ANÁLISIS DE APLICACIÓN DE LA LGPD EN UNA INSTITUCIÓN EDUCATIVA PÚBLICA: UN ESTUDIO DE CASO

ANÁLISE DE APLICAÇÃO DA LGPD NUMA INSTITUIÇÃO PÚBLICA DE ENSINO: UM ESTUDO DE CASO

GDPR APPLICATION ANALYSIS IN A PUBLIC EDUCATIONAL INSTITUTION: A CASE STUDY

Jackson Gomes Soares SOUZA[1]
Francisco Rolfsen BELDA[2]
Carlos Hideo ARIMA[3]

RESUMEN: La intensificación en la recolección, almacenamiento y procesamiento de datos por las instituciones llama la atención acerca de la protección de datos personales. Esta investigación básica aplicada tiene como objetivo verificar, por un estudio de caso, la conformidad entre los instrumentos normativos de protección de datos personales adoptados por una institución de educación tecnológica pública y el establecido por la Ley General de Protección de Datos (LGPD). Las respuestas obtenidas a partir de un cuestionario estructurado fueron tabuladas y procesadas, evidenciando la relación entre el contexto institucional y las dimensiones analizadas para la implementación de protocolos y buenas prácticas. De acuerdo con los resultados, se considera la necesidad de implementar un programa de gobernanza y privacidad que cumpla con las políticas institucionales.

PALABRAS CLAVE: Ley General de Protección de Datos Personales. LGPD. Ambientes de enseñanza.

RESUMO: *A intensificação na coleta, armazenamento e tratamento de dados pelas instituições traz atenção quanto à proteção de dados pessoais. Esta pesquisa básica aplicada visa verificar, por meio de um estudo de caso, a conformidade entre instrumentos normativos de proteção de dados pessoais adotados por instituição pública de ensino tecnológico e o estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD). As respostas coletadas pelo questionário estruturado foram tabuladas e tratadas, demonstrando a relação entre contexto institucional e as dimensões analisadas para a implementação de protocolos e das boas práticas. Conforme os resultados, considera-se a necessidade de implementação de um programa de governança em privacidade que vá ao encontro das políticas institucionais.*

[1] Instituto Federal de Educación, Ciencia y Tecnología de São Paulo (IFSP), Campinas - SP - Brasil. Maestro. Estudiante de Doctorado en Educación Escolar (UNESP). ORCID: https://orcid.org/0000-0003-4952-8618. E-mail: jackson@ifsp.edu.br

[2] Universidad Estatal Paulista (UNESP), Bauru - SP - Brasil. Profesor del Departamento de Comunicación Social. Doctorado en Ingeniería de Producción (EESC-USP). ORCID: https://orcid.org/0000-0001-6350-7026. E-mail: belda@faac.unesp.br

[3] Centro Estatal de Educación Tecnológica Paula Souza (CEETEPS), São Paulo - SP - Brasil. Profesor del Programa de Maestría Profesional en Gestión y Tecnología en Sistemas Productivos e Investigador de la Unidad de Posgrado, Extensión e Investigación del Centro Paula Souza. Doctorado en Contraloría y Contabilidad (USP). ORCID: https://orcid.org/0000-0001-7922-0943. E-mail: charima@uol.com.br

(cc) BY-NC-SA

PALAVRAS-CHAVE: *Lei Geral de Proteção de Dados Pessoais. LGPD. Ambientes para ensino.*

ABSTRACT: *The intensification of data collection, storage and processing by institutions calls attention to personal data protection. This basic applied research aims to verify, through a case study, the compliance between a public institution of technological education's data protection regulation instruments and the addressed by the General Data Protection Law (GDPR). The answers were collected by a structured questionnaire, being subsequently tabulated and processed. The results demonstrate the relationship between the institutional context and dimensions analyzed for the implementation of protocols, good practices and a privacy governance program that meets institutional policies.*

KEYWORDS: *General Data Protection Regulation. GDPR. Learning environments.*

Introducción

Según Davenport (1998, p. 18), "los datos son simples observaciones sobre el estado del mundo" y tienen como características: "fácilmente estructurados, obtenidos por máquinas, a menudo cuantificados y fácilmente transferibles", mientras que la información sería un conjunto de "datos dotados de relevancia y propósito", requiriendo "unidad de análisis, consenso en relación con el significado y, necesariamente, mediación humana". Dicha mediación puede presentarse por la "interacción entre humanos y sistemas, trayendo consigo conceptos como la seguridad de la información y la privacidad involucradas en este proceso" (SOUZA; ARIMA; BELDA, 2020, p. 1310).

Estamos rodeados de diversas tecnologías, por lo que el uso de medios digitales para los procesos de enseñanza y aprendizaje está directamente relacionado con el tratamiento de los datos almacenados y utilizados por las instituciones, y estas deben adoptar políticas de protección de datos e información personal basadas en una legislación específica.

La Ley General de Protección de Datos Personales (LGPD), Ley No. 13.709, del 14 de agosto de 2018 (BRASIL, 2018):

> Prevé el tratamiento de datos personales, también en medios digitales, por una persona física o por una entidad jurídica de Derecho público o privado, con el objetivo de proteger los derechos fundamentales de libertad y privacidad y el libre desarrollo de la personalidad de la persona física.

Con la promulgación de la Enmienda Constitucional No. 115 (EC115), publicado el 11 de febrero de 2022 en la Sección 1, Número 30, Página 2 del Boletín Oficial, la Constitución Federal de Brasil de 1988 ahora contempla la lista de derechos y garantías fundamentales de

(cc) BY-NC-SA

protección de datos, estableciendo la competencia de las entidades federativas para legislar sobre el tema (BRASIL, 2022).

La Ley No. 11.892, de 29 de diciembre de 2008 (BRASIL, 2008), además de otras medidas, establece que:

> Los Institutos Federales son instituciones de educación superior, básica y profesional, pluricurricular y *multicampamento*, especializadas en la provisión de educación profesional y tecnológica en las diferentes modalidades de enseñanza, basadas en la combinación de conocimientos técnicos y tecnológicos con sus prácticas pedagógicas, de conformidad con esta Ley.

