativa a los procedimientos aplicables para la revisión periódica de los sistemas de seguridad.

Estos parámetros servirán como indicadores para que la autoridad pueda llevar a cabo los procedimientos de revisión y evaluación y obtener información de utilidad respecto del estado que guardan sus sistemas en materia de seguridad cibernética.

6.2. Revisión de controles

La etapa de revisión de controles tiene como objetivo evaluar y verificar la efectividad de los controles de seguridad implementadas, así como identificar áreas que requieran ser ajustadas y/o mejoradas para fortalecer el marco GSI y GSTI. Esto implica que la administración fiscal deberá adoptar un sistema que compruebe que los controles previstos en las políticas se aplican de manera adecuada y eficaz.

La revisión de controles internos y externos para monitorear la seguridad de la información es un proceso continuo y multidimensional ya que requiere una combinación de controles técnicos, políticas organizativas y colaboración interinstitucional para proteger la información y, en consecuencia, garantizar la confianza pública en el sistema fiscal.

Al respecto, la OCDE señala que “las jurisdicciones deben revisar los procesos de monitoreo y de cumplimiento en respuesta a infracciones, y la alta dirección debe asegurarse de que las recomendaciones de cambios se aplican en la práctica. Esto significa que las administraciones tributarias deben revisar en general sus procesos de monitoreo, cumplimiento y gestión de infracciones, así como los controles de seguridad relevantes, no solo de forma rutinaria, sino también en base a las lecciones aprendidas de infracciones específicas.”[47]

Esta fase resulta trascendental ya que permite que la administración tributaria pueda validar la efectividad de las medidas implementadas y adecuarlas según se requiera. A mediano plazo, la organización tendrá la certeza de que se mantiene alineada a los estándares de seguridad vigentes y atender de manera proactiva a las amenazas en ciberseguridad al tiempo que mejora la percepción de confianza en la capacidad de la organización para administrar y proteger la información de manera segura y eficaz.

[47] OECD, *Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información,* Op. Cit., págs. 98-99.

En adición a los controles internos señalados anteriormente, las autoridades fiscales deben establecer mecanismos robustos de control externo a través de la implementación de medidas tales como la ejecución de auditorías independientes, la obtención de certificaciones por parte de organismos reguladores o incluso, la colaboración con otras autoridades fiscales -por ejemplo, a través del intercambio de información.

Mediante tales acciones será posible evaluar la efectividad de los controles internos y obtener recomendaciones y/o mejores prácticas para mejorar la seguridad de la información fiscal. Estas revisiones, además de validar la eficacia de los controles internos también permitirá identificar de manera oportuna las vulnerabilidades o debilidades potenciales que podrían verse afectadas indebidamente por amenazas o riesgos tanto internos como externos.

6.3. Pruebas y evaluaciones

La ejecución de pruebas de seguridad informática es esencial para simular ataques y evaluar la capacidad de respuesta de los sistemas ante diferentes escenarios. Estas pruebas proporcionan información valiosa para mejorar la resiliencia y la capacidad de recuperación ante posibles incidentes.

En general, en esta fase la administración tributaria deberá aplicar evaluaciones técnicas y no técnicas para calificar la seguridad y confidencialidad de la información en las jurisdicciones o entidades objeto del diagnóstico. Esto puede incluir análisis de vulnerabilidades, pruebas de penetración, revisión de políticas y procedimientos, entrevistas con personal clave y revisión de documentación relevante.

Auditorías de cumplimiento

Una medida efectiva para evaluar adecuadamente la efectividad de la implementación del marco GSI puede ser la ejecución de una **auditoría** mediante la cual la administración tributaria podrá asegurarse de que cumple con las regulaciones de seguridad y confidencialidad de la información. A través de este procedimiento, será posible identificar, evaluar y mitigar oportunamente los riesgos de la ciberseguridad.

Las auditorías pueden ejecutarse de manera *interna* (si las lleva a cabo personal de la propia administración tributaria) o *externa* (realizada por un tercero experto en la materia); independientemente del enfoque, es necesario que el auditor cuente con un entendimiento claro e integral de la organización, sus objetivos, riesgos y procesos para poder abordar completamente los desafíos de ciberseguridad a los que se enfrenta la autoridad fiscal.

Rubros susceptibles de análisis durante una auditoría[48]	
Evaluación técnica	
Operaciones y tecnología	• Análisis de vulnerabilidades y pruebas de penetración • Acceso a la red y monitoreo / evaluación de amenazas • Revisiones de configuraciones de dispositivos (infraestructura, firewalls, routers, etc.) • Wi-Fi: configuraciones y pruebas de vulnerabilidades / explotación Wi-Fi no autorizado • Puntos de acceso remoto / VPN: evaluación técnica de los puntos de acceso remoto y de la configuración para ayudar a garantizar su protección • Evaluación de aplicaciones / bases de datos, para llevar a cabo análisis de vulnerabilidades, pruebas de penetración y configuración de bases de datos • Seguridad por diseño • Revisiones y análisis de arquitectura • Configuración de seguridad del sistema operativo / base de datos • Proceso de parcheo / procedimientos de remediación • Revisión de códigos.
Evaluaciones de procesos y controles	
	• Gestión de identidades y accesos. • Procedimientos de gestión de acceso. • Gestión de acceso remoto y autenticación. • Gestión de acceso privilegiado. • Seguridad física y personal: Controles de acceso lógico y físico, conciencia de seguridad / ingeniería social y seguridad de los dispositivos móviles. • Evaluaciones de seguridad de las operaciones.
Factores humanos	• Gestión del talento y formación en TI.
Dirección y Gobierno	• Gobierno de ciberseguridad, funciones y responsabilidades. • Integración de la gestión de riesgos cibernéticos y empresariales.
Legal y cumplimiento	• Consideraciones reglamentarias e integración en el marco cibernético.
Gestión de riesgos de la información	• Gestión de riesgos de los proveedores y seguridad. • Análisis de amenazas cibernéticas y proceso de gestión de riesgos: Identificación de amenazas, evaluación y proceso de actualización y gestión del cambio, incluida su integración en el ciclo de vida de desarrollo de software. • Seguridad informática en la nube y evaluación continua. • Clasificación, protección y cifrado de datos, programas de formación y sensibilización en toda la organización.

[48] KPMG, "*The role of internal audit in cyber security readiness*", 2019. Documento disponible en https://assets.kpmg.com/content/dam/kpmg/lu/pdf/2019/lu-en-cyber-databreach-brochure.pdf

6.4. Reportes

Los reportes de seguridad proporcionan una visión integral del estado de la ciberseguridad dentro de las administraciones tributarias. Estos informes son fundamentales para tomar decisiones informadas y asignar recursos de manera efectiva para mitigar riesgos.

6.5. Implementación de acciones de mejora

La implementación de acciones de mejora basadas en los resultados de las pruebas y evaluaciones contribuye a fortalecer la seguridad tecnológica de las administraciones tributarias. Estas acciones pueden referirse a la actualización de software, la capacitación del personal y la implementación de políticas de seguridad más estrictas.

A partir del análisis que la administración tributaria efectúe de la información recabada durante la fase de revisión (i.e. evaluaciones, pruebas, auditorías, reportes) la autoridad estará en posibilidades de identificar las áreas en las que se requiera implementar cambios, ajustes y mejoras. Posteriormente, se deberá diseñar un plan de acción enfocado en abordar las áreas de oportunidad que requieran atenderse, priorizando las acciones con base en su impacto y urgencia. Finalmente, se deberán implementar las acciones de mejora planificadas y probarse a efecto de verificar su adecuado funcionamiento.

La concientización del personal sobre las mejores prácticas de seguridad cibernética es esencial para disminuir la posibilidad de que se presenten posibles ataques internos y el error humano. La capacitación habitual sobre la importancia de mantener contraseñas seguras, identificar correos electrónicos malignos y proteger la información confidencial ayuda a robustecer la postura de seguridad de la administración fiscal.

Asimismo, la inversión en tecnologías de seguridad avanzadas y la actualización constante de los sistemas son necesarias para mantenerse al día ante las diversas amenazas tecnológicas que aumentan exponencialmente. El compromiso continuo con la mejora de la seguridad cibernética es esencial para proteger la información en poder de las autoridades fiscales y así, garantizar la confianza en los sistemas de administración tributaria.

Recomendaciones de la OCDE para garantizar la seguridad y confidencialidad de la información.

Las siguientes recomendaciones se han creado para ayudar a las autoridades fiscales a garantizar que la información confidencial del contribuyente se salvaguarda debidamente.

(…)

- *Existirán políticas y procedimientos exhaustivos sobre la confidencialidad de la información fiscal, se deberán revisar regularmente y estar refrendadas al más alto nivel de la administración fiscal. Asimismo, deberá quedar claro a quién se atribuye la responsabilidad de la implementación de la política dentro de la administración.*
- *Todas las personas que cuenten con acceso a la información confidencial deberán ser sometidas a verificaciones de antecedentes o controles de seguridad.*
- *El contrato laboral o el acuerdo de empleo deberá contener disposiciones relacionadas con las obligaciones del empleado en lo que respecta a la confidencialidad de la información fiscal y, además, dichas obligaciones no cesarán una vez finalizada la relación de empleo. Los consultores, prestatarios de servicios y contratistas estarán obligados por contrato a cumplir con las mismas obligaciones que los empleados (ya sea a tiempo completo o de manera temporal) y dichas obligaciones prevalecerán más allá del período de contrato o colaboración.*
- *Los empleadores deberán ofrecer formación y recordatorios de forma regular explicando las responsabilidades del empleado en relación con la información fiscal confidencial, determinando claramente dónde pueden obtener ayuda en caso de que tengan preguntas o necesiten consejo.*
- *Los locales, o las zonas dentro de las instalaciones, en las que se encuentre la información fiscal deberán ser seguras y no accesibles por parte de personas no autorizadas.*
- *Toda situación de almacenamiento, circulación, acceso o eliminación de documentos que contengan información confidencial (tanto en formato papel como electrónico), deberá realizarse de forma segura y garantizando la confidencialidad de los documentos.*
- *Deberán existir políticas y procedimientos para la gestión de divulgaciones de información confidencial realizadas sin autorización*
- *Todas las solicitudes de información y toda la información que se reciba deberán ser archivadas de forma segura. Se controlará estrictamente el acceso y se actuará según el principio de la "necesidad de conocimiento".*

Fuente: *Garantizando la confidencialidad. Guía de la OCDE sobre la protección de la información objeto de intercambio con fines fiscales.*

7. Generación de datos abiertos en las administraciones tributarias

7.1. Definición

La OCDE define el gobierno abierto como “la cultura de gobernanza basada en políticas innovadoras y políticas y prácticas públicas sostenibles inspiradas en los principios de transparencia, rendición de cuentas y participación de las partes interesadas en apoyo de la democracia y el crecimiento inclusivo”, mientras que un Estado Abierto se da “cuando los poderes ejecutivo, legislativo y judicial, las instituciones públicas independientes y todos los niveles de gobierno -reconociendo sus respectivos roles, prerrogativas e independencia general conforme a sus actuales marcos jurídicos e institucionales- colaboran, explotan sinergias y comparten buena prácticas y lecciones aprendidas entre ellos y con otras partes interesadas para promover transparencia, integridad, rendición de cuentas y participación de las partes interesadas, en apoyo de la democracia y el crecimiento inclusivo”.[49]

Recientemente se ha reconocido la importancia y el impacto de los datos abiertos en relación con los objetivos del desarrollo sostenible ya que se considera que tienen el potencial de transformar la manera en la que los gobiernos se enfrentan a los desafíos globales, proporcionando información valiosa para la toma de decisiones y promoviendo la transparencia, la participación y la innovación. Los gobiernos alrededor del mundo han impulsado iniciativas[50] que no solo promueven la divulgación y uso efectivo de los datos públicos, sino que también han fijado objetivos de gran envergadura como el crecimiento económico sostenible, combate al cambio climático, equidad de género y reducción de la pobreza, entre otros.

En 2024 la OCDE, en el estudio titulado Panorama de las Administraciones Públicas: América Latina y el Caribe 2024[51] publicó -en el capítulo 9 relativo al Gobierno digital y datos abiertos gubernamentales- los resultados del Índice de Datos Abiertos, Útiles y Reutilizables (OURdata)[52]. Este índice evalúa tres pilares fundamentales en materia de datos abiertos gubernamentales:

---

[49] Recomendación del Consejo de la OCDE sobre el Gobierno Abierto. Disponible en https://www.oecd.org/gov/oecd-recommendation-of-the-council-on-open-government-es.pdf

[50] Datos Abiertos para el Desarrollo. Más información disponible en https://www.od4d.net/

[51] OECD (2024), Panorama de las Administraciones Públicas: América Latina y el Caribe 2024, OECD Publishing, Paris, p. 128. Documento disponible en https://doi.org/10.1787/0f191dcb-es.

[52] OURdata es una encuesta que busca evaluar los esfuerzos de las administraciones públicas relativos al diseño e implementación de políticas domésticas de datos abiertos gubernamentales.

a) **Disponibilidad de datos abiertos:** Analiza el grado de adopción e implementación de diversos requisitos para la publicación o divulgación de datos abiertos gubernamentales. Evalúa también la demanda de dichos datos y los conjuntos de datos disponibles.

b) **Accesibilidad de los datos:** Referido a los requisitos establecidos para proporcionar los datos en formatos adecuados y de buena calidad, incluyendo el medio a través del cual se suministran. Evalúa también el grado de participación de los interesados.

c) **Reutilización de los datos:** Analiza el grado de apoyo gubernamental y promoción proactiva en la reutilización de la información.

En relación con esta evaluación, el Índice arrojó que, en relación con los seis países[53] de América Latina y el Caribe incluidos en el análisis, en promedio, puntuaron por debajo de la media de la OCDE[54] en los tres pilares del índice, lo que permite concluir que aún existen áreas en las cuales es necesario adoptar e implementar medidas y políticas más efectivas que promuevan y favorezcan el acceso a la información pública de una manera ágil, sencilla y adecuada.

7.2. Marco legal del gobierno de datos abiertos

A partir de lo antes señalado, uno de los elementos fundamentales de los que depende la eficacia de la implementación de las políticas de datos abiertos es la existencia de un marco legal robusto que cuente con políticas, normas y regulaciones que garanticen la disponibilidad y accesibilidad de la información estableciendo los límites, derechos y obligaciones tanto para la autoridad como para los ciudadanos.

