UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE CIENCIAS JURÍDICAS

DEPARTAMENTO DE DERECHO PENAL

TÍTULO DEL ENSAYO:

"LA RESPONSABILIDAD DEL OFICIAL DE CUMPLIMIENTO FRENTE A LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR FINANCIERO EN EL SALVADOR"

CURSO DE ESPECIALIZACIÓN EN COMPLIANCE Y PREVENCIÓN DEL LAVADO DE DINERO Y ACTIVOS

TRABAJO DE GRADO PARA OBTENER EL TÍTULO DE

LICENCIADO EN CIENCIAS JURÍDICAS

PRESENTADO POR:

DAVID ERNESTO TORRES ORELLANA

DOCENTE ASESOR

MSC. RICARDO ALBERTO MIRANDA MIRANDA

CIUDAD UNIVERSITARIA, SAN SALVADOR, OCTUBRE 2025

ÍNDICE

RESUMEN

En El Salvador, la Ley de Protección de Datos Personales, en adelante "LPDP" o "Ley", requiere que las instituciones nombren a un "*Data Protection Officer*" o Delegado de Protección de Datos, en adelante "DPO". Esta función puede recaer en un empleado interno, como puede ser el Oficial de Cumplimiento, siempre y cuando cumpla con los requisitos, como no tener de conflictos de interés, poseer conocimientos técnicos y jurídicos en protección de datos, y también que posea un certificado que esté debidamente acreditado por una institución certificada en materia de prevención de lavado de dinero y activos y contra el financiamiento del terrorismo.[1]

En el sector financiero, esta práctica es importante, ya que el Oficial de Cumplimiento maneja riesgos legales, de igual forma es importante que este Oficial trabaje de forma independiente y sin presiones. Además, esta designación debe registrarse por escrito de manera clara y conforme a la "Ley".

Si bien la "LPDP" no prohíbe que un Oficial de Cumplimiento sea un "DPO", su designación requiere una evaluación estricta de sus habilidades y destrezas. Es por ello que, es importante entender las funciones y responsabilidades que adquiere este profesional al ser nombrado "DPO" en el sector financiero.

Palabras clave: Oficial de Cumplimiento, Ley de Protección de Datos Personales, sector financiero, Delegado de Protección de Datos.

[1] "Grupo de Trabajo sobre Protección de Datos: *Directrices sobre los delegados de protección de datos*", acceso el 22 de octubre de 2025, https://www.aepd.es/documento/wp243rev01-es.pdf.; "Instituto de Auditores Internos: Certificación AMLCA" IAI, acceso 31 de octubre de 2025, https://www.iaielsalvador.org/certificacion-amlca/.

INTRODUCCIÓN

La implementación de la Ley de Protección de Datos Personales en El Salvador establece un avance importante en saber cómo se gestiona y protege la información personal, sobre todo en el sector financiero. La finalidad de dicha "Ley" es proteger los datos personales, asegurar su seguridad, garantizar la privacidad y dar a las personas la facultad de controlar su información, lo cual genera confianza entre ciudadanos e instituciones.[2] Es por ello que, la "Ley" antes mencionada ordena que las instituciones adopten medidas técnicas y organizativas para proteger la información, incluyendo el nombramiento de un Delegado de Protección de Datos.[3]

En ese sentido, las instituciones financieras deben decidir quién asumirá el rol de Delegado de Protección de Datos. Para buscar la eficiencia y el buen uso de los recursos de la institución, se podría considerar que el Oficial de Cumplimiento asuma este rol. Sin embargo, para que esto ocurra, este Oficial deberá cumplir ciertos requisitos, condiciones y límites legales para evitar conflictos de interés o incumplimientos normativos.[4]

Cumplir con esta Ley de Protección de Datos Personales es importante debido a la gran confidencialidad de los datos que se manejan, como la información de identificación, información crediticia e información patrimonial del titular. Por esto, en la actualidad los Oficiales de Cumplimiento no solo se centran en la prevención del blanqueo de capitales (lavado de dinero) o en la financiación del terrorismo, sino también en la supervisión del tratamiento de datos personales dentro de una institución. Esto quiere decir que los datos se deben recopilar con el consentimiento del titular, respetando sus derechos y protegiéndolos contra el acceso o la divulgación no autorizada, para evitar riesgos que afecten su seguridad.