En este sentido, esta investigación tiene como objetivo estudiar los instrumentos normativos de protección de datos personales adoptados en una institución pública de educación tecnológica y los resultados *actuales* para el desarrollo de políticas y procedimientos en uno de sus *campus*.

Fundamento teórico

Según Pierre Lévy (2014, p. 23), "todavía no sabemos transformar sistemáticamente los datos en conocimiento", trayendo la reflexión sobre una "memoria digital participativa, en proceso de constitución, común a toda la humanidad para resolver este problema de interoperabilidad semántica".

En este sentido, el autor establece una unidad de la naturaleza basada en la noción de información, abordando una imagen sintética de la naturaleza informativa y su concepto científico, concibiendo la naturaleza de la información en capas sucesivas: de los quarks a los átomos, de las moléculas a los organismos, de los sistemas nerviosos a los fenómenos y de los símbolos a los conceptos (LÉVY, 2014). Una posible interpretación sería que los datos serían equivalentes a símbolos, aunque no modalizados, pero no sin sentido.

El 24 de octubre de 1995, el Parlamento Europeo y el Consejo de la Unión Europea publicaron en el Diario Oficial No. L 281 de 23/11/1995, páginas 31 a 50, "Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" (UE, 1995).

El artículo 29 de la Directiva 95/46/CE estableció la creación del "grupo de protección personal en lo que respecta al tratamiento de datos personales", de carácter consultivo e independiente, el "*Article 29 Working Party (WP29)"*, O el Grupo de Trabajo del Artículo 29 (GT29). También trae la definición de datos personales fragmentándolos en 4 (cuatro) pilares o elementos principales:

(cc) BY-NC-SA

> [...] «cualquier información», «relativa a», «persona física», «identificada o identificable». Los cuatro pilares están estrechamente relacionados y se basan entre sí, determinando conjuntamente si la información se considerará o no como datos personales [...] (UE, 2007, p. 6, grifo del autor).

En Brasil, la LGPD, además de traer una definición similar de datos personales, regula en sus 10 (diez) capítulos:

> «Disposiciones generales»; «tratamiento de datos personales»; «derechos del titular»; «tratamiento de datos personales por parte de las autoridades públicas»; «transferencia internacional de datos»; «agentes del tratamiento de datos personales»; «seguridad y buenas prácticas»; «supervisión»; 'Autoridad Nacional de Protección de Datos (ANPD) y Consejo Nacional de Protección de Datos Personales y Privacidad' y 'disposiciones finales y transitorias' (BRASIL, 2018).

El artículo 6 de la LGPD establece, entre otros, principios a observar, de manera que las políticas de tratamiento adoptadas permitan a los usuarios conocer las formas en que se utilizarán sus datos, permitiendo evitar o reducir la recopilación y uso de su información por parte de terceros. Para aplicar los conceptos, se resumieron los principales elementos en dimensiones, según la Tabla 1.

Tabla 1 - Dimensiones de la protección de datos personales

1. **Fundamentos (FUN)**: Preocupación por la "protección de los datos personales cuando se procesan, incluso en medios digitales, con el objetivo de proteger los derechos fundamentales de libertad, privacidad y libre desarrollo de la personalidad de la persona física" (BRASIL, 2018, s/p [web]).
2. **Principios (PRI)**: Cumplimiento de los principios de "propósito, adecuación, necesidad, libre acceso, calidad de datos, transparencia, seguridad, prevención, no discriminación, rendición de cuentas y rendición de cuentas" (BRASIL, 2018, s/p [web]).
3. **Tratamiento de datos personales (TRA):** "Toda operación realizada con datos personales", siendo indispensable el consentimiento del titular "por escrito o por otro medio que demuestre la manifestación de voluntad" "libre e inequívoco" (BRASIL, 2018, s/p [web]).
4. **Derechos del titular (DIR):** El derecho a "revocar el consentimiento", "actualizar", "anonimizar", "bloquear" o "eliminar" los datos personales del interesado (BRASIL, 2018, s/p [web]).

Fuente: Adaptado por autores a partir de la LGPD (BRASIL, 2018)

El capítulo 4 de la LGPD regula el tratamiento por parte de las autoridades públicas, incluyendo hacer referencia directa en el caput del artículo 23 a la Ley N° 12.527 de 18 de noviembre de 2011, también conocida como Ley de Acceso a la Información (LAI), y debe "[...] llevarse a cabo para cumplir con su propósito público, en pos del interés público, con el

(cc) BY-NC-SA

objetivo de ejecutar competencias legales o cumplir con los deberes legales del servicio público" (BRASIL, 2018).

Además, el artículo 50 hace referencias directas, en sus tres apartados, a los principios enumerados en el artículo 6, como la finalidad, la calidad, la seguridad, la prevención y la rendición de cuentas.

Procedimientos metodológicos

Según la clasificación de investigación realizada por el politólogo Donald Stokes, se trata de una investigación básica-aplicada, impulsada por la curiosidad investigativa sobre fenómenos particulares, no necesariamente dirigida a "objetivos explicativos generales o cualquier uso práctico al que se destinen sus resultados" (STOKES, 2005, p. 119).

Según Yin (2001, p. 11 y 47), el estudio de caso es una investigación empírica centrada en "fenómenos contemporáneos insertados en algún contexto de la vida real", teniendo como requisito previo la sistematización de procedimientos a través de protocolos.

Este estudio cubre el "*campus* Campinas vinculado al Instituto Federal de Educación, Ciencia y Tecnología de São Paulo - IFSP" y, por tratarse de un solo estudio de caso, los datos recolectados y su consecuente análisis no permitirán la generalización de los resultados (BRASIL, 2018). Para la recopilación de datos, se adopta un cuestionario digital estructurado como instrumento en la plataforma Google *Forms*. También cuenta con la participación voluntaria de 80 profesores y directivos inscritos en el "Sistema Unificado de Administración Pública" (SUAP) del *campus*, y se recogieron un total de 15 respuestas.