De manera general existen diversas formas en las cuales se pueden implementar o adoptar las políticas relativas a los datos abiertos gubernamentales; lo crucial es que estas políticas se incorporen a la legislación doméstica de las jurisdicciones con el fin de ofrecer certeza jurídica tanto a los ciudadanos como a las propias administraciones respecto de la forma en la que la apertura gubernamental se llevará a cabo. Deberán establecerse los principios básicos rectores, delimitarse claramente los alcances y restricciones que el acceso a la información tendrá, los sujetos obligados y todas las normas de procedimiento que resulten aplicables, relacionadas principalmente con el tiempo y forma en la que se divulgará la información.

[53] Brasil, Chile, Colombia, Costa Rica, México, Perú.

[54] La puntuación asignada de cada pilar tiene un valor de 0 a 1, el puntaje total asignado corresponde a un promedio de las calificaciones de los 3 pilares. En este caso, los países de América Latina y el Caribe obtuvieron una puntuación promedio de 0.37; la puntuación media de los países OCDE fue de 0.48.

Con base en lo anterior, se tiene que las políticas en materia de datos abiertos pueden estar contenidas en diversos instrumentos o cuerpos normativos:

a) **Constitución Nacional.** Varias jurisdicciones han elevado a rango constitucional el reconocimiento expreso al derecho al acceso a la información. A partir de esto se desarrollarían leyes específicas y normatividad secundaria. En este supuesto se encuentran Guatemala, México, Panamá, países que también cuentan con normativas especializadas en materia de transparencia y acceso a la información.

> ***Reconocimiento expreso del derecho al acceso a la información a nivel Constitucional. Panamá.***
>
> *ARTÍCULO 43.*
>
> *Toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos, siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación.*
>
> *ARTÍCULO 44.*
>
> *Toda persona podrá promover acción de hábeas data con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información.*
>
> *Esta acción se podrá interponer, de igual forma, para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución.*
>
> *Mediante la acción de hábeas data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal. La Ley reglamentará lo referente a los tribunales competentes para conocer del hábeas data, que se sustanciará mediante proceso sumario y sin necesidad de apoderado judicial.*

b) **Leyes específicas en materia de transparencia y/o acceso a la información**. Estas normativas constituyen el punto medular de las políticas de gobierno abierto. El enfoque que ha sido adoptado por la mayoría de las jurisdicciones es implementar normativas que abarcan por igual las cuestiones relativas a transparencia y acceso de información con independencia de que exista un reconocimiento expreso del derecho al acceso a la información a nivel constitucional. En este supuesto se encuentran Argentina, Colombia, España, Honduras, Guatemala, México, entre otras.

c) **Regulaciones secundarias.** Primordialmente regulaciones administrativas, normativas, reglamentos, circulares, etc. Relativas a cuestiones procedimentales, normativas administrativas internas, gestión de la información, entre otros supuestos.

7.3. Elementos mínimos de la normativa en materia de transparencia y acceso a la información

De manera general, con independencia del instrumento legal que se utilice para su implementación, la normatividad en materia de transparencia y acceso a la información debe contar, cuando menos con los siguientes elementos:

Objeto: Se refiere a señalar el propósito general de la norma que es el garantizar el acceso a la información en posesión, custodia o control de las autoridades o los sujetos obligados. Se basa en el principio de *máxima publicidad* que indica que cualquier información en posesión de las autoridades debe cumplir con tres atributos: *completa, oportuna* y *accesible.*

Sujetos obligados: Por regla general se considera que son las instituciones de la Administración Pública a nivel central o federal, regional, provincial o municipal, órganos descentralizados y desconcentrados.

Sujetos solicitantes: Cualquier persona tendrá acceso garantizado a la formulación de solicitudes de información, incluso de manera anónima, sin justificar las razones que motivan la solicitud de información.

Divulgación Activa: El sujeto obligado difundirá de manera proactiva la información sin que medie solicitud alguna; la normatividad deberá precisar qué información será susceptible de difundirse proactivamente, por ejemplo, información sobre funcionarios públicos, presupuesto, gestión financiera, obra pública, gasto público, etc.

Obligaciones: Deberán describirse las obligaciones primarias y adicionales que deberán cumplir los sujetos obligados al momento de atender las solicitudes de información.

Casos especiales: Pueden incorporarse supuestos especiales o específicos, dirigidos a sectores específicos o respecto de tipos de información especializada o específica.

Procedimientos aplicables a las solicitudes de información: Deberán describirse claramente los supuestos bajo los cuales los ciudadanos podrán solicitar información. Las normas deberán abarcar, cuando menos, los requisitos aplicables, tramitación, procedimientos de notificación, tiempo y forma de entrega, costos inherentes a la solicitud (aun cuando el trámite debe ser gratuito, es posible que el ciudadano requiera un

formato susceptible de ser cobrado, por ejemplo, copias certificadas), periodos de respuesta, medios y recursos para apelación o impugnación.

Excepciones: Indicar de manera precisa y clara los supuestos bajo los cuales los sujetos obligados podrán denegar de manera válida el acceso a la información. De manera general, las excepciones recaen sobre *información reservada (*excluida por existir un riesgo claro, probable y específico de daño a los intereses públicos) o *información confidencial.*

Acciones sobre transparencia activa. Costa Rica

Decreto No. 40200-MP-MEIC-MC

Artículo 11. *Las instituciones públicas descentralizadas procurarán publicar en su respectivo sitio web oficial, al menos, la siguiente información pública:*

Marco normativo que rige la gestión pública de la institución.
Estructura orgánica, competencias, obligaciones y servicios brindados.
Directorio institucional.
Listado de funcionarios institucionales.
Horario de atención de la Institución.
Descripción detallada de los servicios brindados al público y la forma cómo estos se realizan.
Planes y presupuestos institucionales, así como su forma de ejecución y evaluación.
Procesos para el reclutamiento y selección de personal.
Mecanismos y resultados del proceso de evaluación de desempeño de los funcionarios.
Planillas con el salario bruto.
Plan anual operativo y planes estratégicos.
Memorias anuales y otros informes de gestión.
Informes de la Auditoría Interna sobre la gestión institucional.
Actas de los órganos colegiados establecidos por ley, salvo expresa disposición legal.
Descripción clara y precisa de los trámites y requisitos que se pueden llevar a cabo ante la institución.
Toda la información de las etapas de los procesos de contratación administrativas de la institución.
Mecanismos de presentación de solicitudes de información, peticiones, denuncias y sugerencias para el mejoramiento de la función de la institución, así como cualquier otro medio de participación ciudadana.

Listado de los subsidios, becas, donaciones, exoneraciones o cualquier otra transferencia o beneficio otorgado a personas particulares, sin perjuicio de lo determinado en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, norma número 8968.

Informes de viajes, gastos de representación, costos de viajes, pagos por concepto de viáticos de los funcionarios de la institución, entre otros.

Cualquier otra información que fomente la transparencia y el control en el ejercicio de la función pública.

La publicación de esta información atinente a la gestión de casa institución será en formato abierto, interoperable y accesible.

Clasificación de la información: Deben regularse claramente las categorías aplicables a la información en posesión de las autoridades y los procedimientos para llevar a cabo la clasificación y desclasificación.

Periodismo y el acceso a la información. Honduras.

En la Ley de Transparencia y Acceso a la Información Pública (Decreto 170-2006) de Honduras sobresale un supuesto legal que garantiza a los periodistas el acceso a la información. Esto representa un caso especial dentro del marco normativo relacionado con temas de transparencia y acceso a la información ya que, en primera instancia, se trata de un supuesto dirigido específicamente al sector periodístico y en segunda instancia porque, indirectamente, facilita y salvaguarda el derecho al acceso a la información de la ciudadanía en su conjunto.

Dicha disposición se transcribe a continuación:

Artículo 22. Acceso a la Información por parte de los Periodistas. Las autoridades están obligadas a dar protección y apoyo a los periodistas en ejercicio de su profesión, proporcionándoles la información solicitada sin más restricciones que las contempladas en esta ley y en las demás Leyes de la República.

Órganos especializados: Se pueden constituir órganos que se encargarán de la promoción, garantía y vigilancia del cumplimiento de las obligaciones relativas al acceso a la información.

Creación de órganos reguladores en materia de transparencia. Panamá

Panamá cuenta con una legislación específica cuyo principal objetivo es la creación del órgano que regula y monitorea que efectivamente se cumplan las obligaciones en materia de acceso a la información.

Ley 33 del 25 de abril de 2013 que crea la
Autoridad Nacional de Transparencia y Acceso a la Información

Artículo 1. Se crea la Autoridad Nacional de Transparencia y Acceso a la Información, en adelante la Autoridad, como institución pública, descentralizada del Estado, que actuará con plena autonomía funcional, administrativa e independiente, en el ejercicio de sus funciones, sin recibir instrucción de ninguna autoridad, órgano del Estado o persona. (…)

Artículo 2. La Autoridad velará por el cumplimiento de los derechos consagrados en la Constitución Política de la República de Panamá en el tema de Derecho Constitucional de petición y de acceso a la información, así como por los derechos previstos en los convenios, acuerdos, tratados, programas internacionales y nacionales en materia de prevención contra la corrupción y por la inserción e implementación de las nuevas políticas de prevención en la gestión pública a nivel gubernamental por iniciativa propia o por propuestas nacionales o internacionales.

Infracciones y Sanciones aplicables en casos de incumplimiento y violaciones a las obligaciones de transparencia.

Sanciones por incumplimiento a las obligaciones de transparencia. República Dominicana

Ley General de Libre Acceso a la Información Pública, No. 200-04.

De las Sanciones Penales y Administrativas
Impedimento u Obstrucción del Acceso a la Información

Artículo 30. El funcionario público o agente responsable que en forma arbitraria denegare, obstruya o impida el acceso del solicitante a la información requerida, será sancionado con pena privativa de libertad de seis meses a dos años de prisión, así como con inhabilitación para el ejercicio de cargos públicos por cinco años.

7.4. Ámbito internacional

Alianza para el gobierno abierto

En el ámbito internacional sobresale una iniciativa que tiene como objetivo primordial proveer una plataforma internacional que busca incorporar a gobiernos, sociedad civil y ciudadanía tendiente a garantizar el acceso a la información y la rendición de cuentas.

Esta iniciativa, lanzada en 2011, se conoce como la Alianza para el Gobierno Abierto (*Open Government Partnership*) y a la fecha del presente incluye 75 países[55], 150 gobiernos locales (estatales y/o municipales) y múltiples organizaciones de la sociedad civil.

Para adherirse a la Alianza, se requiere que los gobiernos cumplan con los criterios de elegibilidad básica. Estos criterios evalúan cuatro rubros distintos: transparencia fiscal, acceso a la información, divulgación de activos de funcionarios públicos y participación ciudadana. Adicionalmente, se aplicará una evaluación de *verificación de valores* que se enfoca en la interacción de los gobiernos y las organizaciones de la sociedad civil, primordialmente el control de la entrada y salida de éstas a la vida pública y el grado en que el gobierno intenta reprimirlas.

Finalmente, los gobiernos deberán respaldar la *Declaración de Gobierno Abierto*[56] a través de la cual refrendarán su compromiso con los principios de gobierno abierto y transparente mediante el diseño e implementación de un plan de acción a través de una consulta pública e informes anuales de autoevaluación respecto de la relevancia de los principios básicos de gobierno abierto y la implementación de Plan de Acción.

Ahora bien, para el periodo 2023 – 2028, la Alianza ha diseñado una estrategia global que gira en torno a cinco objetivos fundamentales que deberán implementarse atendiendo a las capacidades y condiciones de cada uno de los miembros, estos objetivos son:

a) Formar una comunidad cada vez mayor, comprometida e interconectada de personas reformadoras, activistas y líderes de gobierno abierto.

[55] En el caso de **América**, los países miembros -a la fecha del presente- son: Argentina, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, Estados Unidos, Guatemala, Honduras, Jamaica, México, Panamá, Paraguay, Perú, República Dominicana y Uruguay. El Salvador fue miembro por el periodo de 2011 a 2023, actualmente su estatus en la Alianza aparece como *retirado*.

[56] Texto completo disponible en https://www.opengovpartnership.org/es/process/joining-ogp/open-government-declaration/

b) Lograr que el gobierno abierto sea fundamental en la operación y las prioridades de los gobiernos de todos los niveles y poderes.

c) Proteger y ampliar el espacio cívico.

d) Acelerar el avance colectivo en favor de las reformas de gobierno abierto.

e) Ser un centro de casos innovadores, evidencias e historias de gobierno abierto inspiradoras.

La Alianza cuenta con un medio de revisión para calificar el estado que guarda la implementación de los Planes de Acción diseñados por los gobiernos miembros, este medio, conocido como Mecanismo de Revisión Independiente está conformado por un grupo multinacional de expertos que evalúa el grado de avance en la implementación.

Los resultados de la revisión se publican en Reportes que reflejan el nivel de progreso en materia de transparencia, rendición de cuentas y participación ciudadana de los planes de acción y también contienen recomendaciones técnicas para guiar la actuación de las partes orientadas a la consecución de sus objetivos.

Ahora bien, en relación con la participación de las jurisdicciones de la región, sobresale lo siguiente:

a) Costa Rica: Se adhirió a la Alianza en 2022 a nivel local. A la fecha ha presentado un Plan de Acción y ha asumido dos compromisos relativos a la administración local.

b) Guatemala: Adherido a nivel nacional en 2011. Ha presentado, en total, seis Planes de Acción – el último presentado en 2023- y ha asumido 126 compromisos. Entre estos compromisos resaltan: *Acciones institucionales para fortalecer los datos abiertos, Actualización participativa del Plan de Gobierno digital, Fortalecimiento de datos abiertos, Creación e implementación de una estrategia integral sobre transparencia, gobierno abierto y anticorrupción, Fortalecimiento de mecanismos anticorrupción de transparencia y resultados que evidencian el nivel nacional e internacional* y *Acciones para seguir avanzando en la adopción de controles internacionales de transparencia fiscal, compras y contrataciones.*

c) Honduras: Adherido en 2011, ha presentado cinco Planes de Acción (el último Plan fue presentado el 2023) y, a la fecha, ha asumido 93 compromisos. Los compromisos relacionados con transparencia y acceso a la información más relevantes fueron: *Datos abiertos, Aplicación de la Ley de Transparencia y Acceso a la Información Pública, Política integral, transparencia, probidad y ética, La ética en el servicio público, Respeto del derecho del ciudadano a obtener información de los registros públicos.*

d) Panamá: Se adhirió a la Alianza en 2012, a la fecha ha presentado cinco planes de acción y ha asumido 48 compromisos. Los más relevantes son: *Implementación de la Ley de Transparencia, Institucionalización del gobierno abierto de Panamá* y *Responsabilidad de las instituciones públicas.*

e) **República Dominicana:** Se adhirió -a nivel local- en 2022, asumiendo cinco compromisos y 1 Plan de Acción.