Por lo tanto, se dice que un Oficial de Cumplimiento adquiere responsabilidades legales, y no solo técnicas, ya que el incumplimiento de estas obligaciones puede llevar a sanciones civiles, administrativas e incluso penales. Por ello, este ensayo busca analizar por qué estos Oficiales son importantes para la privacidad de las instituciones financieras y cómo enfrentan los retos que plantea esta nueva "Ley". Asimismo, se analizarán las

---

[2] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de la República de El Salvador, 2024), artículo 1.
[3] Ibíd**.** 15-22.
[4] Juan Francisco Rodríguez Ayuso, "Requisitos para ser Delegado de Protección de Datos", *Revista Derecho*, (2020), https://www.unir.net/revista/derecho/requisitos-para-ser-delegado-de-proteccion-de-datos/.

funciones y responsabilidades que adquiere el Oficial de Cumplimiento al ser nombrado como Delegado de Protección de Datos, teniendo en cuenta las disposiciones legales correspondientes para el sector financiero y los estándares internacionales de privacidad.[5]

1. RESPONSABILIDAD DEL OFICIAL DE CUMPLIMIENTO DENTRO DEL MARCO NORMATIVO

Para entender las responsabilidades de los Oficiales de Cumplimiento según la Ley de Protección de Datos Personales en el sector financiero, es necesario analizar el marco legal. La protección de datos es un derecho constitucional que permite a la gente decidir sobre su información personal. Así mismo lo regula la Constitución de El Salvador, en su artículo 2, la cual establece que toda persona tiene derecho a la seguridad, por lo tanto, también al honor, la vida privada y a la propia imagen.[6] Por ello, la "LPDP" obliga a las instituciones financieras y otras entidades que manejan datos personales a proteger estos derechos y prevenir usos incorrectos o ilegales de esa información.

La "Ley" requiere que todas las personas y entidades, públicas o privadas, que manejen datos personales sigan los principios básicos como la legalidad, la finalidad legítima, la necesidad, la proporcionalidad, la seguridad y la transparencia. Asimismo, les brinda a los titulares de los datos una serie de derechos, conocidos como ARCO-POL (acceso, rectificación, cancelación, oposición, portabilidad, olvido y limitación del tratamiento de datos), detallados en el artículo 4 de la mencionada "Ley". Estos derechos permiten a los dueños controlar sus datos personales, asegurando su protección y garantizando un uso responsable y eficaz.[7]

Dentro de la "LPDP", se establecen principios rectores sobre el uso de datos personales. Uno de los fundamentales es el consentimiento informado, mencionado en los artículos 5 literal c) y 26 al 31. Este consentimiento debe ser claro, expreso y directo, lo cual es fundamental en el sector financiero, ya que se maneja información delicada sobre datos patrimoniales, crediticios y financieros.[8] Los Oficiales de Cumplimiento designados por la Superintendencia del Sistema Financiero, en adelante "SSF", son importantes porque

[5] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de El Salvador, 2024), artículos 16-22.
[6] Constitución de la República de El Salvador. (El Salvador: Asamblea Legislativa de El Salvador, 1983), artículo 2.
[7] Ibíd. Artículo 4.
[8] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de El Salvador, 2024), artículos 5 literal c) y 26-31.

aseguran que las entidades cumplan con lo estipulado en las diversas leyes correspondientes.[9] Dentro de sus obligaciones está que sean responsables y deben actuar de forma anticipada, previniendo problemas y cuidando los datos personales desde el principio.[10]