Según Likert (1932), los estudios que involucran declaraciones de opinión y actitud se consideran un método indirecto para evaluar disposiciones que se significan y expresan más fácilmente en forma verbal y, en consecuencia, se pueden agrupar en patrones. Por ello, se utilizará la escala Likert, en la que las respuestas obtenidas emiten el grado de acuerdo de los participantes con la frase, contemplando niveles del 1 al 5 de la escala, clasificados respectivamente como: "Totalmente en desacuerdo", "En desacuerdo", "Neutral", "Estoy de acuerdo" y "Estoy totalmente de acuerdo".

Con respecto a la investigación de los instrumentos normativos adoptados por el IFSP en cumplimiento de los requisitos abordados en la LGPD, la investigación documental de este estudio incluye el Estatuto de la institución y las Ordenanzas más recientes, que aprueban el Reglamento Interno del Comité de Gobernanza Digital y que actualizan la "Política de

(cc) BY-NC-SA

Seguridad de la Información y la Comunicación - PoSIC", así como la "Política de Protección de Datos Personales" (BRASIL, 2020).

Análisis de datos

La interpretación de los resultados inicialmente se basará en la siguiente estructura: PDP - Perfil de los Participantes y CDI - Contexto de la institución.

Las dimensiones de protección de datos personales se investigarán a continuación:

- FUN - Fundamentos de la protección de datos personales;
- PRI - Principios de protección de datos personales;
- TRA - Tratamiento de datos personales;
- DIR - Derechos del titular de los datos personales.

La muestra tiene 15 respuestas recogidas. El perfil de los participantes se caracteriza según el grupo de edad, la escolaridad, el tiempo en la institución y si la persona participante ocupa actualmente un puesto directivo, según la Tabla 2.

Tabla 2 - Perfil de los participantes

Docentes	Grupo de edad	Escolarización	Tiempo de la institución	Director
D1	30 a 39 años	Maestros	entre 4 y 10 años	No
D2	50 a 59 años	Doctorado	entre 4 y 10 años	No
D3	30 a 39 años	Maestros	entre 4 y 10 años	No
D4	30 a 39 años	Maestros	entre 10 y 20 años	No
D5	50 a 59 años	Doctorado	Más de 20 años	Sí
D6	40 a 49 años	Doctorado	entre 4 y 10 años	Sí
D7	60 a 69 años	Doctorado	entre 4 y 10 años	No
D8	50 a 59 años	Maestros	entre 4 y 10 años	No
D9	30 a 39 años	Doctorado	entre 4 y 10 años	Sí
D10	40 a 49 años	Doctorado	entre 4 y 10 años	Sí
D11	50 a 59 años	Doctorado	entre 4 y 10 años	No
D12	50 a 59 años	Doctorado	entre 4 y 10 años	No
D13	40 a 49 años	Maestros	entre 4 y 10 años	No
D14	30 a 39 años	Maestros	entre 4 y 10 años	No
D15	18 a 29 años	Maestros	entre 4 y 10 años	No

Fuente: Resultados de la búsqueda

El perfil del participante cambia según el nivel de educación que tenga, y se observa que solo dos grupos de edad comprenden el 64% de los docentes, que tienen entre 30 y 39 años y entre 50 y 59 años; mientras que en el primer rango la mayor concentración es la de maestrías, en el segundo, la mayoría tiene doctorados.

El análisis del contexto de la institución (CDI) abarca la investigación de:

(cc) BY-NC-SA

- CDI1 – Adopción de una Política de Seguridad de la Información y las Comunicaciones (PoSIC) suficientemente esclarecedora por parte de la institución;
- CDI2 - Controles técnicos de protección de los datos personales almacenados;
- CDI3 - Transparencia y libre acceso a la información y datos personales almacenados;
- CDI4 - Capacitación o eventos que cubren la privacidad y protección de datos personales y operativos;
- CDI5 - Adopción de diferentes métodos de autenticación;
- CDI6 - Comunicación, a través de avisos, sobre privacidad y protección de datos personales;
- CDI7 - Conciencia de seguridad de la información;
- CDI8 - Sensibilización sobre la protección de la información confidencial en formato electrónico.

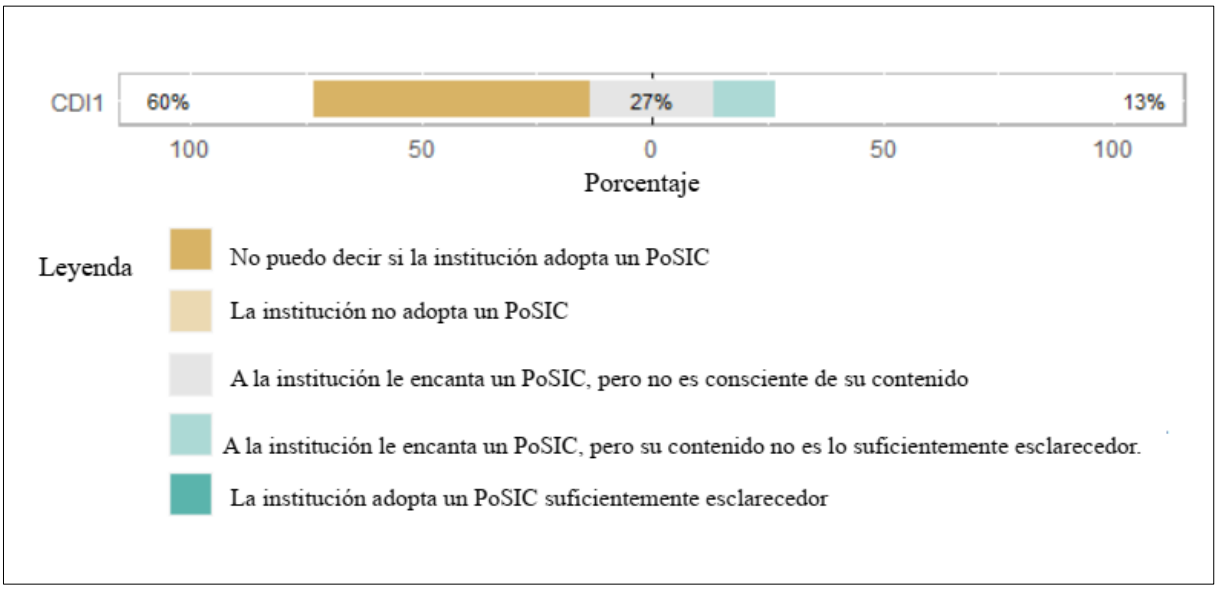
Inicialmente, la ciencia de los resultados con respecto a la adopción de una Política de Seguridad de la Información y las Comunicaciones (PoSIC) suficientemente esclarecedora por parte de la institución, abordada por el elemento CDI1, aportará evidencia de posibles respuestas neutrales en las declaraciones sobre el contexto de la institución.