Open Data Charter

Otro proyecto relevante en materia de datos abiertos es el *Open Data Charter*[57]*, que* es una iniciativa global que promueve la apertura y transparencia en la publicación de datos. Su objetivo es fomentar que los gobiernos, organizaciones y empresas publiquen datos de manera abierta, accesible y reutilizable para que la sociedad pueda beneficiarse de ellos.

El *Open Data Charter* establece principios fundamentales para promover la apertura y el uso efectivo de los datos gubernamentales. Estos principios son:

a) **Acceso y uso:** Los datos deben estar disponibles para todos, sin restricciones de acceso y con permisos claros para su uso.

b) **Calidad y cantidad**: Los datos deben ser precisos, oportunos y completos, garantizando su utilidad para diversas aplicaciones.

c) **Transparencia**: La apertura de datos debe promover la transparencia en la gestión gubernamental y mejorar la rendición de cuentas.

d) **Innovación y valor agregado:** La disponibilidad de datos debe fomentar la innovación, creando valor económico y social a través de nuevas aplicaciones y servicios.

e) **Participación:** Debe facilitarse la participación ciudadana y el compromiso cívico mediante el acceso a datos relevantes y comprensibles.

Declaración de Punta del Este

En 2022, se llevó a cabo la 6ª Reunión de la Declaración de Punta del Este, cuyo principal objetivo es maximizar el uso efectivo de la información intercambiada bajo los diferentes estándares de intercambio de información para fines fiscales. También busca abordar la evasión fiscal, la corrupción y otros delitos financieros a través del uso amplio de información, la creación de marcos eficaces que permitan disponer y acceder a información de beneficiarios finales, el aprovechamiento de la información financiera obtenida de manera automática, entre otros asuntos.

[57] https://opendatacharter.org/principles/

Como resultado de esta reunión, la Asamblea General emitió cuatro recomendaciones:

a) *Adoptar, siempre en su ámbito legal de actuación, un papel activo y de vanguardia en la adaptación de la sociedad a los desafíos del desarrollo digital y el aprovechamiento de las oportunidades de las nuevas tecnologías*; mediante, entre otras medidas, el reforzamiento de la seguridad informática de la información tributaria y las comunicaciones, estableciendo modelos adecuados de gobernanza de los datos en la era digital e implementando planes de continuidad de las operaciones fundamentales de la administración tributaria.

b) *Establecer sinergias con la sociedad -las empresas, los ciudadanos y el resto de los organismos y estamentos del Estado- de cara a fomentar el desarrollo de sus países y sociedades;* colaborando internamente, con pleno respeto a los mandatos de protección de la privacidad, maximizando la utilidad de la información precisa y rápida de la que disponen las administraciones tributarias gracias a innovaciones tecnológicas e implementando una política de disponibilidad de datos abiertos, resguardando la privacidad de los contribuyentes y utilizando técnicas de anonimización de datos.

c) *Contribuir a fomentar, en el marco de su actuación, la inclusión social y la lucha contra la informalidad;* colaborando dentro del marco legal de cada país y asegurando el respeto a los derechos de los contribuyentes en la adecuada implantación de políticas sociales, aprovechando la calidad y la cantidad de información que manejan las administraciones tributarias.

d) *Fomentar las mejores prácticas en el desarrollo del personal de las administraciones tributarias para conseguir los objetivos de funcionamiento, recaudación y control previamente fijados.*

7.5. Datos abiertos disponibles

La importancia de publicación de datos en las administraciones tributarias se explica principalmente por las siguientes razones:

a) Transparencia y rendición de cuentas: Permite a los ciudadanos y a las organizaciones de la sociedad civil monitorear cómo se recaudan y utilizan los fondos públicos, promoviendo una gestión más eficiente y ética de los recursos.

b) Mejora de la toma de decisiones: Partes interesadas del sector privado, academia, sociedad civil entre otros pueden tomar decisiones más informadas basadas en datos actualizados y precisos, lo que puede llevar a políticas fiscales más efectivas y equitativas.

c) **Fomento de la innovación y el desarrollo económico:** Los datos abiertos pueden servir como base para el desarrollo de nuevas herramientas y aplicaciones que simplifiquen los procesos fiscales, mejoren la experiencia del usuario y promuevan la conformidad voluntaria.

En 2022 el *Open Data Barometer y Data for Development* publicaron el Barómetro Global de Datos, con el objetivo de evaluar el estado de los datos a nivel mundial, buscando promover el aprendizaje colectivo sobre prácticas efectivas y estrategias exitosas. Según el Barómetro[58] los datos abiertos deben cumplir con requisitos esenciales para garantizar su efectividad y utilidad, entre ellos se encuentra estar disponibles gratuitamente y sin restricciones, ser accesibles para todos los ciudadanos, mantener una alta integridad y calidad, ser estructurados para facilitar la interoperabilidad y promover la participación de la comunidad en su uso y mejora continua.

Una mirada a los portales abiertos de Administraciones Tributarias más avanzadas muestra que los atributos que generalmente se encuentran presentes en iniciativas de datos abiertos son los siguientes:

a) **Accesibilidad:** los datos están disponibles de manera accesible y fácil de encontrar para el público en general, sin barreras técnicas o burocráticas significativas. Por ejemplo, la Agencia de Ingresos de Canadá (CRA por sus siglas en inglés) ha publicado 292 registros en el Portal de Gobierno Abierto.

b) **Actualización regular:** existe un compromiso con la actualización periódica de los datos, asegurando que la información disponible sea relevante y precisa en todo momento. En el caso específico de Canadá, de los 292 registros, 251 se actualizan anualmente, 13 no tienen una planificación específica para su actualización, 11 se actualizan trimestralmente, 11 según sea necesario, 5 se actualizan mensualmente y 1 semestralmente.

c) **Formatos interoperables:** Los datos se ofrecen en formatos estándar, lo que facilita su uso por parte de desarrolladores, investigadores y ciudadanos en general. En el caso específico de Canadá, el 98% de los registros están disponibles en formato .CSV, el 73% está disponible como HTML y solo 31% como PDF. Adicionalmente 18 registros están habilitados mediante interfaz de programación de aplicaciones (API por sus siglas en inglés).

d) **Retroalimentación por parte de usuarios:** Se fomenta la retroalimentación por parte de los usuarios y se promueve la participación ciudadana en la mejora continua de los servicios y la información disponible. En el caso específico de Canadá, el país cuenta con un Foro Multisectorial sobre Gobierno Abierto.

[58] El texto se encuentra disponible en el siguiente enlace: https://globaldatabarometer.org/wp-content/uploads/2022/05/GDB-Report-Spanish.pdf

Foro multisectorial sobre gobierno abierto – Canadá

Establecido el 24 de enero de 2018, el Foro Multisectorial sobre Gobierno Abierto tiene por objetivo (i) proporcionar aportes y consejos sobre los compromisos de gobierno abierto del Gobierno de Canadá, (ii) identificar nuevas áreas de enfoque, (iii) fortalecer la comunidad de gobierno abierto en todo Canadá

Los términos de Referencia del Foro Multisectorial detallan las siguientes responsabilidades y funciones del foro:

***1. Asesoramiento sobre compromisos de gobierno abierto**: El foro proporciona asesoramiento y recomendaciones sobre los compromisos específicos de gobierno abierto adoptados por el Gobierno de Canadá, asegurando que estos sean coherentes con los principios de transparencia y participación ciudadana.*

***2. Identificación de nuevas áreas de enfoque:** Además de revisar los compromisos actuales, el foro tiene la tarea de identificar áreas emergentes o prioritarias donde el gobierno abierto pueda ser fortalecido o expandido. Esto incluye explorar nuevas tecnologías y métodos para mejorar la apertura y accesibilidad de los datos gubernamentales.*

***3. Desarrollo de la comunidad de gobierno abierto:** El foro promueve la colaboración y el intercambio de mejores prácticas entre diferentes partes interesadas, fortaleciendo así la comunidad de gobierno abierto a lo largo y ancho de Canadá. Esto se logra a través de eventos, talleres y otras actividades diseñadas para fomentar la participación y el aprendizaje conjunto.*

***4. Estructura de miembros:** El foro está compuesto por un total de 12 posiciones de miembros, distribuidas en ocho para representantes de la sociedad civil y cuatro para miembros del Gobierno de Canadá. Esta estructura asegura una representación equilibrada y diversa de los intereses y perspectivas relacionadas con el gobierno abierto.*

***Fuente**: Gobierno de Canadá*

Catálogo de datos abiertos de la Agencia Estatal de Administración Tributaria de España

Algunos ejemplos de datos abiertos disponibles en España son los siguientes:

1. *Avance de ventas interiores en grandes empresas y Pymes: proporciona datos semanales sobre las ventas realizadas por empresas tanto grandes como pequeñas y medianas (PYMEs) en el mercado interior español. Su propósito es ofrecer una visión general de la evolución de las ventas en el mercado nacional, lo que puede ser útil para analizar tendencias económicas y comerciales.*

2. *Observatorio de márgenes empresariales: proporciona datos trimestrales para el seguimiento y análisis de los márgenes empresariales, información que proviene de las declaraiones de Impuesto sobre Sociedades, así como de modelos de IVA y retenciones sobre rendimientos del trabajo. Estos datos incluyen variables de la Cuenta de Pérdidas y Ganancias del Impuesto sobre Sociedades, cifras de ventas y compras del IVA, y datos sobre masa salarial y perceptores de salarios.*

3. *Estadistica de PYMES societarias y no societarias: cifras anuales relativa a las actividades económicas facilitada por los empresarios y profesionales personas físicas en sus declaraciones anuales del Impuesto sobre la Renta y en la información relativa a los estados contables que las empresas societarias presentan en sus declaraciones anuales del Impuesto sobre Sociedades.*

4. *Estadística de los declarantes del Impuesto sobre la Renta de las Personas Físicas de los mayores municipios por código postal: proporciona un análisis detallado de la renta bruta media y otras magnitudes declaradas a nivel de código postal. Esta estadística refleja la gran disparidad en la renta media entre barrios de grandes ciudades y núcleos rurales dispersos. Los municipios seleccionados cumplen al menos uno de los siguientes criterios: tener más de 200,000 habitantes, recibir más de 100,000 declaraciones de IRPF, o tener una renta bruta total superior a 2,200 millones de euros.*

5. *Ventas diarias (Información semanal SII) La estadística del Sistema de Suministro Inmediato de Información (SII) ofrece datos diarios sobre las ventas de empresas obligadas a usar este sistema, incluyendo Grandes Empresas, grupos del IVA y aquellas inscritas en el Registro de Devolución Mensual. Este sistema proporciona información de ventas más actualizada que los informes mensuales o trimestrales tradicionales del IVA. Las ventas diarias representan aproximadamente el 70% del total de ventas interiores de los contribuyentes del IVA. La publicación incluye un informe y series históricas desde el 1 de julio de 2017, que sirven para analizar la coyuntura económica y complementar otros informes de ventas y recaudación tributaria.*

Fuente: *Agencia Tributaria de España*

Catálogo de datos abiertos de la Agencia de Ingresos de Canadá

Algunos ejemplos de datos abiertos disponibles en la Agencia de Ingresos de Canadá son:

1. *Estadísticas del T2 sobre investigación científica corporativa y desarrollo experimental: proporcionan información clave sobre los impuestos y la contabilidad al 31 de marzo de 2024. Estas tablas incluyen datos selectos de todas las declaraciones T2 de corporaciones que fueron evaluadas o reevaluadas, y cubren los años fiscales que concluyeron entre 2015 y 2021. La información brinda detalle sobre el impacto y la implementación de los créditos fiscales.*
2. *Cumplimiento de presentación del T1 edición 2024: brinda datos sobre las declaraciones que fueron presentadas tarde o a tiempo. Las declaraciones se agrupan según características demográficas, geográficas y económicas.*
3. *Estadísticas individuales de Impuestos por Área (ITSA): presentan información sobre el impuesto sobre la renta personal basada en áreas geográficas. Las estadísticas están compiladas por provincia y territorio, así como para todo Canadá. Las tablas proporcionan estadísticas sobre ingresos e impuestos según áreas geográficas específicas, clasificación del estado fiscal, clase de ingresos totales, clase de fuente de ingresos y género.*

***Fuente**: Agencia de Ingresos de Canadá*

8. Gobernanza de datos en las administraciones tributarias

Las administraciones tributarias han experimentado un notable incremento en la disponibilidad de sus datos, tanto en volumen como en variedad de formatos. Este aumento se explica por diferentes factores entre ellos la transformación digital que ha revolucionado la recolección de datos; el crecimiento exponencial en la capacidad de procesamiento y almacenamiento; la expansión de las redes de comunicaciones; y el acceso generalizado a Internet de banda ancha, entre otros.

Evolución de las administraciones tributarias en la OCDE:

- *De 2014 a 2019, las tasas promedio de presentación electrónica han aumentado significativamente entre un 13% y un 18%.*
- *Más del 80% de los pagos (por valor y número) se realizan electrónicamente.*
- *Cerca del 50% de las administraciones tributarias precargan las declaraciones de impuestos personales (PIT) con gastos deducibles específicos.*
- *Las nuevas fuentes de datos permiten que la precarga se extienda a las declaraciones de IVA (Impuesto sobre el Valor Agregado) y de impuesto sobre sociedades (CIT).*
- *Un número creciente de administraciones tributarias utiliza asistentes virtuales para responder consultas de los contribuyentes y apoyar el autoservicio.*
- *Utilizan inteligencia artificial en servicios que apoyan a los contribuyentes y funcionarios fiscales.*
- *El porcentaje de administraciones tributarias que permiten el registro en línea de los contribuyentes ha aumentado del 70% en 2015 al 97% en 2019.*
- *Con la creciente disponibilidad de datos, el enfoque del trabajo de cumplimiento puede cambiar hacia la prevención.*

Fuente: *CIAT (2022)*

En el actual contexto de creciente volumen de datos digitales y su reconocida importancia como activos críticos para la toma de decisiones, las estrategias que permitan gestionar y aprovechar estos datos de manera integral han tomado cada vez mayor relevancia. Estas estrategias generalmente se les conoce como gobernanza de datos.