Por lo tanto, la "LPDP" establece que se deben adoptar medidas técnicas y administrativas para asegurar el manejo correcto de los datos. En ese sentido, el Oficial de Cumplimiento debe crear una política de privacidad interna, para vigilar la seguridad de los datos, revisar los procesos y asegurar que los titulares tengan un medio para ejercer sus derechos ARCO-POL. De igual forma, el Oficial debe verificar que exista una política de privacidad clara y completa, y que las transferencias internacionales de datos personales se hagan solo con el consentimiento del titular. [11]

1.1 INFRACCIONES Y SANCIONES POR EL INCUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS Y LA LEY DE CIBERSEGURIDAD

En caso que se incumplan las obligaciones establecidas en la Ley de Protección de Datos Personales, la Agencia de Ciberseguridad del Estado, en adelante "ACE", será la encargada de garantizar la protección de la información digital del Estado. Además, esta agencia es la responsable de supervisar que se cumplan las obligaciones que establece la "LPDP".[12] Según la Ley de Ciberseguridad y Seguridad de la Información la "ACE" tiene diversas responsabilidades, dentro de las cuales se encuentran crear políticas y normativas, gestionar incidentes de ciberseguridad, registrar el daño por las amenazas o incidentes a nivel nacional, promover la educación en ciberseguridad, crear auditorias y evaluaciones de riesgos, etc.

---

[9] "Unidad de Investigación Financiera, Fiscalía General de la República: Preguntas frecuentes – oficiales/encargados de cumplimiento titulares y suplentes", UIF/FGR, acceso el 22 de octubre de 2025, https://www.uif.gob.sv/preguntas-oficiales-y encargados/#:~:text=Respuesta%3A%20Los%20oficiales%20de%20cumplimiento,los%20que%20se%20encuentran%2C%20las.

[10] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de El Salvador, 2024), artículos 16-22.; "BLP Legal: Ley para la Protección de Datos Personales en El Salvador", BLP Legal, acceso el 13 de octubre de 2025, https://blplegal.com/es/ley-para-la-proteccion-de-datos-personales-en-el-salvador/.

[11] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de El Salvador, 2024).

[12] "Asamblea Legislativa: Transferencia de recursos permitirá funcionar la Agencia de Ciberseguridad del Estado", Asamblea Legislativa, acceso el 21 de octubre de 2025, https://www.asamblea.gob.sv/node/13555.; Ley de Ciberseguridad y Seguridad de la Información (El Salvador: Asamblea Legislativa de El Salvador, 2024), artículo 7.

Asimismo, esta Agencia de Ciberseguridad cuenta con la responsabilidad de imponer sanciones a las entidades que no cumplan con las reglas estipuladas en los distintos cuerpos normativos correspondientes, dentro de la Ley de Ciberseguridad y Seguridad de la Información, igualmente se encuentran definidos los tipos de infracciones que pueda llegar a cometer cualquier institución con sus respectivas sanciones. Estas infracciones se clasifican en leves, graves y muy graves, con multas que van de 1 a 40 salarios mínimos. Algunos ejemplos de infracciones leves son no informar a los titulares sobre sus derechos o que la institución no tenga una política de privacidad apropiada. Las infracciones graves incluyen el uso de datos para fines no autorizados o la restricción del ejercicio de los derechos. Y, por último, las infracciones muy graves se refieren al uso de datos sin autorización o la venta ilegal de datos personales.[13]

En el caso de las infracciones mencionadas anteriormente, las sanciones pueden ser de tipo administrativo, dependiendo de la naturaleza de la falta cometida. Sin embargo, si una persona incurre en un delito informático, podría enfrentarse a las penas estipuladas en la Ley Especial contra los Delitos Informáticos y Conexos. Esta ley establece sanciones para diversos tipos de delitos relacionados con el acceso no autorizado a sistemas informáticos, el robo de información o la manipulación de datos. Además, contempla delitos como la interferencia con sistemas informáticos, el daño a estos sistemas, violaciones de seguridad, fraudes informáticos y hurtos mediante medios digitales.