Como también se puede observar en la Figura 1, el 40% de los participantes está de acuerdo en que la institución adopta un PoSIC; sin embargo, el 26,67% dice desconocer su contenido, y el 13,33% que su contenido no es lo suficientemente esclarecedor.

A pesar de que el 60% de los participantes no puede decir si la institución adopta un PoSIC, una inferencia prematura de este fenómeno podría cuestionar su nivel de familiaridad con el tema abordado. Sin embargo, los participantes añaden en sus respuestas que "en la institución los servidores saben poco sobre la LGPD, y no hay medidas institucionales adoptadas para la protección de datos, estando a cargo del sentido común de la protección de datos del servidor", y aún "sin tener ningún conocimiento sobre protección de datos en nuestra institución".

(cc) BY-NC-SA

Figura 1 - Representación gráfica de las respuestas CDI1



Fuente: Resultados de la búsqueda

Para un análisis adecuado, los factores relacionados con este punto se investigan con mayor profundidad tanto en los siguientes elementos de la CDI como en los análisis de las dimensiones de protección de datos personales.

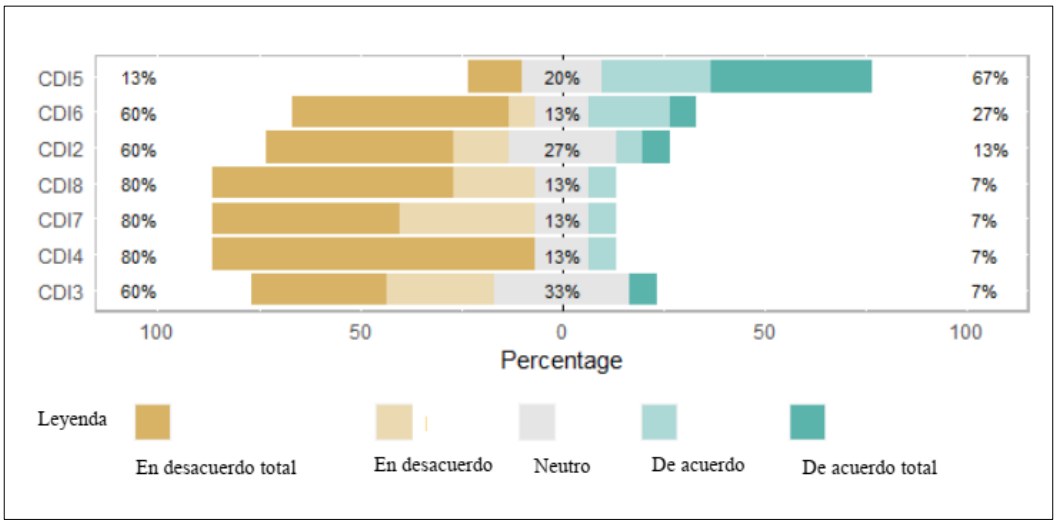
En secuencia, se observa de la Figura 2 que el único aspecto que presentó un alto grado de acuerdo (67%) fue CDI5, que se refiere al hecho de que la institución adopta, para el acceso de los usuarios a los sistemas, diferentes métodos de autenticación, como usuario y contraseña, biometría, tokens por aplicaciones.

Las otras respuestas presentan un alto grado de desacuerdo, y se pueden dividir en dos grupos, uno con un 80% de desacuerdo y el otro con un 60% de desacuerdo. Con un 80% son CDI4, CDI7 y CDI8, cuando abordan aspectos relacionados con la realización de capacitaciones o eventos que se ocupan de la privacidad y protección de datos personales; a la ciencia del contexto de la seguridad de la información; y cómo proteger la información sensible en formato electrónico.

Luego, con un 60% de desacuerdo, están CDI2, CDI3 y CDI6, cuando se trata de aspectos institucionales respecto a la implementación de controles técnicos para proteger los datos personales almacenados en sus sistemas; se ofrece a los interesados transparencia y libre acceso a la información y los datos personales almacenados en sus sistemas; y la comunicación de cuestiones relacionadas con la privacidad y la protección de datos.

(cc) BY-NC-SA

Figura 2 - Representación gráfica de las respuestas de CDI2 a CDI8



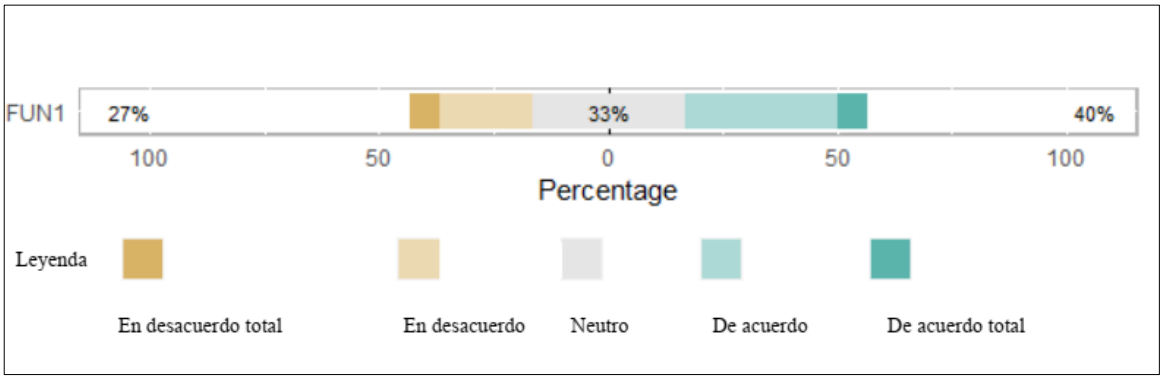
Fuente: Resultados de la búsqueda

También es destacable el hecho de que CDI2, CDI3 y CDI5 presentan un cierto grado de neutralidad en relación con los otros aspectos analizados, especialmente el 33% de CDI3, cuando se trata de transparencia y libre acceso a la información, lo que indica una posible relación de los índices aquí analizados con el fenómeno observado en CDI1.