DAMA International define la gobernanza de datos como "el ejercicio de autoridad y control (planificación, monitoreo y aplicación) sobre la gestión de datos como activos"[59]. En este contexto, un programa de gobernanza de datos tiene la tarea de formular políticas y procedimientos que promuevan prácticas de gestión de datos en todos los niveles organizativos, con el objetivo de optimizar su aprovechamiento al máximo. CIAT (2022) complementa esta definición indicando que la gobernanza de datos debe asegurar la confidencialidad, disponibilidad, calidad e integridad de los datos, fortaleciendo además los marcos legales de protección y cumplimiento[60].

La gobernanza de datos también puede apoyarse en herramientas tecnológicas, como los sistemas de gestión de datos maestros (MDM) o plataformas de inteligencia de negocios, que permiten una mejor gestión, análisis y control de la información. Un ejemplo destacado es el de Estonia, que ha implementado una estrategia de gobernanza de datos que integra sistemas de verificación cruzada automática entre diferentes agencias, lo que mejora la eficiencia y minimiza los errores humanos.

8.1. Elementos mínimos en una estrategia de gobernanza de datos para Administraciones Tributarias (AT)

En 2022, el CIAT publicó en inglés la guía práctica "Gobierno de Datos para las Administraciones Tributarias"[61], que proporciona un marco detallado sobre cómo las administraciones pueden lograr una gestión efectiva de sus datos y transformarse en organizaciones impulsadas por los mismos. La guía incluye un modelo de gobernanza ajustable para administraciones tributarias, diseñado como un punto de partida que puede ser evaluado y adaptado según las necesidades específicas de cada entidad. La siguiente sección toma como referencia los elementos clave que el CIAT recomienda para una estrategia de gobernanza:

[59] Sebastian-Coleman, L. (2018) "Navigating the labyrinth: An executive guide to data management" (1st ed.). Technics Publications.

[60] A diferencia de la gestión de datos que busca valor de estos activos, la gobernanza de datos se enfoca en cómo se toman decisiones sobre ellos y en cómo las personas y procesos deben comportarse al respecto.

[61] En 2024 se publicó la traducción de la guía a español y se encuentra disponible en el siguiente enlace: https://www.ciat.org/Biblioteca/DocumentosTecnicos/Espanol/2024_gobierno_datos.pdf

a) Principios y políticas: Analiza los principios de gobernanza de datos que facilitan la colaboración entre las partes interesadas para alcanzar objetivos comunes. Si bien, cada administración tributaria debe identificar las políticas de datos más adecuadas para su contexto, el CIAT propone los siguientes 5 principios.

Principio 1: Datos como activos de la administración tributaria • **Declaración:** Los datos son un recurso y activo de la administración tributaria. • **Justificación:** La administración tributaria requiere el uso de datos para garantizar el control de cumplimiento y diseñar servicios personalizados. • **Implicación:** Asegurar el tratamiento y la calidad de los datos como un recurso valioso en todo su ciclo dentro de la administración tributaria.	**Principio 2: Privacidad y protección de datos** • **Declaración:** Promover el cumplimiento de la privacidad de los datos de los contribuyentes siguiendo leyes y regulaciones. • **Justificación:** Los datos de los contribuyentes y de la administración tributaria deben ser tratados según lo dictan las leyes tributarias, de transparencia y protección de datos. • **Implicación:** Garantizar el cumplimiento de las leyes tributarias y de protección de datos; los datos no deben ser utilizados para otros fines distintos a los especificados.
Principio 3: Transparencia en la gestión • **Declaración:** La gestión de datos debe mostrar transparencia en toda la administración tributaria. • **Justificación:** Las actividades de gestión de datos deben ser transparentes para las diferentes partes interesadas. • **Implicación:** Proporcionar evidencia clara y precisa de las actividades de gestión de datos, controles utilizados, tratamiento de datos, definiciones, modelos y procesos.	**Principio 4: Control y auditorías en la gestión** • **Declaración:** La gestión de datos (y gobernanza) debe ser susceptible a auditoría y control. • **Justificación:** Las decisiones, procesos y controles relacionados con la gestión de datos deben ser auditables y documentar evidencias que respalden su cumplimiento. • Implicación: Formalizar los procesos y modelos operativos, asegurando evidencia de cumplimiento.
Principio 5: Responsabilidad y gestión de datos • **Declaración:** Para gobernar los datos, la administración tributaria debe definir los límites de responsabilidad de los actores en la gestión y gobernanza de los datos. • **Justificación:** Para la gobernanza de datos, es fundamental mantener las responsabilidades y el modelo de administración de manera clara y precisa. • **Implicación:** Ajustar los procesos de gestión, estructuras organizativas adecuadas para gestionar correctamente los datos, e integrar prácticas de gestión en la administración tributaria.	

Fuente: CIAT (2022)

b) Capacidades: Establece las competencias fundamentales que una administración fiscal debe desarrollar para garantizar una práctica efectiva de gobierno de datos. Cuando una AT adopta la gobernanza de datos

por primera vez, es recomendable concentrarse en el desarrollo de capacidades básicas, por ejemplo, definir el alcance y alineación de la estrategia de datos dentro de la administración tributaria, así como asegurar un compromiso con la estrategia a nivel directivo. Una vez establecidas estas capacidades, pueden incorporarse capacidades intermedias, por ejemplo, la gestión de metadatos, la gestión de riesgos y el control de calidad de los datos, entre otros. Finalmente se pueden contemplar capacidades avanzadas, como la gestión de valoración de datos. Si bien estas son recomendaciones, la administración puede ajustar su desarrollo según sus necesidades particulares.

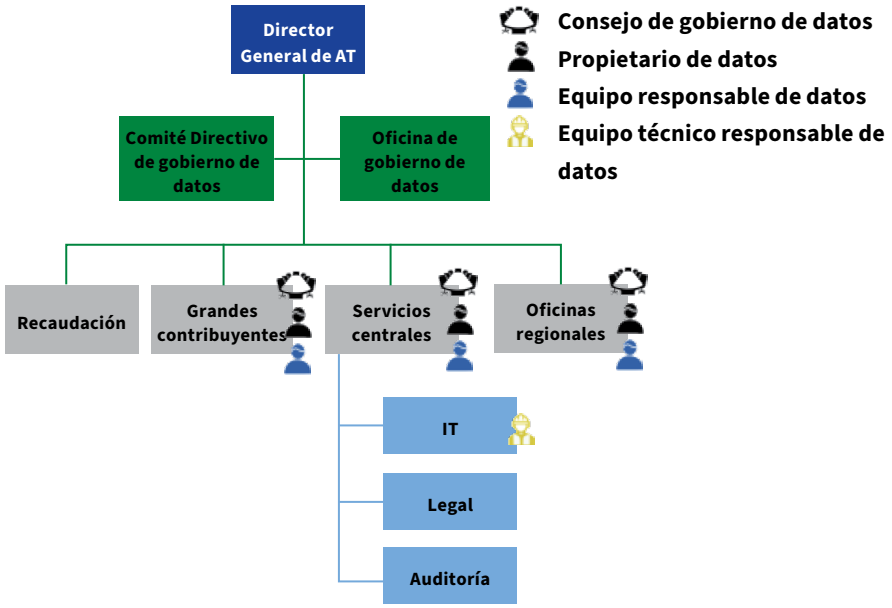
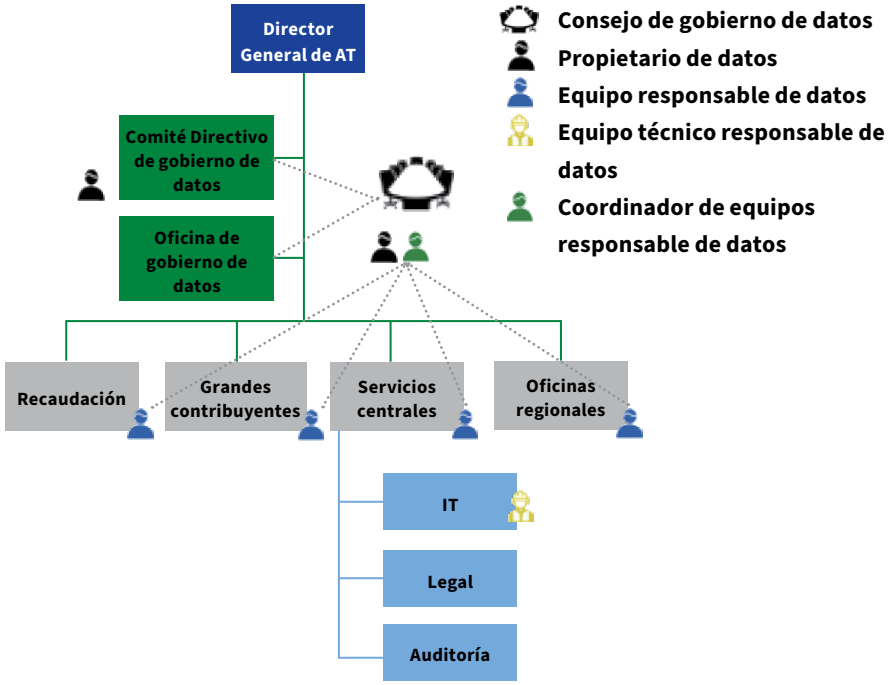
c) **Estructura organizativa, roles y responsabilidades:** Según las necesidades y recursos humanos disponibles de la AT, se recomienda una estructura que permita optimizar la gestión de datos dentro de la entidad, asegurando una dirección estratégica sólida y un cumplimiento efectivo de las políticas de gobernanza de datos. Por ejemplo:

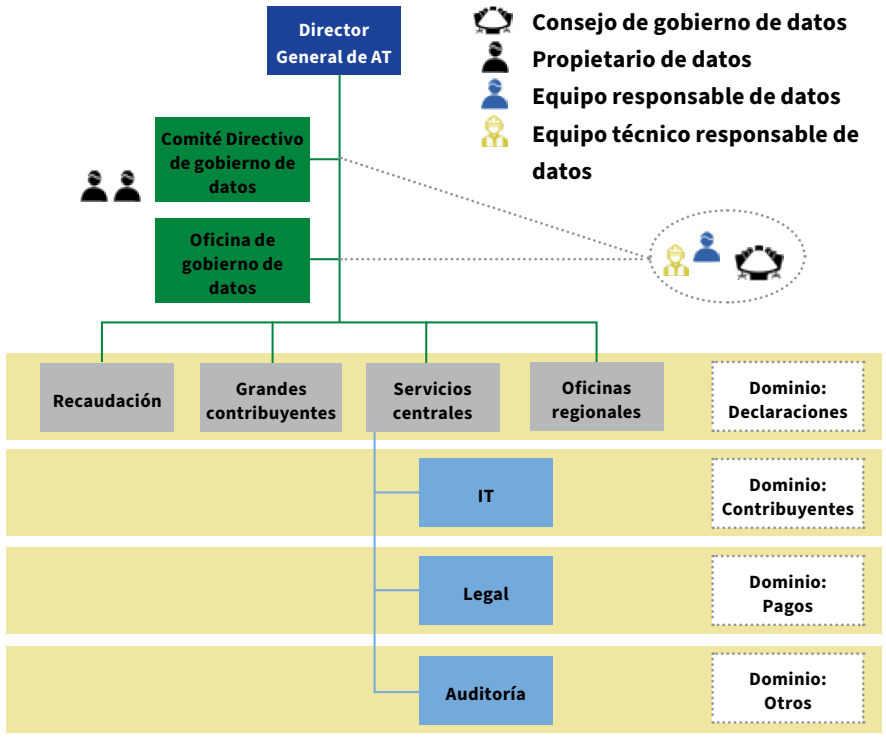
Comité directivo de gobierno de datos	Este es el principal órgano dentro de la administración tributaria. Se conforma por ejecutivos de alto nivel responsables de procesos intensivos en datos, por ejemplo, el director de datos o gerente de gobierno de datos, y los propietarios/encargados de los datos. Este comité tiene la responsabilidad primordial de definir estrategias, aprobar presupuestos y priorizar decisiones estratégicas relacionadas con la gestión de datos. Además, colabora con otros órganos de alto nivel y resuelve problemas organizativos vinculados a los datos.
Consejo de gobierno de datos	Este cuerpo es responsable de las actividades de gestión y gobernanza de datos, así como de manejar problemas o incidentes relacionados con los datos. Está integrado por el Gerente de Gobierno de Datos, Custodios de Datos, y Arquitectos de Datos. El consejo colabora con diversas partes interesadas para definir y abordar problemas de datos, resolver conflictos iniciales y gestionar mejoras potenciales a lo largo del ciclo de los datos de la administración tributaria. Asegura también la implementación efectiva de las políticas de gestión y gobernanza de datos en coordinación con la Oficina de Gobierno de Datos, alineando los esfuerzos con la estrategia de datos y los objetivos tributarios.
Oficina de gobierno de datos	Esta unidad es responsable de liderar las definiciones, control y estándares de gestión de datos en la administración tributaria, fomentando la documentación, comunicación y cumplimiento de las políticas de datos. En administraciones tributarias pequeñas donde una unidad independiente no es viable, se recomienda compartir esta función fuera de la estructura de TI. Las principales responsabilidades de la Oficina incluyen documentar, apoyar, publicar y liderar las actividades y decisiones del Comité Directivo y el Consejo de Gobierno de Datos.

Fuente: CIAT (2022)

d) **Organización de gobernanza de datos:** Es esencial evaluar cómo integrar la gobernanza de datos en la estructura organizacional de una administración tributaria para articular y asignar responsabilidades. CIAT propone tres modelos principales (i) el funcional, (ii) por tipo de contribuyentes (por ejemplo,

grandes contribuyentes, pequeñas y medianas empresas, individuos, etc.), y (iii) un modelo mixto que combina ambos enfoques. Independientemente del modelo elegido, es crucial establecer políticas sólidas de datos y asegurar la coordinación entre los Propietarios de Datos y los Custodios de Datos en diversos departamentos, posiblemente con el respaldo de Consejos Intermedios de Gobierno de Datos.