También abarca delitos más específicos con el contenido de los datos personales, como la manipulación de registros, la manipulación fraudulenta de tarjetas inteligentes, el acceso indebido a bienes o servicios a través de estos medios, la alteración o daño a la integridad de los datos, la interceptación de comunicaciones y la divulgación no autorizada de información personal. En todos estos casos, quienes sean hallados culpables podrían recibir una pena de prisión que va de uno a doce años, dependiendo de la gravedad del delito.[14]

---

13 Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de la República de El Salvador, 2024), artículos 56-57. Ley de Ciberseguridad y Seguridad de la Información (El Salvador: Asamblea Legislativa de El Salvador, 2024), artículos 8-24.

14 Ley Especial contra los Delitos Informáticos y Conexos (El Salvador: Asamblea Legislativa de El Salvador, 2015) artículos 4-13 y 15-27.

2. LA FUNCIÓN DEL OFICIAL DE CUMPLIMIENTO EN LA IMPLEMENTACIÓN DE POLÍTICAS DE PROTECCIÓN DE DATOS Y GESTIÓN DE CIBERSEGURIDAD

Los Oficiales de Cumplimiento no solo deben aplicar las normas, sino que también, deben asegurarse que estas se cumplan dentro de la institución u organización. Es por ello que, su labor debe ser reactiva, preventiva y formal, buscando evitar sanciones y promover el respeto por los derechos fundamentales de los titulares. La "LPDP" requiere una mejor administración de los datos personales, y los Oficiales de Cumplimiento asumen esta tarea desde una perspectiva técnica, ética y legal, protegiendo los datos, la integridad de las entidades financieras y el derecho a la privacidad de los ciudadanos.[15]

En las entidades supervisadas por la "SSF", como bancos, aseguradoras, administradoras de fondos y cooperativas, tienen la obligación de designar un Oficial de Cumplimiento. Este cargo es fundamental para asegurar que la institución cumpla con lo establecido en la "LPDP" y otras regulaciones correspondientes.[16] El trabajo de este Oficial incluye aspectos prácticos y legales, solicitando una interpretación exacta de las leyes y un entendimiento claro de cómo se aplican dentro de la institución.

Una tarea fundamental del Oficial de Cumplimiento es la creación y aplicación de políticas internas claras sobre el manejo de datos personales, esto implica definir cómo se usarán, guardarán, accederán y eliminarán los datos, así como implementar medidas para evitar su uso indebido.[17] Además, el Oficial debe asegurar que estas políticas cumplan y respeten los principios rectores establecidos en el artículo 5 de la LPDP".[18]

Asimismo, el Oficial de Cumplimiento debe asegurarse que la política de protección de datos no se limite a la teoría, sino que se implemente en la práctica; para ello, debe de programar auditorías internas, revisar cómo se están manejando los datos, descubrir

---

[15] Francisco José Santamaria Ramos, "El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano", *Revista Derecho*, PUCP (2020).; Jorge Agustín Viguri Cordero, "Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos", *Revista de Internet*, *(*2021), https://dialnet.unirioja.es/metricas/documentos/ARTREV/8222608

[16] Ley Contra el Lavado de Dinero y de Activos (El Salvador: Asamblea Legislativa de El Salvador, 2015), artículos 2,10.

[17] "BLP Legal: Ley para la Protección de Datos Personales en El Salvador", BLP Legal, acceso el 14 de octubre de 2025, https://blplegal.com/es/ley-para-la-proteccion-de-datos-personales-en-el-salvador/.

[18] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de El Salvador, 2024), artículo 5.

posibles riesgos y sugerir mejoras.[19] El objetivo de estas auditorías es encontrar cualquier irregularidad u anomalía que pueda conllevar a problemas administrativos o legales. Es por ello que el Oficial de Cumplimiento debe mantenerse informado y actualizado sobre las nuevas leyes, las prácticas en protección de datos para prevenir posibles problemas y además fortalecer las políticas de las instituciones.