El análisis de las dimensiones de protección de datos personales incluirá los Fundamentos (FUN), Principios (PRI), Tratamiento (TRA) y Derechos del Titular (DIR).

Con respecto a los motivos de protección de datos personales (FUN), las disposiciones del artículo 1 de la LGPD se basan en las disposiciones del artículo 1 de la LGPD, estableciendo que la institución, en sus diversas actividades, debe preocuparse por la "protección de los datos personales cuando se procesan", "incluso en los medios digitales, con el objetivo de proteger los derechos fundamentales de libertad, privacidad y el libre desarrollo de la personalidad de la persona física" (BRASIL, 2018).

Figura 3 - Representación gráfica de las respuestas de FUN1



Fuente: Resultados de la búsqueda

(cc) BY-NC-SA

Según la Figura 3, se observa que, a pesar del 40% de acuerdo por parte de los encuestados, existe un alto grado (33%) de neutralidad en comparación con el total y, además, aproximadamente un 27% de desacuerdo, lo que trae resultados divergentes y no concluyentes.

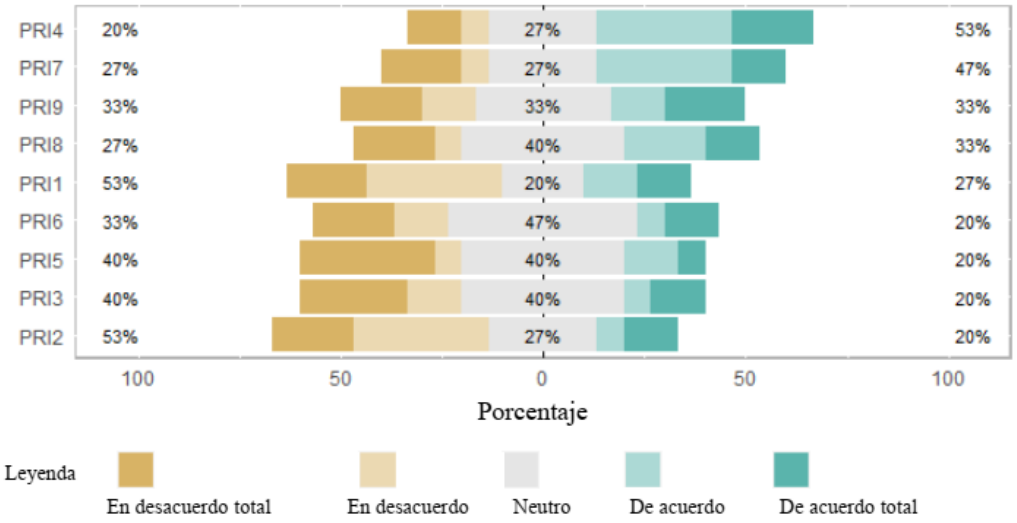
El análisis de los principios de protección de datos personales (PRI) abarca la investigación de si, durante el proceso de recopilación y procesamiento de datos personales, la institución informa a sus titulares:

- PRI1 – "Finalidad(es) específica(s) del uso de estos datos" (BRASIL, 2018);
- PRI2 - "El nivel de compromiso para cumplir con el propósito (s) informado (BRASIL, 2018);
- PRI3 – "Se permite la consulta libre y fácil sobre la forma y la duración del procesamiento, así como la integridad de sus datos personales" (BRASIL, 2018);
- PRI4 - "Si permite la actualización de sus datos" (BRASIL, 2018);
- PRI5 – "Si proporciona accesibilidad y claridad de la información sobre el desempeño del tratamiento" (BRASIL, 2018);
- PRI6 – "Si utiliza medidas técnicas y administrativas capaces de proteger los datos personales del acceso no autorizado y situaciones accidentales o ilegales de destrucción, pérdida, alteración, comunicación" (BRASIL, 2018);
- PRI7 – "Se utilizan medidas para prevenir la ocurrencia de daños debidos al procesamiento de datos personales", tales como restricciones de acceso y autenticación, adopción de encriptaciones (BRASIL, 2018);
- PRI8 – "Será imposible llevar a cabo el procesamiento con fines discriminatorios, ilegales o abusivos", desde la recopilación hasta su uso, modificación, difusión y eliminación de datos (BRASIL, 2018);
- PRI9 – "Se adoptará el cumplimiento de las normas de protección de datos personales, asumiendo la responsabilidad de la efectividad de estas medidas" (BRASIL, 2018).

La Figura 4 muestra que las respuestas presentaron un rango entre 20% y 46.67% de neutralidad, y pueden indicar la necesidad de prestar atención a los principios enumerados por la LGPD, en particular el PRI6 - principio de seguridad, previsto en el Artículo 6, punto VII, que trata del uso por parte de la institución de "medidas técnicas y administrativas capaces de proteger datos personales" (BRASIL, 2018).

(cc) BY-NC-SA

Figura 4 - Representación gráfica de las respuestas PRI



Fuente: Resultados de la búsqueda

Aun analizando las respuestas con alto índice de neutralidad en comparación con las tasas de acuerdo y desacuerdo, PRI8 - "principio de no discriminación", previsto en el artículo 6, punto IX, a pesar del acuerdo de 33.33%, presenta un grado aún mayor (40%) de neutralidad, hecho que se asocia con 26.67% de desacuerdo cuando se trata de la adopción de medidas por parte de la institución que imposibilitan "realizar un trato con fines discriminatorios, desde la recopilación hasta su uso, modificación, difusión y eliminación de datos (BRASIL, 2018).