<table>
<tr>
<td> 
</td>
<td>En administraciones tributarias grandes puede ser beneficioso establecer coordinación entre los Consejos de Gobernanza de Datos y la Oficina de Gobernanza de Datos. Designar un Propietario de Datos único puede ayudar a gestionar eficientemente los datos compartidos entre múltiples partes interesadas. Los Administradores Técnicos de Datos (equipo técnico responsable de los datos) están centralizados en TI. Además, el cumplimiento normativo es cada vez más importante, requiriendo agentes específicos en áreas de negocio de las instituciones tributarias.</td>
</tr>
<tr>
<td> 
</td>
<td>En administraciones tributarias puede ser útil contar con tres entidades clave: el Comité Directivo de Gobernanza de Datos, el Consejo de Gobernanza de Datos y la Oficina de Gobernanza de Datos. El Consejo centraliza los esfuerzos tácticos al reunir propietarios y administradores de datos para gestionar las necesidades de gobernanza, mientras que la Oficina coordina las ejecuciones operativas y participa activamente en las sesiones del Comité Directivo y del Consejo de a través de su líder designado.</td>
</tr>
</table>



En otras administraciones tributarias se puede optar por un enfoque basado en los dominios de datos específicos de la administración tributaria. Los Administradores de Datos de cada dominio participan en el consejo de gobernanza de datos (por ejemplo, el Administrador de Datos de Grandes Contribuyentes). Los Administradores Técnicos de Datos pueden también participar si es necesario según la organización o los administradores de datos.

Fuente: CIAT (2022) y CIAT (2024)

e) **Modelo ligero de gobernanza:** Cuando una administración tributaria tiene el objetivo de incorporar poco a poco la gobernanza de datos, a menudo no es práctico cambiar su estructura organizativa. Un enfoque ligero podría distribuir responsabilidades entre unidades existentes o cuerpos colegiados. Por ejemplo, el control y cumplimiento podría estar a cargo de la unidad de control interno, las definiciones tecnológicas podrían estar a cargo del departamento de TI, mientras que la calidad de datos le correspondería al consejo de gobernanza de datos, y la estrategia al comité estratégico. Esto no solo optimiza recursos, sino que también fomenta una cultura de gestión de datos y mejora la alfabetización en datos en toda la organización. Este modelo, aunque provisional, requiere un consejo de gobernanza de datos como mínimo, que puede empezar como equipo de proyecto. Se recomienda eventualmente evolucionar hacia una estructura más robusta de gestión de datos, iniciando con la formalización de una Oficina de Gobernanza de Datos.

f) **Gestión de datos:** La gestión incluye principalmente a los gestores de datos del área funcional y a los gestores técnicos de datos del lado de TI. Se encarga de manejar los datos de manera responsable, consistente y confiable. Se recomienda los siguientes roles:

Gestores de datos	Responsabilidades
Oficial de gobernanza de datos	• Diseñar y proponer la estrategia de datos al Comité Directivo de Gobernanza de Datos para su aprobación. • Definir y supervisar programas de gobernanza de datos. • Nombrar miembros del Comité Directivo y del Consejo de Gobernanza de Datos. • Liderar y coordinar decisiones de ambos cuerpos. • Facilitar la identificación y satisfacción de necesidades de datos. • Impulsar mejoras continuas en el modelo de gobernanza de datos. • Integrar el modelo de gobernanza con otros modelos de gestión. • Desarrollar y comunicar productos de gobernanza de datos. • Promover prácticas de gestión de datos dentro y fuera de la organización.
Propietario de datos	• Aprobar definiciones de atributos/elementos de datos. • Definir dimensiones de calidad de datos y umbrales aceptables. • Garantizar la calidad y definiciones de datos en su dominio. • Liderar cambios necesarios de datos. • Supervisar acciones de remediación y corrección de datos. • Autorizar el acceso y envío de datos conforme a políticas de seguridad y privacidad. • Responsable de datos compartidos con otras instituciones. • Participar activamente en el Consejo de Gobernanza de Datos según necesidades del Comité Directivo.
Gestor de datos funcional	• Ejecutar o coordinar planes de acción para mejorar la calidad de los datos. • Coordinar esfuerzos para identificar y abordar las causas de problemas de calidad de datos. • Apoyar al Propietario de Datos en definiciones relacionadas con datos en su dominio, como fuentes autorizadas y reglas de calidad. • Colaborar en la definición de clasificaciones de datos y conceptos dentro de su área.
Custodio de datos o gestor técnico de datos	• Apoyar a los gestores funcionales de datos con información, con la extracción, transformación y carga de datos (ETL por sus siglas en inglés), y la inteligencia empresarial (BI por sus siglas en inglés), etc. • Ejecutar o apoyar mejoras de calidad de datos y fuentes de datos. Este rol, generalmente ubicado en áreas de TI.

Fuente: CIAT (2022)

g) **Dimensiones de calidad de datos:** Las dimensiones permiten monitorear y mejorar la calidad mediante el establecimiento de umbrales mínimos de tolerancia. La selección de estas dimensiones debe basarse en las características que mejor representen la situación actual de la administración tributaria, con el objetivo de identificar sus prioridades. A continuación, se presenta un resumen de las diferentes dimensiones adoptadas en calidad de datos:

Dimensión de calidad	Definición
Exactitud	Grado en el que los datos representan el verdadero valor del atributo deseado en un contexto específico. Por ejemplo, si la dirección registrada de un contribuyente es precisa.
Completitud	Grado en el que los datos asociados tienen valor para todos los atributos definidos. Por ejemplo, si todas las obligaciones fiscales de los contribuyentes fueron completadas.
Consistencia	Grado de coherencia con otros datos existentes, eliminando contradicciones. Por ejemplo, una empresa cerrada o una persona fallecida no debería presentar declaraciones de impuestos.
Integridad	Grado de precisión y consistencia de los datos. Asegura que los datos sean precisos y completos. Por ejemplo, si un representante legal identificado por un contribuyente está registrado.
Razonabilidad	Grado en el cual los datos son lógicos y se ajustan a las expectativas razonables.
Oportunidad	Grado en el cual los datos están actualizados y disponibles dentro del período de tiempo requerido para su uso. Por ejemplo, la llegada en tiempo real de datos de facturas electrónicas a la administración tributaria.
Unicidad	Grado en el cual los datos no se repiten innecesariamente. Por ejemplo, asegura que ninguna entidad exista más de una vez en el conjunto de datos, garantizando que cada entidad única tenga un valor crítico único dentro del conjunto.
Validez	Grado en el cual los datos cumplen con las reglas y definiciones establecidas para un propósito específico. Por ejemplo, Esto incluye tipos de datos, formatos y precisión esperados, válidos dentro de un período específico, como la representación uniforme de fechas.

Fuente: CIAT (2022) y DAMA

Aunque esta lista no es exhaustiva, puede servir como guía inicial para desarrollar una estrategia de calidad de datos. Sin embargo, es recomendable que cada administración tributaria evalúe sus principales problemas de calidad de datos y establezca prioridades para abordarlos.

8.2. Generación de datos de calidad

En los últimos años, organizaciones como la OCDE, el Banco Mundial, el Banco Interamericano de Desarrollo (BID) y el CIAT han desarrollado herramientas y manuales específicamente diseñados para fortalecer a las administraciones tributarias. Estas herramientas están dirigidas a facilitar una mejora significativa en términos de tecnología, modernización y adopción de buenas prácticas internacionales. Uno de estos instrumentos son los modelos de madurez, ampliamente utilizados en procesos de autoevaluación para medir las capacidades actuales en áreas funcionales, estratégicas u organizativas específicas. Estos modelos establecen diferentes niveles y criterios de madurez con el objetivo de proporcionar una visión común sobre los cambios necesarios que una organización debe implementar para alcanzar niveles superiores de desarrollo en el futuro, si así lo decide.

En 2022, la OCDE publicó el Modelo de Madurez de Análisis de Datos, el cual abarca dos perspectivas fundamentales: la estratégica y la operativa. Desde la perspectiva estratégica se evalúan los siguientes atributos:

a) **Estrategia de capacidades analíticas**: evalúa si la administración tributaria cuenta con una estrategia general que abarca toda la administración y si esta se formuló con la colaboración de grupos de interés externos.

b) **Gobernanza**: analiza si la AT cuenta con una junta de gobernanza de datos en la cual participan miembros externos a fin de garantizar la armonización entre los procesos analíticos de la administración y aquellos que utilizan otros entes gubernamentales y los contribuyentes.

c) **Cultura**: mide si la administración cuenta con una cultura organizativa que fomenta la innovación y formación continua, en la que todos los niveles de la organización comprenden y buscan oportunidades para aplicar el análisis de datos, asegurando así la optimización del sistema tributario.

d) **Presupuesto:** examina si el proceso de planificación presupuestario para la inversión y gasto en analítica está completamente integrado en los procesos de presupuestación de toda la administración.

La segunda perspectiva, la operativa, se enfoca en analizar cómo la dirección y el personal de la administración apoyan el desarrollo de la estrategia y el marco de gobernanza. Específicamente, se enfoca en evaluar los siguientes atributos:

a) **Tecnológicos (infraestructura informática):** evalúa si se dispone de una infraestructura informática integral para los servicios analíticos, incluyendo la existencia de un repositorio centralizado para la exploración de datos en la mayoría de los sistemas.

b) **Gestión de datos:** evalúa cómo se manejan los datos a lo largo del tiempo, desde la recolección hasta el análisis y la utilización.

c) **Gestión del talento:** analiza cómo se gestiona y desarrolla el capital humano, utilizando un enfoque estructurado para medir la efectividad y la evolución de las prácticas de gestión de talento.

d) **Retroalimentación:** mide la capacidad de las AT para utilizar los datos y los resultados de sus análisis de manera efectiva para mejorar continuamente sus procesos y decisiones.

e) **Gestión de proyectos:** examina la capacidad de las AT para planificar, ejecutar y controlar iniciativas de análisis de datos de manera efectiva. Esto incluye la habilidad de definir claramente los objetivos del proyecto, asignar recursos adecuados, y establecer planes detallados para guiar la ejecución.

f) **Capacidades analíticas:** evalúa las habilidades de la AT para recolectar, procesar, interpretar y utilizar datos de manera efectiva con el fin de tomar decisiones informadas.

g) **Ámbitos de uso:** analiza qué tanto se integra el análisis de datos en la toma de decisiones.

A través de los siguientes cinco niveles de madurez se evalúa cada perspectiva y cada atributo:

a) **Incipiente:** Este nivel describe a las administraciones tributarias que han comenzado a avanzar en analítica, pero aún tienen mucho camino por recorrer. En esta etapa, se enfatizan los logros alcanzados y se reconocen posibles limitaciones.

b) **En progreso:** Aquí se encuentran las administraciones tributarias que han implementado o están implementando reformas en analítica para acercarse al nivel promedio de las administraciones avanzadas.

c) **Consolidado:** Este nivel es típicamente alcanzado por las administraciones tributarias avanzadas, como los miembros del Foro de Administración Tributaria.

d) **Destacado:** Representa el nivel más avanzado actualmente posible mediante acciones propias de la administración tributaria.

e) **Ambicionado:** En este nivel se considera lo que podría lograrse a mediano plazo, a medida que se adoptan nuevas tecnologías y se avanza hacia una administración tributaria más eficiente. Se reconoce que alcanzar este nivel de manera uniforme puede ser difícil debido a la necesidad de cooperación con actores externos y otros desafíos globales.

Siguiendo el modelo de la OCDE (2022) el cuadro a continuación detalla los atributos indicativos y sus medios de verificación según el nivel de madurez en generación de datos de calidad y capacidades analíticas:

Atributo	Medio de verificación
Digitalización	• **Incipiente:** no se ha digitalizado un número importante de fuentes de datos y las fuentes digitalizadas se mantienen en sistemas independientes. • **En proceso:** la mayoría de las fuentes están digitalizadas y algunos datos centralizados. • **Consolidado:** todas las fuentes importantes están digitalizadas y existe un repositorio central para la mayoría de los datos. • **Destacado:** existe acceso a una amplia gama de fuentes y datos no estructurados. • **Ambicionado:** existe un repositorio integral compartido con otros organismos que cuenta con acceso casi en tiempo real a datos de terceros.
Ontología y metadatos[62]	• **Incipiente:** falta una ontología común y procesos para crear y mantener metadatos. • **En proceso:** existe conciencia de la necesidad de una ontología común, pero no se implementa regularmente y si bien existe un intento de crear metadatos es incoherente. • **Consolidado:** se implementa una ontología común y existen procesos establecidos para crear y mantener metadatos. • **Destacado:** existe automatización avanzada en el mantenimiento de ontología y metadatos e integración con herramientas analíticas avanzadas. • **Ambicionado:** existe automatización completa en mantenimiento de ontología y traducción de reglas e integración total con herramientas analíticas.
Calidad de datos	• **Incipiente:** escasa conciencia sobre la importancia de la calidad de los datos, y documentación limitada, con errores y valores faltantes frecuentes. • **En proceso:** algunas partes de la organización comprenden la importancia de la calidad de los datos y hay un control de calidad parcialmente automatizado. • **Consolidado:** existe una comprensión generalizada sobre la importancia de la calidad de los datos, hay controles automatizados y se llevan a cabo ejercicios de corrección de errores, aunque en su mayoría manual. • **Destacado:** control de calidad y corrección de errores altamente automatizados. • **Ambicionado**: control de calidad y corrección de errores completamente automatizados en tiempo real.

[62] **Ontología** se refiere a una visión integral de los conceptos, términos y estructuras comunes (metadatos) empleados en la administración tributaria. Por ejemplo, en este ámbito, tanto los funcionarios como los sistemas informáticos deberían adoptar una única definición de “contribuyente”, estableciendo así la ontología correspondiente. **Metadatos** se refiere datos adicionales que describen características esenciales de los elementos de los datos. Estos pueden abarcar detalles estructurales como el tipo de dato y el número de registros; aspectos de calidad que incluyen reglas de validación, calidad de los datos y densidad de la información; así como aspectos relacionales que indican la posible integración con datos de otros sistemas.