Otro aspecto importante a considerar es la respuesta ante problemas de ciberseguridad, dentro de esto se incluyen la identificación de accesos no permitidos, las pérdidas de datos, las filtraciones de información o las violaciones de los derechos de los titulares de los datos. En vista de ello, los Oficiales de Cumplimiento deben poner en marcha los protocolos establecidos por la institución u organización para reducir el daño, investigar el origen del problema e informar a la "ACE". Su función en estos casos debe ser tanto técnica como estratégica, ya que no solo deben resolver el problema, sino también trabajar para que no se vuelva a repetir.[20] Es fundamental que el Oficial de Cumplimiento trabaje de cerca con los equipos de seguridad informática para asegurar una respuesta coordinada y eficaz ante cualquier riesgo de ciberseguridad.

El Oficial de Cumplimiento también desarrolla un papel importante en la capacitación y concientización del personal. Puesto que, puede impartir cursos para asegurar que todos los empleados valoren la importancia de la protección de datos y sepan cómo aplicar las políticas internas en su trabajo cotidiano. Sin embargo, es esencial que dichas capacitaciones deben ser continuas y ajustarse a los distintos niveles de la organización, desde la dirección hasta los empleados con menor jerarquía, para crear una buena cultura interna y concientización sobre la protección de datos.[21]

De igual forma el Oficial de Cumplimiento se desempeña como el principal representante entre la institución financiera y las entidades supervisoras, como la "SSF" y la "ACE", con las que debe mantener una comunicación continua, presentar informes y sobre todo cooperar con las inspecciones. Para esto, se necesita tener un conocimiento claro

[19] Normas para la gestión del riesgo operacional de las entidades financieras NPB4-50 (El Salvador: Superintendencia del Sistema Financiero, 2022), artículo 10.
[20] "ALTA Legal: Protección de datos en El Salvador", ALTA, acceso el 14 de octubre de 2025, https://altalegal.com/comunicacion/proteccion-de-datos-en-el-salvador/.
[21] Guía para formular programas de cumplimiento en materia de competencia (El Salvador: Superintendencia de Competencia, 2022).

y actualizado de los procesos internos de la institución, ya que cualquier error, infracción o irregularidad puede dar lugar a una o varias sanciones.

Además de sus deberes de supervisión, el Oficial de Cumplimiento debe construir una cultura organizacional que valore la privacidad, la gestión ética de los datos y las prácticas responsables, ya que estas acciones influyen directamente en la imagen y la seguridad legal de la institución.[22]

3. LIMITACIONES QUE PRESENTA EL OFICIAL DE CUMPLIMIENTO

La función del Oficial de Cumplimiento es fundamental para que las instituciones financieras cumplan con las leyes. Sin embargo, este trabajo presenta desafíos importantes, de modo que el trabajo de este oficial va más allá de la comprensión de las leyes, pues también debe manejar temas internos como la falta de personal preparado, pocos recursos y la cultura de la empresa.

Además de establecer una cultura institucional fuerte y comunicarse bien con las autoridades reguladoras, los Oficiales de Cumplimiento se enfrentan con retos específicos. Uno de los más importantes es lograr que la institución respete la "LPDP" y las normas actuales de ciberseguridad. Para lograr dichos desafíos este Oficial puede desarrollar cambios internos importantes, como revisar políticas, modernizar contratos y adaptar sistemas técnicos.[23]

Un artículo publicado en la revista Estrategia & Negocios indicó que una gestión administrativa adecuada se debe de complementar con una cultura de seguridad bien estructurada; de lo contrario las leyes pueden quedarse en meras formalidades sin una aplicación real, lo que podría perjudicar el cumplimiento legal y las operaciones de la organización.[24] La revista destaca la necesidad de integrar la seguridad y la protección de

---

[22] "García & Bodán: Ley para la Protección de Datos Personales*:* Un avance para el ecosistema digital de El Salvador", García & Bodán, acceso el 10 de octubre de 2025, https://garciabodan.com/ley-para-la-proteccion-de-datos-personales-un-avance-para-el-ecosistema-digital-de-el-salvador/.

[23] "ALTA Legal: Protección de datos en El Salvador", ALTA*,* acceso el 14 de octubre de 2025, https://altalegal.com/comunicacion/proteccion-de-datos-en-el-salvador/.