En este mismo intervalo de neutralidad del 40%, PRI5 - "principio de transparencia", previsto en el artículo 6, punto VI, también presenta un 40% de desacuerdo y atención a posibles ajustes por parte de la institución con respecto a la garantía, a los titulares, de accesibilidad y claridad de la información sobre el "desempeño del tratamiento y los respectivos agentes responsables" del procesamiento de datos (BRASIL, 2018).

Situación similar ocurre con PRI3 - "principio de libre acceso", previsto en el artículo 6, punto IV, que establece que la institución garantiza a los titulares "consultas facilitadas y gratuitas sobre la forma y duración del procesamiento, así como sobre la integridad de sus datos personales" (BRASIL, 2018).

El principio PRI9 - "principio de rendición de cuentas y rendición de cuentas", enumerado por el artículo 6, punto X, presenta tasas iguales de 33,33% por desacuerdo, neutralidad y acuerdo al abordar la adopción de medidas de "cumplimiento y cumplimiento de las normas de protección de datos personales, siendo responsable de la efectividad de estas medidas" (BRASIL, 2018).

(cc) BY-NC-SA

El mayor grado de desacuerdo se da en PRI1 y PRI2, con un índice de 53,33%. PRI1 - "principio de finalidad", previsto en el artículo 6, inciso I, establece que el "tratamiento es para fines legítimos, específicos, explícitos e informados para el titular, sin posibilidad de tratamiento adicional de manera incompatible con estos fines" (BRASIL, 2018).

En el mismo contexto, PRI2 - "principios de adecuación y necesidad", previstos en el Artículo 6, puntos II y III, tratan del "nivel de compromiso para cumplir con los fines del procesamiento de datos informados al titular, limitando el tratamiento al mínimo necesario" (BRASIL, 2018).

PRI4 y PRI7 fueron los únicos elementos que presentaron un mayor grado de acuerdo que los demás. Con un acuerdo del 53,33%, PRI4 - "principio de calidad", previsto en el artículo 6, inciso V, establece que "se garantiza al titular la posibilidad de actualización, exactitud, claridad y pertinencia de sus datos, de acuerdo con la necesidad y para el cumplimiento de la finalidad de su tratamiento" (BRASIL, 2018).

Mientras que con un 46,66% de acuerdo, PRI7 - "principio de prevención", previsto en el artículo 6, punto VIII, se ocupa de la "adopción de medidas para prevenir la ocurrencia de daños debidos al procesamiento de datos personales", como las restricciones de acceso y autenticación y la adopción de cifrado (BRASIL, 2018).

El análisis del "procesamiento de datos personales" (TRA) abarca la investigación de si la institución:

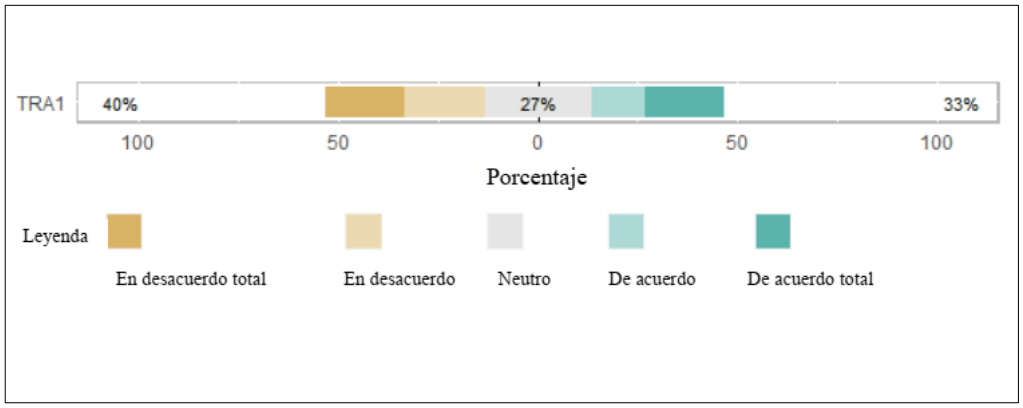
- TRA 1 – solicita a los titulares legales o tutores su "consentimiento por escrito o por cualquier otro medio que demuestre voluntad" si existe un interés en el procesamiento de datos (BRASIL, 2018).

Se observa que las respuestas presentan un cierto grado de neutralidad (26,67%) en comparación con los otros índices y, como también se puede ver en la Figura 5, el índice discordante total es del 40%, mientras que el acuerdo total es del 33,33%.

Con respecto al 40% de desacuerdo, se observa la necesidad por parte de la institución de solicitar a los titulares o tutores legales su consentimiento si existe interés en el tratamiento de datos, de acuerdo con lo dispuesto en el artículo 7 de la LGPD, punto I (BRASIL, 2018). Además de esto, hay otros nueve elementos que contienen las hipótesis que deben cumplirse para que se pueda realizar el procesamiento de datos personales (BRASIL, 2018).