Gestión del talento	• **Incipiente:** la formación de analistas se da a través de tutorías y autoaprendizaje y hay faltante de programas estructurados de desarrollo. • **En progreso:** planes de carrera de analistas poco claros, lo que dificulta la retención de talento, y mínima facilitación de formación y fomento del desarrollo de competencias. • **Consolidado:** selección de analistas mediante proceso específico, priorización creciente de competencias analíticas en procesos de selección y hay organización de redes profesionales de analistas para intercambio de habilidades. • **Destacado:** planes de carrera definidos, establecimiento de vínculos con universidades con entendimiento claro de competencias necesarias, y apoyo y formación estructurada que fomenta el aprendizaje autodirigido en tecnologías avanzadas. • **Ambicionado:** se ofrecen oportunidades hasta niveles directivos, hay estrecha colaboración con universidades para el diseño de planes de carrera en sector público y oferta continua de cursos profesionales y aprendizaje en diversos ámbitos.
Retroalimentación	• **Incipiente:** se da una evaluación esporádica de los resultados del análisis de datos, las opiniones de los usuarios se recogen de manera informal y circunstancial y el aprendizaje no se documenta ni se aplica en proyectos futuros de manera sistemática. • **En progreso:** se da una evaluación de resultados al finalizar los proyectos, aunque no de manera sistemática y se da la retroalimentación formal de usuarios, aunque no siempre se aplica en proyectos futuros. • **Consolidado:** los usuarios prueban y revisan resultados durante el desarrollo del análisis de datos, la retroalimentación se considera esencial y aplicada para mejorar proyectos futuros y las lecciones aprendidas formalmente se documentan y son y utilizadas para mejoras futuras. • **Destacado:** los resultados son evaluados según protocolos predefinidos y de forma periódica, hay retroalimentación cuantitativa y cualitativa exhaustiva y estructurada de cada proyecto, los resultados son utilizados sistemáticamente para mejorar proyectos futuros y hay una revisión externa de expertos. • **Ambicionado:** se usa inteligencia artificial para separar efectos de la analítica de otros factores, hay supervisión continua en tiempo real de modelos analíticos, y las recomendaciones son incorporadas según la supervisión continua.
Gestión de proyectos	• **Incipiente:** proyectos analíticos gestionados de manera independiente según las capacidades individuales de los analistas, con pocos procesos formales. • **En progreso:** algunos proyectos involucran a usuarios operativos, aunque la participación es intermitente debido a recursos limitados. • **Consolidado:** los usuarios operativos son involucrados reactivamente en proyectos analíticos. • **Destacado:** usuarios operativos están completamente integrados en proyectos analíticos avanzados, aportando ideas y asegurando que los resultados cumplan con necesidades operativas específicas.

	• **Ambicionado:** equipos multidisciplinarios de usuarios operativos, expertos en gestión de proyectos y analistas trabajan conjuntamente. Procesos rigurosos abarcan aplicaciones analíticas avanzadas como inteligencia artificial y despliegue en tiempo real, validados y revisados periódicamente de manera comparativa con organizaciones líderes externas.
Capacidades analíticas	• **Incipiente:** análisis de datos basados en hipótesis limitadas, lo que puede llevar a conclusiones incorrectas. Los analistas tienen habilidades básicas en manejo y visualización de datos, pero carecen de metodologías estadísticas avanzadas. • **En progreso:** combina análisis basados en hipótesis, exploración de datos y modelización básica, permitiendo descubrir patrones desconocidos. Los analistas avanzados poseen habilidades de modelización y comprensión del sistema tributario. • **Consolidado:** se enfoca en exploración de datos y modelización con técnicas estadísticas variadas. Los analistas realizan pruebas sistemáticas de precisión y utilizan métodos de validación cruzada. Tienen buen dominio del razonamiento estadístico y capacidades sólidas en manejo y visualización de datos. • **Destacado:** utiliza datos estructurados y no estructurados, *big data* y técnicas estadísticas avanzadas como aprendizaje automático e inteligencia artificial. Los analistas avanzados son expertos en razonamiento estadístico, diversas técnicas de modelización y visualización de datos. • **Ambicionado:** implementa un conjunto completo de herramientas para visualización de datos, procesamiento del lenguaje natural y aprendizaje automático. Todos los analistas tienen un profundo conocimiento de técnicas avanzadas y aplicaciones estadísticas para resolver problemas operativos complejos.
Ámbitos de uso	• **Incipiente:** Limitaciones en el uso de la analítica y adaptación parcial al entorno cambiante de la administración tributaria. • **En progreso:** algunos departamentos utilizan analistas de datos para combinar fuentes de datos y apoyar el cumplimiento de los cometidos tributarios, como evaluar perfiles de riesgo y descubrir anomalías graves. • **Consolidado:** utilización de análisis de datos sofisticados para detectar anomalías, riesgos y problemas potenciales relacionados con la legislación tributaria, con creciente automatización para identificar cuestiones que requieren investigación adicional. • **Destacado:** integración de la analítica en una amplia gama de procesos dentro de la administración tributaria, apoyada cada vez más por aplicaciones de inteligencia artificial para identificar problemas y recomendar acciones automáticas o manuales. • **Ambicionado:** la analítica de datos está completamente integrada en los sistemas naturales de los contribuyentes, simplificando el cumplimiento y reduciendo costos tanto para la administración tributaria como para los contribuyentes.

Fuente: OCDE (2022)

Invertir en la calidad de los datos es clave para que las entidades cumplan su misión de manera efectiva y eficiente. Aunque muchas de las administraciones tributarias más avanzadas tecnológicamente reconocen la importancia de contar con datos de alta calidad, especialmente en el contexto del Big Data; pocas de las menos desarrolladas tecnológicamente han tomado medidas concretas para asegurar la calidad de los datos que reciben.

Desafíos e implicaciones que acompañan la baja calidad de la información:

1. Duplicación de datos: *Es un problema común en administraciones tributarias debido a la falta de estandarización en los formatos de datos. Para mitigarlo, es imprescindible utilizar herramientas especializadas en la duplicación de datos. Estas soluciones han evolucionado significativamente y ahora tienen la capacidad de detectar incluso entradas notablemente diferentes pertenecientes al mismo contribuyente.*

2. Formatos inconsistentes: *Los sistemas enfrentan dificultades cuando existen variedad de formatos de datos, como en fechas, números de identificación fiscal y direcciones. Para abordar este desafío, es crucial establecer directrices claras para la entrada de información y respaldarlas con reglas de validación que garanticen la consistencia de los datos.*

3. Información incompleta: *Es un problema significativo para herramientas analíticas y algoritmos cuando los datos se introducen de manera incompleta, vaga o inconsistente. Implementar reglas de validación constituye una solución efectiva para asegurar que no se generen registros a menos que se incluya toda la información esencial.*

4. Unidades e idiomas múltiples: *Son un desafío significativo, especialmente cuando existen diferencias en las unidades de medida y la gestión de caracteres especiales. Es fundamental iniciar definiendo tantos campos como sea posible como identificadores codificados. Por ejemplo, en lugar de permitir campos de texto para ingresar descripciones, es preferible utilizar catálogos previamente definidos. De esta forma la administración puede enfocarse en desarrollar diccionarios de datos que facilite la mejora del análisis y la gestión de la información.*

5. Datos inexactos: *Existe el riesgo de utilizar datos incorrectos en análisis y evaluaciones de riesgos. Estos problemas suelen ser difíciles de detectar, especialmente si el formato es técnicamente aceptable. Por ejemplo, introducir un número de identificación fiscal válido pero incorrecto. Es crucial que la administración siga procedimientos claros y establezca reglas de validación para mejorar la calidad de la información y garantizar el cumplimiento normativo.*

Fuente*: BM y CIAT (2022)*

8.3. Ámbito internacional

Una revisión de los países de la OCDE muestra que países como Australia, Canadá, Reino Unido, entre otros han progresado significativamente en la implementación de marcos legales y estrategias de gobernanza de datos a nivel nacional. Estos marcos están diseñados para asegurar que la gestión de sus datos en todo el gobierno cumpla con rigurosos estándares de seguridad, calidad y eficiencia. En las administraciones tributarias en estos países, la digitalización se ha convertido en un enfoque central, aprovechando tecnologías avanzadas para mejorar la recolección y análisis de datos fiscales. Este enfoque no solo facilita el cumplimiento de las obligaciones fiscales por parte de los contribuyentes, sino que también fortalece la gestión y supervisión por parte de las autoridades tributarias.

Lecciones de Corea del Sur – Proceso de digitalización

El proceso de digitalización en Corea del Sur pasó por dos etapas distintas. Desde 1967 hasta 1996, la Administración Tributaria se enfocó en la automatización de procesos y la informatización de datos existentes mediante la instalación de computadoras y la formación de personal. Si bien estos esfuerzos inicialmente se concentraron en la acumulación de datos y en la construcción de capacidades básicas, a diferencia de la gestión o el análisis sofisticado de datos, sentó las bases para desarrollos posteriores.

Desde finales de los años noventa, la digitalización se intensificó en dos frentes principales. Primero, el gobierno estableció una infraestructura integrada de bases de datos para recopilar, almacenar y analizar datos tributaria. Esto incluyó la digitalización de servicios públicos relacionados con impuestos, como identificación nacional, registro de empresas, emisión de certificados fiscales y presentación de documentos en línea, además de colaboraciones público-privadas para sistemas de facturación electrónica, entre otros. Segundo, la implementación de leyes y regulaciones para detectar transacciones no rastreables y exponer ingresos ocultos, modernizando el intercambio de datos entre instituciones y clarificando beneficios y sanciones. De esta forma se diseñaron esquemas únicos e incentivos para mejorar el cumplimiento tributario en Corea del Sur.

En 2015, la administración tributaria introdujo el Nuevo Sistema Tributario Integrado (NSTI), marcando un avance significativo desde el anterior Sistema Tributario Integrado (STI). El NSTI unificó más de 30 sistemas tributarios fragmentados en un solo sistema cohesivo. Este desarrollo fue impulsado por la necesidad de simplificar la gestión de datos, reducir costos administrativos y mejorar la eficiencia. El NSTI se compone de dos partes principales: el Sistema Nacional Electrónico de Impuestos de Próxima Generación (NGH), diseñado como un portal en línea para los contribuyentes, y un portal interno para la Administración Tributaria que facilita el funcionamiento del NSTI.

***Fuente**: BID (2024)*

Oficina de Impuestos de Australia (ATO, por sus siglas en inglés)

Durante el período de 2019 a 2022, la ATO experimentó un aumento significativo del 16% en las cuentas de deuda y un incremento del 70% en la deuda cobrable debido a las difíciles condiciones económicas generadas por la pandemia de COVID-19. Tras pausar muchas acciones durante la crisis sanitaria, en 2022 la ATO reanudó sus actividades de cobro, implementando mejoras sustanciales en su capacidad analítica. En particular:

1. La ATO mejoró sus modelos analíticos conocidos como Financial Resilience Insights (FRI), lo que permitió una segmentación más precisa de sus clientes y una identificación más exacta de sus activos e ingresos. Además, introdujo dispositivos de Perfil Corporativo del Cliente (ECP) para tener una mejor comprensión de la capacidad financiera de sus contribuyentes. Esta iniciativa permitió que los contribuyentes con una capacidad financiera sólida optaran por pagar en su totalidad o acceder a planes de pago más cortos y óptimos, mientras que aquellos con menos capacidad financiera recibieron apoyo mediante planes de pago más largos y sostenibles, según los análisis realizados.

2. La ATO ajustó la combinación de modelos analíticos para mejorar la precisión en las predicciones y reorientó el enfoque de los modelos que mostraban deterioro en su rendimiento debido a la falta de datos de entrenamiento durante la pausa en las acciones más firmes de cobro.

3. Además, la ATO evaluó las perspectivas de cobro para varios grupos específicos de deudores, buscando optimizar las estrategias de recuperación según las características y riesgos de cada grupo.

Este enfoque detallado en la aplicación de la ciencia de datos y el modelado analítico refleja cómo la ATO respondió a los desafíos económicos derivados de la pandemia, utilizando herramientas avanzadas para adaptar sus estrategias de gestión de deudas y mejorar la eficacia de sus operaciones.

***Fuente**: ATO*

Mejoras en la integridad y calidad de datos en Suecia

Suecia ha tomado varias medidas para mejorar la calidad de los datos relacionados con la administración tributaria:

1. Cumplimiento con el RGPD: La Agencia Tributaria de Suecia (Skatteverket) ha implementado las regulaciones de la Unión Europea sobre protección de datos (RGPD) en sus procesos de procesamiento de datos personales. Esto incluye informar a los contribuyentes sobre sus derechos y cómo se procesan sus datos.

2. Disposiciones especiales para la Agencia Tributaria: Suecia ha establecido reglas adicionales que regulan qué datos puede procesar la Agencia Tributaria, para qué fines y por cuánto tiempo pueden almacenarse los datos. Esto brinda un marco legal sólido para el manejo de datos sensibles.

3. Intercambio de información controlado: La Agencia Tributaria comparte información con otras agencias gubernamentales de manera controlada y limitada a lo estrictamente necesario para fines tributarios, respetando los principios de proporcionalidad y minimización de datos.

4. Uso de analítica de datos: La Agencia Tributaria utiliza cada vez más herramientas de análisis de datos para detectar patrones y mejorar la identificación y coincidencia de datos de contribuyentes.

Fuente: *Skatteverket*

9. Uso de la nube

El uso de la nube ha jugado un rol importante en la transformación digital de las administraciones tributarias al permitir mejorar la capacidad para recibir, almacenar y procesar grandes volúmenes de datos. Como lo define el BID (2020) [63] la computación en la nube abarca más que el simple almacenamiento de información. Se trata de la entrega de servicios bajo demanda por parte de proveedores tecnológicos y se realiza a través de internet o redes privadas.

Los servicios de computación en la nube funcionan de manera similar a un entrono tradicional de TI, su diferencia radica principalmente en cómo se gestiona, mantiene y acceden a los recursos tecnológicos. Los servicios de nube, generalmente se clasifican en tres grupos[64]:

- **Infraestructura como servicio (IaaS por sus siglas en inglés):** los proveedores de servicios en la nube ofrecen a consumidores la oportunidad de alquilar servidores, almacenamiento, redes y otros recursos de infraestructura fundamentales de TI. Aunque el Proveedor del servicio gestiona y controla la infraestructura, el consumidor tiene control sobre los sistemas operativos y el almacenamiento. Por ejemplo, se ofrecen máquinas virtuales, almacenamiento en la nube, redes virtuales privadas entre otros.
- **Plataforma como servicio (PaaS por sus siglas en inglés):** los proveedores de servicios en la nube permiten a los consumidores desplegar aplicaciones propias o adquiridas en la infraestructura de la nube utilizando las herramientas proporcionadas por el proveedor. Aunque el proveedor se encarga de la gestión y el control de la infraestructura, el cliente mantiene el control sobre las aplicaciones implementadas. Por ejemplo, *AWS Lambda*, *Azure App Service* y plataformas "*low-code*"[65] entre otras.
- **Software como servicio (SaaS por sus siglas en inglés):** los proveedores de servicios proporcionan a los consumidores acceso a aplicaciones de software que se ejecutan en la infraestructura de la nube. Estas aplicaciones se pueden utilizar desde diferentes dispositivos cliente a través de interfaces como

[63] Texto disponible en: https://publications.iadb.org/es/publications/spanish/viewer/Computacion-en-la-nube-Contribucion-al-desarrollo-de-ecosistemas-digitales-en-paises-del-Cono-Sur.pdf

[64] Texto disponible en: https://publications.iadb.org/en/publications/english/viewer/Cloud-Computing-Opportunities-and-Challenges-for-Sustainable-Economic-Development-in-Latin-America-and-the-Caribbean.pdf

[65] proporcionan una solución de desarrollo *low-code*, es decir permite a usuarios crear aplicaciones empresariales rápidamente mediante una interfaz gráfica sin necesidad de codificación extensa. Las plataformas más conocidas son *OutSystems, Mendix, Appian* entre otros.

navegadores web o interfaces de programas. El proveedor de la nube maneja la mayoría de los aspectos de la oferta de SaaS, excepto las configuraciones específicas del usuario para las aplicaciones. Por ejemplo, Microsoft 365, Google *Workspace, ServiceNow* entre otros.