[24] "Estrategia y Negocios (E&N): Retos y claves ante nuevas leyes de ciberseguridad y protección de datos en El Salvador"*,* E&N, acceso el 10 de octubre de 2025, https://www.revistaeyn.com/tecnologia-cultura-digital/retos-y-claves-ante-nuevas-leyes-de-ciberseguridad-y-proteccion-de-datos-en-el-salvador-KL25486419.

datos en toda la empresa, desde los líderes hasta los empleados, para protegerla de las amenazas y vulnerabilidades.

3.1 LA ESCASEZ DE PERSONAL ESPECIALIZADO Y EL MANEJO DE LOS RIESGOS OPERATIVOS Y TECNOLÓGICOS

Un problema crucial que enfrenta este Oficial de Cumplimiento es la escasez de personal especializado; este es un problema muy grave que pueden presentar las instituciones, ya que tienen la falta de formación esencial en la privacidad y seguridad digital, lo que conlleva a la falta de calidad y capacidad de respuesta ante los problemas que puedan llegar a surgir.

Es por esto que las instituciones se ven obligadas a buscar apoyo externo o a poner en marcha soluciones temporales, lo que no siempre garantiza el cumplimiento adecuado de las normas. La falta de personal capacitado puede dar lugar a informes de riesgos incompletos, respuestas lentas a los problemas de seguridad y una supervisión interna deficiente.[25]

Asimismo, es importante reconocer que la cultura interna juega un papel fundamental. Como se indicó en el artículo proporcionado por la revista E&N, todavía hay instituciones que no ven la protección de datos como parte importante de su identidad y deber social. Es decir, no basta con solo tener documentos que marquen políticas; sino que es necesario que cada empleado las apliquen día a día. Sin este compromiso de todos, los esfuerzos de algunos resultan ineficaces; por lo que se debe de capacitar a los empleados, comunicar las políticas de privacidad de forma clara y además fomentar que todos en la institución se preocupen por proteger los datos.[26]

Si bien el trabajo del Oficial de cumplimiento se enfoca en supervisar, prevenir y anticipar cualquier tipo de riesgo o anomalía que pueda presentar la institución, siempre están expuestos a los riesgos de fugas de datos, errores humanos en la gestión de la información y en algunos casos a ciberataques que puedan comprometer la integridad de la institución; por lo que, identificar estos riesgos es una de las primeras tareas de este Oficial.

---

[25] "ALTA Legal: Protección de datos en El Salvador", ALTA, acceso el 14 de octubre de 2025, https://altalegal.com/comunicacion/proteccion-de-datos-en-el-salvador/.

[26] "Estrategia y Negocios (E&N): Retos y claves ante nuevas leyes de ciberseguridad y protección de datos en El Salvador", acceso el 10 de octubre de 2025, https://www.revistaeyn.com/tecnologia-cultura-digital/retos-y-claves-ante-nuevas-leyes-de-ciberseguridad-y-proteccion-de-datos-en-el-salvador-KL25486419.

Para controlar estos riesgos, éste debe examinar de manera continua los efectos de los procedimientos internos, las debilidades tecnológicas y los posibles fallos en la estructura de datos.

Como se ha establecido anteriormente el Oficial de Cumplimiento se enfrenta a distintos tipos de riesgos o posibles riesgos que abarcan desde problemas de seguridad hasta accesos no autorizados, que pueden conllevar hasta la pérdida de credibilidad de la institución con los titulares. Es por ello que, no solo basta contar con políticas de privacidad bien estructuradas sino debe de haber un responsable que aparte de fomentar a los demás empleados a seguirlas, debe de responder con rapidez, eficacia y sobre todo transparencia ante estos riesgos.

El manejo de estos problemas de seguridad no solo significa corregir los problemas técnicos, sino el deber actuar de manera rápida y organizada ante estas situaciones que puedan poner en riesgo la información personal de los usuarios. En estos casos el Oficial de Cumplimiento cumple un rol fundamental, ya que, es el encargado de detectar el problema y además coordinar la respuesta conjuntamente con los equipos correspondientes, y es donde se asegura que se tomen las medidas necesarias para proteger los datos y evitar que el problema se vuelva a repetir.