Figura 5 - Representación gráfica de las respuestas TRA

(cc) BY-NC-SA

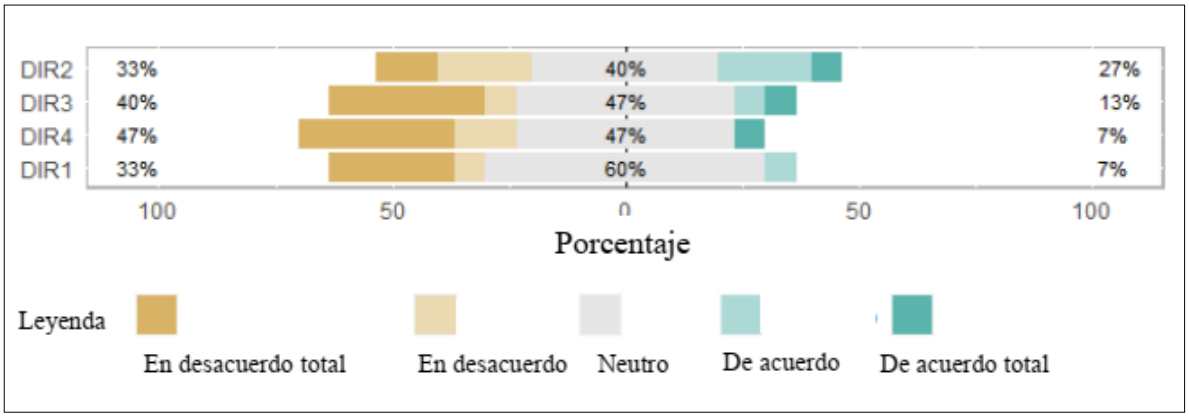


Fuente: Resultados de la búsqueda

El análisis de los "derechos del interesado" (DIR) abarca la investigación de si, al final del propósito específico del procesamiento, la institución garantiza a los interesados el derecho a: DIR1 – "Retiro del consentimiento"; DIR2 - "Anonimización de datos personales"; DIR3 - "Bloqueo de datos personales"; DIR4 - "Eliminación de datos personales" (BRASIL, 2018).

Se observa en la Figura 6 que las respuestas presentaron un rango entre 40% y 60.00% de neutralidad, lo que puede indicar la necesidad de prestar atención a los "derechos del interesado" enumerados por la LGPD, especialmente el DIR1 – "derecho del titular a revocar su consentimiento" previsto en el Artículo 18, punto IX (BRASIL, 2018).

Figura 6 - Representación gráfica de las respuestas de DIR



Fuente: Resultados de la búsqueda

Consideraciones finales

Los resultados y análisis de los datos demuestran la relación entre el contexto institucional y la investigación de las dimensiones que atañen a fundamentos, principios, tratamiento de datos personales y derechos del interesado, haciendo referencia a la necesidad

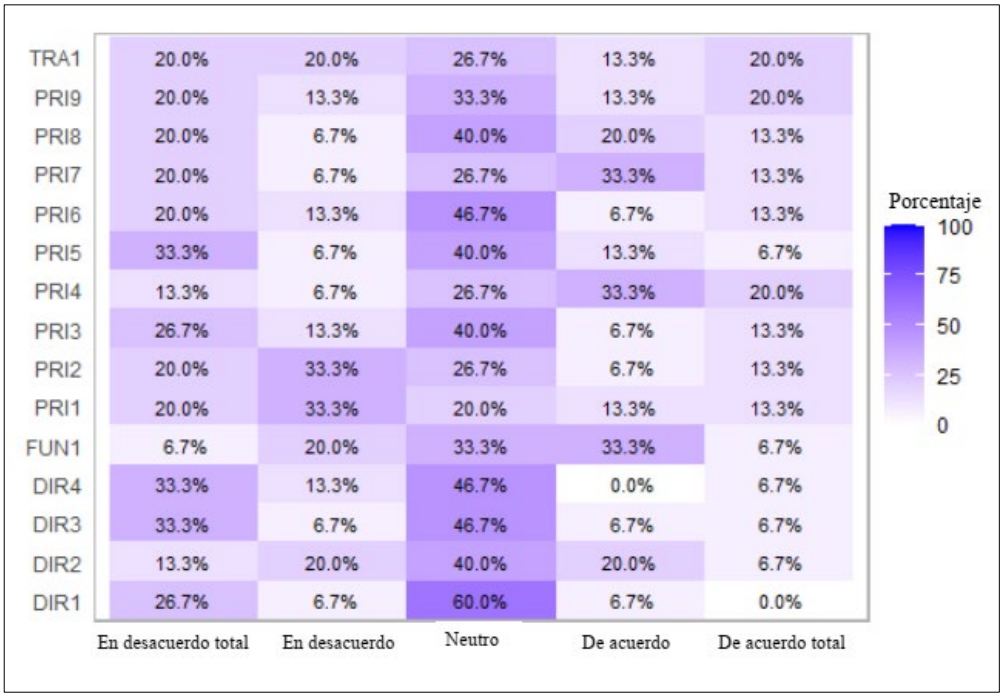
(cc) BY-NC-SA

de adaptaciones por parte de la institución que, a pesar de adoptar un PoSIC, se observa que gran parte de los participantes afirman no saber decir que esto ocurre.

Esta afirmación corrobora el alto grado de desacuerdo respecto a la adopción de controles técnicos, transparencia y libre acceso, capacitación o eventos que se ocupen de la privacidad, la comunicación y la concientización sobre la seguridad de la información. La única excepción radica en la adopción por parte de la institución de diferentes métodos de autenticación, lo que mejora significativamente la seguridad de los controles de acceso.

A su vez, se observa a través del mapa de calor de la Figura 7 que el análisis de las dimensiones presenta un cierto grado de neutralidad -la región central del mapa- en comparación con las de desacuerdo y acuerdo.

Figura 7 - Mapa de calor de las respuestas a las dimensiones de protección de datos personales