Estos servicios se pueden a su vez presentar bajo cuatro modelos de despliegue, que dependen en gran medida en los requerimientos y usos del consumidor.

- **Nube pública:** nube diseñada para que sea de uso abierto para el público. Los usuarios sean individuos, instituciones académicas o empresas pueden contratar el servicio para gestionar y operar la nube, pero la infraestructura existe en las instalaciones del proveedor.
- **Nube privada:** nube diseñada para uso exclusivo de una sola organización o entidad, lo que proporciona mayor control y seguridad. Generalmente esta nube puede estar alojada en las instalaciones de la organización en sitio (*on-premise*) o ser gestionada por un proveedor externo, pero es exclusivamente de esa organización.
- **Nube comunitaria:** la nube se diseña para uso exclusivo de una comunidad o varias organizaciones con un interés en común, únicamente los miembros de esta comunidad son quienes poseen, gestionan y operan la nube.
- **Nube híbrida:** combina dos o más de las infraestructuras anteriores permitiendo la interoperabilidad entre ellas. También puede integrar servicios de centros de cómputo o infraestructura en sitio (*on-premise*).

En la actualidad existen diferentes proveedores de servicios de nube pública con una amplia gama de productos y servicios que se adaptan a diferentes necesidades de infraestructura, desarrollo y software. Por ejemplo, *Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud* entre otros. Cada uno de estos proveedores ofrece servicios clave en computación, almacenamiento, bases de datos, redes y herramientas de desarrollo. Lo que permite que consumidores puedan construir, desplegar y gestionar las aplicaciones necesarias en la nube con las características específicas según sus necesidades. Adicionalmente, estos servidores también permiten crear redes virtuales privadas dentro de la nube pública proporcionando un entorno de red aislado.

9.1. Seguridad en la nube

Como se mencionó anteriormente en la sección seguridad de la información, los estándares internacionales en seguridad informática consisten en una serie de mejores prácticas, directrices y requisitos técnicos

destinados a asegurar la protección de la información en organizaciones y sistemas a nivel global. Su objetivo principal es facilitar la adopción e implementación de medidas robustas de seguridad, resguardar datos confidenciales, gestionar riesgos y garantizar el cumplimiento de regulaciones en diversas jurisdicciones alrededor del mundo. Además de la ISO/IEC-27001, también se cuentan con normas para la seguridad en la nube, específicamente:

- **Norma ISO-27017.-** Establece una serie de recomendaciones y prácticas de seguridad relevantes para el entorno de servicios en la nube, ayudando a las organizaciones a gestionar de manera más eficaz los riesgos asociados con este tipo de tecnología y a proteger sus activos de información en un entorno en constante evolución. La norma busca mejorar la seguridad de la información en la nube mediante la implementación de controles y prácticas específicas, promoviendo una mayor confianza y seguridad tanto para los proveedores como para los clientes de servicios en la nube.
- **Norma ISO-27018.-** proporcionar un marco para la protección de datos personales en servicios de nube pública, para garantizar que los proveedores de servicios en la nube gestionen y protejan adecuadamente la información personal de sus clientes. Esto ayuda a mejorar la confianza en los servicios en la nube y a cumplir con las expectativas y requisitos de privacidad de los usuarios y reguladores. De esta forma se busca asegurar que los datos personales en la nube estén protegidos y gestionados de acuerdo con las mejores prácticas y regulaciones aplicables, promoviendo una mayor seguridad y privacidad en el uso de servicios en la nube.

Adicionalmente, existen los informes de Controles de Sistema y Organización[66] (SOC, por sus siglas en inglés), evaluaciones realizadas por externos e independientes que demuestran cómo un proveedor de servicios en la nube cumple con los controles y objetivos clave de cumplimiento. Estos informes incluyen información sobre los controles internos relacionados con los informes financieros, así como sobre la seguridad del sistema, su disponibilidad y las características de seguridad y documentos de cumplimiento de confidencialidad. La política de seguridad debe requerir que los proveedores presenten documentación que confirme que sus servicios cumplen con las certificaciones de seguridad de terceros.

9.2. Beneficios y desafíos de la nube

Si bien la adopción de servicios en la nube ha simplificado el acceso a tecnologías digitales y ha proporcionado a los gobiernos beneficios tales como la disminución de costos operativos y una mayor

[66] Leer más sobre esto en el siguiente enlace https://publications.iadb.org/es/publications/spanish/viewer/Contratacion-publica-de-servicios-de-computacion-en-la-nube-Mejores-prácticas-para-su-implementacion-en-America-Latina-y-el-Caribe.pdf

eficiencia en la prestación de servicios públicos, también presenta desafíos que se deben gestionar. La transición a la nube, aunque ofrece oportunidades para modernizar y optimizar, también plantea riesgos relacionadas con la seguridad de los datos, la privacidad, y la dependencia de proveedores externos. A continuación, se resumen los principales beneficios y riesgos, identificados a partir de las experiencias de los países de Centroamérica, Panamá y República Dominicana.

Los beneficios sustanciales de la adopción de la nube se resumen en:

- **Ahorro de costos:** la nube evita grandes inversiones iniciales en infraestructura física. En su lugar se adopta un modelo de pago por uso que ajusta los gastos de acuerdo con el consumo real de los recursos en la nube. Este enfoque no solo reduce los costos operativos y de mantenimiento a largo plazo, sino que también permite ajustar el gasto según las necesidades cambiantes de la entidad.
- **Escalabilidad y flexibilidad:** la nube permite a los gobiernos adaptar sus recursos de TI de manera dinámica y ágil para responder a cambios en la demanda sin la necesidad de realizar inversiones adicionales en infraestructura física. Esta capacidad de escalabilidad asegura que los recursos estén disponibles según las necesidades específicas, ya sea en momentos de alta demanda o durante periodos de menor actividad, optimizando así el rendimiento y la eficiencia operativa.
- **Acceso a tecnologías emergentes y herramientas avanzadas:** la nube facilita el acceso a tecnologías emergentes y herramientas avanzadas, promoviendo la innovación continua. Esto permite a los gobiernos optimizar la eficiencia operativa y mejorar la calidad del servicio.
- **Seguridad mejorada:** los proveedores de servicios en la nube ofrecen acceso a una amplia gama de expertos y herramientas de ciberseguridad, garantizando una protección robusta a la información. La infraestructura de nube está equipada con medidas avanzadas de seguridad, que incluyen cifrado, monitoreo continuo y controles de acceso, entre otros.

Algunos de los principales desafíos para la migración del gobierno hacia la nube son:

- **Restricciones legales:** en algunos países la regulación no permite que datos de la administración central o información crítica del Estado pueda ser transferida hacia otras jurisdicciones. Es decir, la información debe ser alojada en territorio nacional, impidiendo que sea gestionada por proveedores de servicios de nube.
- **Restricciones presupuestarias:** en algunos países se puede complicar el uso de contratos abiertos o multianuales, que implican pagos variables, como ocurre con los modelos de servicios en la nube basados en pago por uso o por demanda. Estas normativas suelen clasificar el gasto en tecnología como una inversión, dejando pocas opciones para tratar estos gastos como parte del presupuesto corriente.

- **Infraestructura requerida para servicios en la nube:** para el uso efectivo de servicios en la nube, los países requieren redes de banda ancha de alta velocidad, un suministro de energía fiable y constante entre otros. Estos elementos son fundamentales para que los proveedores de servicios en la nube puedan ofrecer sus servicios de manera eficiente y confiable.
- **Falta de conocimiento y capacidades internas:** muchas dependencias gubernamentales no cuentan con el conocimiento necesario sobre el funcionamiento de los servicios en la nube ni con las capacidades requeridas para gestionar infraestructura virtual, reestructurar procesos, adaptarse a soluciones no propietarias y administrar contratos de outsourcing.
- **Seguridad, protección y privacidad de datos:** aunque los proveedores de servicios generalmente garantizan una mayor seguridad en la nube, la protección y privacidad de los datos es una responsabilidad compartida entre los controladores de datos (también conocidos como usuarios) y los procesadores de datos. Los controladores de datos deben implementar medidas técnicas y organizativas adecuadas para proteger los datos personales contra la destrucción ilegal, pérdida accidental, alteración o divulgación no autorizada. Además, deben seleccionar procesadores que ofrezcan suficientes medidas de seguridad. Los usuarios de servicios en la nube pueden usar cifrado para proteger aún más sus datos, asegurando que solo las entidades con las claves de cifrado puedan acceder a la información.

9.3. Aspectos por considerar en la migración a servicios de la nube

En 2023 el Banco Mundial publicó un marco de evaluación de la nube[67] que proporciona un listado de recomendaciones clave para entidades responsables de la adquisición de estos servicios. Este marco ofrece prácticas valiosas a tomar en consideración para una adopción segura y efectiva de la nube. En esta sección, se hace referencia a la metodología del Banco Mundial como una guía para ayudar a los países de Centroamérica, Panamá y República Dominicana en sus procesos de migración. No obstante, se exhorta a los países a personalizar este listado de verificación según sus contextos específicos y necesidades particulares.

- **Clasificación de datos:** según el Banco Mundial la clasificación de datos se puede definir a partir de tres objetivos de seguridad comúnmente establecidos en normas como la ISO 27001.
  - **Confidencialidad,** significa preservar las restricciones autorizadas sobre el acceso y la divulgación de la información, protegiendo la privacidad personal y la información confidencial; una pérdida de confidencialidad ocurre con la divulgación no autorizada de información.

[67] La publicación está disponible en el siguiente enlace https://openknowledge.worldbank.org/server/api/core/bitstreams/60a6b421-da41-4c7c-9362-9ff277709281/content

- **Integridad,** significa proteger la información contra modificaciones o destrucción indebidas, asegurando su autenticidad; una pérdida de integridad se manifiesta en la modificación o destrucción no autorizada de datos.
- **Disponibilidad** significa asegurar un acceso y uso oportuno y confiable de la información; una pérdida de disponibilidad se produce cuando se interrumpe el acceso a o uso de la información o de un sistema de información.

A partir de estos objetivos se puede definir si los datos son de carácter público, oficial, secreto o ultrasecreto. Esta clasificación permite determinar el nivel de protección necesario para cada tipo de dato y asegura que se apliquen las medidas de seguridad adecuadas según la sensibilidad del dato. Datos públicos, que tienen baja sensibilidad, requieren menos protección que datos confidenciales o de confidencialidad máxima, que necesitan medidas de seguridad más estrictas debido a su alto nivel de sensibilidad.

	Público	Oficial	Secreto	Ultrasecreto
Impacto en la confidencialidad, integridad y disponibilidad	**Impacto bajo:** a pérdida de confidencialidad, integridad o disponibilidad podría esperarse que tenga un efecto adverso limitado en las operaciones organizacionales, los activos de la organización o los individuos.	**Impacto moderado:** La pérdida de confidencialidad, integridad o disponibilidad podría esperarse que tenga un efecto adverso serio en las operaciones organizacionales, los activos de la organización o los individuos.	**Impacto alto:** La pérdida de confidencialidad, integridad o disponibilidad de los datos podría esperarse que tenga un efecto adverso severo o catastrófico en las operaciones organizacionales, los activos de la organización o los individuos.	**Impacto alto:** La pérdida de confidencialidad, integridad o disponibilidad de los datos de **confidencialidad máxima** podría esperarse que tenga un efecto adverso excepcionalmente grave en las operaciones organizacionales, los activos de la organización o los individuos.

Fuente: Banco Mundial (2022)

- **Alojamiento de datos:** según el nivel de clasificación de datos del punto anterior también se deben contemplar consideraciones legales y de seguridad al decidir si los datos gubernamentales deben almacenarse dentro de las fronteras geográficas del país. Entre las consideraciones clave se encuentra analizar si otros países cuentan con leyes adecuadas de protección de datos y si existen acuerdos de transferencia de datos con esos países. Además, es importante considerar la estabilidad política y la capacidad legal de los países en los que se almacenarán los datos. Para seleccionar proveedores de nube adecuados, se recomiendan los siguientes requisitos de seguridad:

Requerimientos de seguridad	Público	Oficial	Secreto/Ultrasecreto
Certificaciones	Sin requisito (aunque se recomienda alineación con certificaciones, por ejemplo, ISO)	Certificación requerida (por ejemplo, ISO)	Certificación requerida (por ejemplo, ISO)
Ubicación de los datos	No es requerido	La institución debe determinar si se debe establecer un requisito de residencia de datos oficiales dentro de las fronteras geográficas del país	Se recomienda exigir a los proveedores de servicios de nube que aseguren que los datos permanezcan dentro de las fronteras geográficas del país.
Tipo de despliegue de la nube	Nube pública	Nube pública	Nube privada o comunitaria (el procesamiento y almacenamiento se recomienda que sea *on-premise*).
Autorizaciones de Seguridad (“*security clearance*”) para Proveedores del servicio	No es requerido	No es requerido	Requerido

Fuente: Banco Mundial (2022)

- **Evaluación de riesgos y preparación:** se recomienda considerar la realización de (i) una evaluación de riesgos internos, para identificar y analizar los riesgos asociados con la integración de servicios en la nube en el entorno actual de la agencia y (ii) una evaluación de preparación para la nube, para examinar la capacidad técnica y operativa de la agencia para integrar y administrar eficazmente el servicio en la nube. Realizar estas evaluaciones de manera anticipada garantiza que la entidad no solo pueda manejar el servicio en la nube de manera segura y eficiente, sino que también cumpla con los requisitos técnicos y operativos necesarios para una implementación exitosa.