4. VIGILANCIA NORMATIVA Y CUMPLIMIENTO REGULATORIO

Para garantizar el cumplimiento a las leyes y procedimientos internos dentro de cualquier institución financiera, el Oficial de Cumplimiento tiene la responsabilidad fundamental de mantener una revisión continua de las regulaciones establecidas por el Banco Central de Reserva, en adelante "BCR", prestando especial atención a las normativas NRP-23 y NRP-24, las cuales establecen nuevos requisitos de seguridad tecnológica, es por ello que el Oficial de Cumplimiento debe estar al tanto de cualquier cambio en las regulaciones aplicables, además debe ser capaz de coordinar y adecuar estos cambios a lo requerido por la institución. [27]

Es así que la responsabilidad que asume este Oficial no solo implica que se mantenga informado sobre las actualizaciones y cambios en estas regulaciones, sino

[27] Normas técnicas para la gestión de la seguridad de la información (NRP-23), (El Salvador: Banco Central de Reserva de El Salvador, 2020), artículos 9, 23, 30 y 31.; Normas técnicas para el sistema de gestión de la continuidad del negocio (NRP-24) (El Salvador: Banco Central de Reserva de El Salvador, 2020), artículos 4, 5, 10 y 14.

también logre una comprensión total de su uso práctico en las actividades diarias. Lo cual conlleva analizar cuidadosamente cada aspecto de las normas, desde los requisitos formales hasta las consecuencias al momento de tomar una decisión y la realización de tareas.

4.1 LA COORDINACIÓN CON LOS DEPARTAMENTOS TECNOLÓGICOS Y JURÍDICOS

Para la actualización de los sistemas es necesario tener una comunicación constante con otros departamentos de la institución, por ejemplo, con el departamento de tecnología y el departamento jurídico, ya que esta coordinación es fundamental para garantizar la aplicación de las medidas técnicas y la eficacia de los procesos de protección de datos.[28]

Para lograr esto, es importante establecer canales de comunicación claros y directos entre los equipos involucrados. De igual forma, las reuniones periódicas, tanto presenciales como virtuales, pueden ser de gran ayuda para analizar los avances, resolver problemas y tomar decisiones en conjunto. Dentro de estas reuniones deberán de estar los representantes de todos los departamentos afectados, dando así sus puntos de vista y buscando las medidas pertinentes para solventar el problema que presentan, garantizando siempre cumplir con lo estipulado en las regulaciones pertinentes.

De igual forma, es importante documentar cuidadosamente cada paso del proceso de mejora. Esto incluye el desarrollo de manuales técnicos, guías de usuario y procedimientos de solución de problemas. Por esto se dice que una documentación completa y detallada puede ser de gran valor para futuros mantenimientos y actualizaciones, y también para capacitar a nuevos miembros del equipo de trabajo.[29]

5. OBJETIVOS DEL CUMPLIMIENTO: EVITAR SANCIONES Y PRESERVAR LA OPERATIVIDAD

En principio, la coordinación entre las instituciones y los entes reguladores se enfoca en dos objetivos principales. El primero, busca asegurar que las organizaciones cumplan con las regulaciones vigentes, con la finalidad de evitar posibles multas o sanciones impuestas por las autoridades supervisoras; y el segundo, busca salvaguardar la

[28] Normas para la gestión del riesgo operacional de las entidades financieras NPB4-50 (El Salvador, Superintendencia del Sistema Financiero, 2022.

[29] Guía para formular programas de cumplimiento en materia de competencia (El Salvador: Superintendencia de Competencia, 2022), página 33-34.

integridad y la estabilidad de las operaciones de las instituciones.[30] Es por ello que dicha coordinación es con la finalidad de asegurar el cumplimiento normativo dentro de la organización, aparte que, con estas medidas, se reducen riesgos de funcionamiento y se fortalece la confianza en la institución.