Fuente: Resultados de la búsqueda

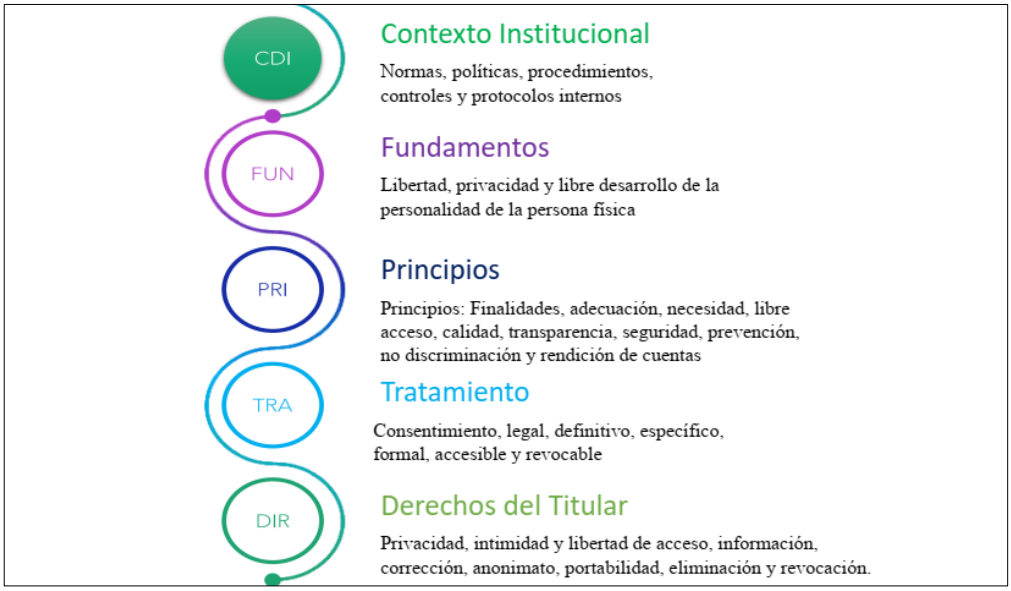
Las dimensiones analizadas abordan elementos obligatorios de la LGPD cuando se trata de derechos fundamentales previstos constitucionalmente, como la libertad, la privacidad, el libre desarrollo de la personalidad de la persona física para la protección de datos personales, así como el cumplimiento de los principios enumerados por la ley: finalidad, adecuación, necesidad, libre acceso, calidad, transparencia, seguridad, prevención, no discriminación, rendición de cuentas.

(cc) BY-NC-SA

Además, al tratar sus datos personales, el consentimiento del titular deberá demostrar su expresión expresa e inequívoca de voluntad, así como los derechos a revocar el consentimiento, alteración, anonimización, bloqueo o supresión de los datos personales. Asimismo, debe garantizarse que cada «finalidad» sea única, legítima, especificada, explícita y «adecuada» al contexto de cada finalidad informada, de modo que la operación se limite a la más mínima «necesidad» y permita su «libre acceso» de forma completa, gratuita y facilitada, garantizando la «calidad de los datos» por su exactitud, pertinencia, actualización y «transparencia», sin renunciar a la adopción de medidas capaces de demostrar la «seguridad». «prevención», «no discriminación», «rendición de cuentas y rendición de cuentas» por parte del agente de tratamiento.

La Figura 8 representa los elementos discutidos y analizados aquí, ilustrando el flujo de protección de datos personales dentro de la institución.

Figura 8 - Flujo de protección de datos personales



Fuente: Elaboración propia

Las adaptaciones necesarias al *campus* se presentan en la relación del contexto institucional con las dimensiones de protección de datos personales proporcionadas por la LGPD, demostrando la necesidad de implementar un programa de gobernanza de la privacidad que cumpla con el PoSIC institucional, de manera transparente, con controles técnicos, capacitación, comunicaciones y sensibilización.

(cc) BY-NC-SA

Tales medidas consolidan un vínculo de compromiso y promueven una relación de confianza entre el interesado y la institución, porque son efectivamente integradas, aplicables y adaptativas.

REFERENCIAS

BRASIL. **Lei n. 11.892, de 29 de dezembro 2008**. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências. Brasília, DF: Presidência da Repúlica, 2008. Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm. Acceso en: 13 dic. 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponible en: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm http://. Acceso em: 30 agosto 2020.

BRASIL. **Portaria IFSP n. 4296, de 14 de dezembro de 2020**. Aprova a atualização da Política de Segurança da Informação e Comunicação - PoSIC no âmbito do Instituto Federal de Educação, Ciência e Educação de São Pauto - IFSP. São Paulo: IFSP, 2020. Disponible en: https://www.ifsp.edu.br/component/content/article?layout=edit&id=2679. Acceso: 11 feb. 2022.

BRASIL. **Emenda Constitucional n. 115**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Atos do Congresso Nacional, 2022. Disponible en: https://in.gov.br/en/web/dou/-/emenda-constitucional-n-115-379516387. Acceso: 11 feb. 2022.

DAVENPORT, T. H. **Ecologia da informação:** Por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

LÉVY, P. **A esfera semântica**. São Paulo: Annablume, 2014.

LIKERT, R. A technique for the measurement of attitudes. **Archives of Psychology**, v. 22, n. 140, p. 55, 1932. Disponible en: https://psycnet.apa.org/record/1933-01885-001. Acceso: 06 nov. 2021.

SOUZA, J. G. S.; ARIMA, C. H.; BELDA, F. R. Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 15, n. 3, p. 1309-1321, jul./set. 2020. Disponible en: https://periodicos.fclar.unesp.br/iberoamericana/article/view/13584. Acceso: 18 oct. 2021.

STOKES, D. E. **O quadrante de Pasteur**: A ciência básica e a inovação tecnológica. Campinas: Editora da Unicamp, 2005.

(cc) BY-NC-SA

UNIÃO EUROPEIA. **Diretiva n. 95/46/CE, de 24 de outubro de 1995**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Estrasburgo: Parlamento Europeu, 1995. Disponible en: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EL. Acceso em: 03 marzo 2021.

UNIÃO EUROPEIA. Opinion 4/2007 on the concept of personal data. **European Commission**, 2007. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acceso el: 03 marzo 2021.

YIN, R. K. **Estudo de caso**: Planejamento e métodos. 2. ed. Porto Alegre: Bookman, 2001.

Cómo hacer referencia a este artículo

SOUZA, J. G. S; BELDA, F. R.; ARIMA, C. H. Análisis de aplicación de la LGPD en una institución educativa pública: Un estudio de caso. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 17, n. 3, p. 1864-1880, jul./sept. 2022. e-ISSN: 1982-5587. DOI: https://doi.org/10.21723/riaee.v17i3.16789

Enviado en: 18/02/2022
Revisiones requeridas en:27/03/2022
Aprobado en: 10/05/2022
Publicado en:01/07/2022

Procesamiento y edición: Editora Ibero-Americana de Educação.
Corrección, formateo, normalización y traducción.

(cc) BY-NC-SA