- **Caso de negocio:** se recomienda preparar un Caso de Negocio (“Business Case”) detallado para la adopción del servicio en la nube que incluya los siguientes elementos:
  - Alcance del servicio en la nube requerido.
  - Presupuesto y cálculo del costo total de propiedad.

- Habilidades del personal necesarias para apoyar el entorno de servicios en la nube.
- Infraestructura requerida para habilitar el servicio en la nube.
- Beneficio previsto del servicio en la nube.
- Resultado de las Evaluaciones de Riesgos y Preparación.

- **Requisitos de seguridad en la nube:** se debe identificar y definir los requisitos de seguridad necesarios para el contrato del servicio en la nube, basado en los niveles de clasificación de datos de los sistemas de información relevantes.
- **Cumplimiento de leyes, regulaciones y guías de la agencia:** se debe garantizar que la seguridad de los datos cumpla con las leyes y regulaciones nacionales aplicables, así como con las políticas de seguridad de información existentes.
- **Contrato:** se debe formalizar un contrato legalmente válido con el proveedor de servicios de nube antes de utilizar el servicio.
- **Duración del contrato:** se recomienda considerar contratos de corto plazo (de dos años o menos), con opciones de portabilidad para evitar la dependencia excesiva de un único proveedor.
- **Copias de seguridad de datos:** se debe coordinar con el proveedor de servicios de nube un mecanismo efectivo de copias de seguridad de los datos en la nube.
- **Protección y propiedad de los datos:** se debe asegurar que el proveedor de servicios de nube no exija derechos de propiedad sobre los datos almacenados, independientemente del formato o medio de almacenamiento. Además, se debe implementar un mecanismo de protección adecuado.
- **Continuidad del servicio:** se debe asegurar que el proveedor de servicios de nube implemente controles de seguridad en la nube adecuados y que realice pruebas periódicas de los planes de continuidad y recuperación ante desastres comunicando los resultados a la agencia.
- **Monitoreo continuo:** es necesario colaborar con el proveedor para mantener un entorno seguro en la nube pública. Las actividades pueden incluir notificaciones de incidentes de seguridad y notificaciones de cambios en los controles de seguridad.
- **Protección de datos y aplicaciones:** se debe asegurar que, al finalizar el contrato de servicio, todos los datos y aplicaciones sean transferidos a un nuevo proveedor de servicios, devueltos a la agencia o eliminados permanentemente, garantizando así la protección y correcta disposición de la información.

Caso Guatemala:

En 2019, la Superintendencia de Administración Tributaria (SAT) de Guatemala se convirtió en la institución pionera en el uso de la nube en el país. Actualmente, la SAT cuenta con dos plataformas en la nube: AWS para sistemas transaccionales, como el registro tributario y la facturación electrónica, y Azure para funciones de analítica, incluyendo el data warehouse. La decisión de adoptar tecnologías en la nube fue motivada por la necesidad de gestionar de manera eficiente la facturación electrónica, que abarca alrededor de 2,000 millones de documentos anuales.

Beneficios obtenidos por la SAT al migrar servicios a la nube:

- *Escalabilidad y agilidad, al incorporar nuevas soluciones en gobierno de manera rápida y eficiente*
- *Modernización de la administración tributaria*
- *Creación de eficiencias operativas*
- *Mayor capacidad de almacenamiento y procesamiento*

Desafíos y consideraciones cuando se inició el proceso de migración:

- *Asegurar cumplimiento normativo*
- *Necesidad de personal capacitado en nuevas tecnologías*
- *Entender cómo funciona el costo/precio del uso de la nube funciona.*

Fuente: *SAT y AWS (2019)*

Caso Reino Unido:

G-Cloud es una iniciativa del gobierno del Reino Unido diseñada para simplificar la adquisición de servicios en la nube por parte de los departamentos gubernamentales y fomentar la adopción de la informática en la nube en todo el gobierno. El programa consiste en una serie de acuerdos marco con proveedores de servicios en la nube, y una tienda en línea el Digital Marketplace, donde se listan estos servicios. Esto permite a las organizaciones del sector público comparar y adquirir servicios sin necesidad de un proceso de revisión exhaustivo.

Para ser incluido en el Digital Marketplace, los proveedores deben autoevaluarse y luego someterse a una verificación por parte del Servicio Digital Gubernamental (GDS), que actúa a su discreción. En 2014, el proceso de incorporación a G-Cloud se simplificó para reducir el tiempo y el costo para el gobierno del Reino Unido.

En lugar de una evaluación centralizada de los servicios en la nube, el nuevo proceso exige que los proveedores de servicios en la nube se auto certifiquen y presenten pruebas en apoyo de los 14 principios de seguridad en la nube de G-Cloud.

***Fuente*:** Microsoft (2024)

Referencias

Banco Interamericano de Desarrollo. (2022). *Cloud Computing: Opportunities and Challenges for Sustainable Economic Development in Latin America and the Caribbean.* https://publications.iadb.org/en/publications/english/viewer/Cloud-Computing-Opportunities-and-Challenges-for-Sustainable-Economic-Development-in-Latin-America-and-the-Caribbean.pdf

Banco Interamericano de Desarrollo. (n.d.). *Computación en la nube: Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.* https://publications.iadb.org/es/publications/spanish/viewer/Computacion-en-la-nube-Contribucion-al-desarrollo-de-ecosistemas-digitales-en-paises-del-Cono-Sur.pdf

Banco Interamericano de Desarrollo. (n.d.). *Contratación pública de servicios de computación en la nube: Mejores prácticas para su implementación en América Latina y el Caribe*. https://publications.iadb.org/es/contratacion-publica-de-servicios-de-computacion-en-la-nube-mejores-practicas-para-su

Banco Mundial. (2022). *Data Classification Matrix and Cloud Assessment Framework: Cloud Assessment Framework and Evaluation Methodology.* https://openknowledge.worldbank.org/server/api/core/bitstreams/60a6b421-da41-4c7c-9362-9ff277709281/content.

Barómetro Global de Datos. (2022). *Open Data Barometer y Data for Development.* https://opendatabarometer.org/leadersedition/report/

Canada Revenue Agency. (n.d.). *Taxpayer Bill of Rights*. https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/taxpayer-bill-rights.html

CIAT. (2020). *Las TIC como herramienta estratégica para potenciar la eficiencia de las administraciones tributarias*. https://www.ciat.org/Biblioteca/Estudios/2020_TIC-CIAT-FBMG.pdf

CIAT. (2024). *Gobierno de datos para las administraciones tributarias.* https://biblioteca.ciat.org/opac/book/5884?_gl=1*1jdmgnn*_ga*MTk2NzA5MDM5NS4xNzIzMDg4MTI5*_ga_MHWYD6C0X9*MTcyOTA5NTEwMS41LjAuMTcyOTA5NTEwMS42MC4wLjA.

Costa Rica. *Sistema Costarricense de Información Jurídica.* (n.d.). http://www.pgrweb.go.cr/scij/avanzada_pgr.aspx

Declaración de los Derechos del Hombre y del Ciudadano. https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/espagnol/es_ddhc.pdf

El Salvador. Ministerio de Hacienda. (n.d.). https://www.mh.gob.sv/

El Salvador. Portal de Transparencia Fiscal. (n.d.). https://www.transparenciafiscal.gob.sv/ptf/es/MarcoNormativo/AdministracinTributaria.html

Estados Unidos. Internal Revenue Service. (n.d.). https://www.irs.gov/

Góngora Pimentel, G.D. (n.d). *Estudios en Homenaje a Héctor Fix Zamudio – El reconocimiento del Derecho Administrativo Sancionador en la Jurisprudencia Constitucional Mexicana*, IIJ – UNAM, México.

Guatemala. Superintendencia de Administración Tributaria. (n.d.). https://portal.sat.gob.gt/portal/

HM Revenue & Customs, *The HMRC Charter,* Reino Unido. Información disponible en https://www.gov.uk/government/publications/hmrc-charter/the-hmrc-charter

Honduras. Servicio de Administración de Rentas. (n.d.). https://www.sar.gob.hn/

Huerta, C. (n.d.). *Sobre la distinción entre derechos fundamentales.* Corte Interamericana de Derechos Humanos. https://www.corteidh.or.cr/tablas/r28772.pdf

Internal Revenue Service. (n.d.). *Carta de Derechos del Contribuyente – versión en español.* Documento disponible en: https://www.irs.gov/es/taxpayer-bill-of-rights

KPMG. (2019). *The role of internal audit in cyber security readiness*. https://assets.kpmg.com/content/dam/kpmg/lu/pdf/2019/lu-en-cyber-databreach-brochure.pdf

México. Servicio de Administración Tributaria (n.d.). https://www.sat.gob.mx/home

National Institute of Standards and Technology. (n.d.). https://www.nccoe.nist.gov/data-security

Organización de Estados Americanos (OEA). (n.d.). *Convención Americana sobre Derechos Humanos – Pacto de San José.* https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Organización de Estados Americanos (OEA). (2013). *El Acceso a la Información Pública, un Derecho para ejercer otros Derechos*. https://www.oas.org/es/sap/dgpe/concursoinformate/docs/cortosp8.pdf

Organización de Estados Americanos (OEA). (2021). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Organización de las Naciones Unidas. (n.d.). *Declaración Universal de los Derechos Humanos – Resolución 217A (III).* https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf

Organización de las Naciones Unidas. (n.d.). *Derechos Humanos.* https://www.un.org/en/global-issues/human-rights

OECD. (2017). *Estándar para el Intercambio Automático de Información sobre Cuentas Financieras.* https://www.oecd.org/es/publications/estandar-para-el-intercambio-automatico-de-informacion-sobre-cuentas-financieras-segunda-edicion_9789264268074-es.html

OECD. (2021)., *Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información*. https://web-archive.oecd.org/tax/transparency/documents/confidentiality-ism-toolkit_es.pdf

OECD. (2020). *Panorama de las Administraciones Públicas América Latina y el Caribe 2020*. https://doi.org/10.1787/1256b68d-es

OECD. (2024). *Panorama de las Administraciones Públicas: América Latina y el Caribe 2024*. https://doi.org/10.1787/0f191dcb-es.

OECD. (2007). *Perspectivas de la OCDE. Capital Humano: Cómo moldea tu vida lo que sabes. Resumen en español*. https://www.oecd-ilibrary.org/docserver/9789264029095-sum-es.pdf?expires=1721158015&id=id&accname=guest&checksum=0B33A3E116BBA88CA0AA16B137FEB6E9

OECD. (n.d.). *Recomendación del Consejo de la OCDE sobre el Gobierno Abierto*. https://www.oecd.org/gov/oecd-recommendation-of-the-council-on-open-government-es.pdf

OECD. (2020). *Respuesta de las Administraciones Tributarias al COVID-19: Consideraciones acerca dela continuidad de actividades y servicios* define a las actividades *esenciales* como *aquellas funciones en las que el tiempo es un factor crítico cuya indisponibilidad o malfuncionamiento, incluso durante horas, afectaría a los sistemas de continuidad de la actividad de la administración, a personas, edificios y proveedores, dando lugar a un nivel inaceptable de desorganización en su labor e interrupción de sus actividades, al deterioro del servicio a clientes o a daños reputacionales.* https://read.oecd-ilibrary.org/view/?ref=133_133006-nruwv5tdpl&title=Respuesta-de-las-administraciones-tributarias-al-COVID-19-Consideraciones-acerca-de-la-continuidad-de-actividades-y-servicios

OECD. (n.d.). *Taxpayer's Rights and Obligations – Practice Note*. https://www.oecd.org/tax/administration/Taxpayers'_Rights_and_Obligations-Practice_Note.pdf

OECD. (2022). *Modelo de Madurez de Análisis de Datos*. https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/modelo-de-madurez-de-analisis-de-datos.pdf

Organización Internacional de Normalización. (n.d.). https://www.iso.org/es/home

Panamá. Dirección General de Ingresos. Ministerio de Economía y Finanzas. (n.d.) https://dgi.mef.gob.pa/

Prodecon. (2014). *Transparencia, Secreto Fiscal y Uso Indebido de Comprobantes*. https://portal.prodecon.gob.mx/Documentos/analisis-sistemicos/estudios-tecnicos/secreto-fiscal/mobile/index.html#p=1

República Dominicana. Dirección General de Impuestos Internos. (n.d.) https://dgii.gov.do/Paginas/default.aspx

Rüdiger, P. (1990). *Human Resource Management: An international comparison*. Human Resource Management: An International Comparison – Google Libros

Sebastian-Coleman, L. (2018). *Navigating the labyrinth: An executive guide to data management* (1st ed.). Technics Publications.

Servicio de Administración Tributaria de México. (n.d.). *Carta de los derechos del contribuyente auditado*. http://omawww.sat.gob.mx/informacion_fiscal/derechos_contribuyentes/Documents/Carta_Contr_Aud_072014.pdf

UNESCO. (n.d.). *Access to Information Laws.* https://www.unesco.org/en/access-information-laws

Anexo

Marco jurídico en materia de confidencialidad, acceso a la información y transparencia

País	Confidencialidad de la información			Acceso a la información y transparencia			Marco sancionador
	Constitución política	Código tributario	Protección de datos	constitución política	Leyes acceso a la información	Leyes de transparencia	Normativas adicionales o complementarias
Costa Rica	Artículo 30	Código de Normas y Procedimientos Tributarios. Artículos 115, 115 bis y 117	Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales – Ley n.º 8968 Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 37554-JP,	N/A	Transparencia y Acceso a la Información Pública N° 073-MP-MEIC-MC Decreto Ejecutivo N° 40199-MP Apertura de Datos Públicos		N/A
El Salvador	N/A	Artículo 28	Lineamientos Generales de Protección de Datos Personales	N/A	Ley de Acceso a la Información Pública	N/A	Ley especial contra los delitos informáticos y conexos
Guatemala	Artículo 24	Artículo 101-A	Ley Integral de Protección de Datos Personales en Poder de Terceros*	Artículo 30 Artículo 31	Ley de Acceso a la Información Pública	N/A	N/A
Honduras	Artículo 182	N/A	Ley de Protección de Datos Personales y Acción de Hábeas Data	N/A	Ley de Transparencia y Acceso a la Información Pública		N/A
Panamá	Artículo 29 Artículo 42	Artículo 722	Ley 81 para la Protección de Datos	Artículo 43 Artículo 44	Ley de Transparencia y Acceso a la Información – Ley 6 del 22 de enero de 2002.		N/A
República Dominicana	Artículo 44	Artículo 47	Ley núm. 172-13 Protección integral de los datos personales (…)	N/A	Ley General de Libre Acceso a la Información Pública No. 200-04.		

ciat@ciat.org