6. COORDINACIÓN DEL OFICIAL CON ENTIDADES REGULADORAS

El Oficial de Cumplimiento debe asumir la responsabilidad de establecer una buena comunicación entre los diversos entes reguladores, tales como la "SSF", la "ACE" y el "BCR". Es por ello que el Oficial de Cumplimiento posee como objetivo primordial el garantizar que tanto los titulares afectados ante cualquier problema y las autoridades competentes sean informados de inmediato; esto no solo es por cumplir una obligación legal establecida en la "LPDP", sino que también refleja un compromiso con la transparencia que debe poseer dicho Oficial, y además esto es esencial para garantizar una confianza con el usuario.[31]

Si bien dicha coordinación es fundamental para el buen desempeño del sistema, es posible que ocurran dificultades por las distintas prioridades de cada institución. Estas diferencias podrían llevar a la repetición de actividades, retrasos en el cumplimiento de tareas y confusión entre las instituciones. Para reducir este tipo de dificultades, se puede sugerir promover una comunicación clara y fluida entre las instituciones, también se puede dar una planificación en conjunto y guardar registros adecuados de los procesos.

Asimismo, se habla acerca de la importancia que puede tener la Unidad de Investigación Financiera, en adelante UIF, si bien no tienen una relación directa con el tema de protección de datos personales, puede aportar con un papel complementario, es decir, puede llegar a reforzar el tema del cumplimiento financiero, ya que, esta institución tiene como objetivo gestionar en su totalidad los riesgos de privacidad y seguridad de la información. Por lo que las directrices que están estipuladas en su instructivo son esenciales

[30] Normas técnicas para la gestión de la seguridad de la información (NRP-23), (El Salvador: Banco Central de Reserva de El Salvador, 2020); Normas técnicas para el sistema de gestión de la continuidad del negocio (NRP-24) (El Salvador: Banco Central de Reserva de El Salvador, 2020).

[31] Ley de Supervisión y Regulación del Sistema Financiero (El Salvador: Superintendencia del Sistema Financiero, 2024); "Asamblea Legislativa: Transferencia de recursos permitirá funcionar la Agencia de Ciberseguridad del Estado", Asamblea Legislativa, acceso el 21 de octubre de 2025, https://www.asamblea.gob.sv/node/13555.; Ley de Ciberseguridad y Seguridad de la Información (El Salvador: Asamblea Legislativa, 2024), artículo 7.

para orientar el trabajo del Oficial de cumplimiento, ya que estas incluyen los principios de prevención, control y reporte que son fundamentales para asegurar que se cumplan los lineamientos establecidos por las entidades regulatorias pertinentes.

Es por ello que la coordinación que tiene el Oficial de Cumplimiento con las entidades reguladoras y contraloras debe ser fundamental, constante, pero sobre todo eficiente. Por lo que las entidades como la "SSF", la "ACE" y el "BCR" no solo aportan beneficios en la orientación técnica en cuanto al cumplimiento normativo financiero, sino que también aportan conocimientos claves sobre la supervisión y la gestión de incidentes de ciberseguridad. Con este apoyo que le brindan al Oficial logra implementar de manera efectiva todas las medidas y recomendaciones necesarias para garantizar que se cumplan todos los lineamientos normativos.

7. LOS RIESGOS Y SANCIONES ANTE EL INCUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

El Oficial de Cumplimiento tiene una función fundamental en el cumplimiento de las instituciones financieras según lo estipulado por la "LPDP". El incumplimiento de esta Ley podría generar serias consecuencias, poniendo en riesgo la reputación y el funcionamiento de la institución. Por tanto, es fundamental conocer las consecuencias legales, los riesgos institucionales y las medidas necesarias para prevenir estos problemas.

Si una institución financiera no cumple con lo estipulado en la "LPDP", el ente regulador, en este caso la "ACE", tiene la facultad de imponer sanciones, tales como multas económicas. La ley de Ciberseguridad y Seguridad de la Información establece medidas que tienen como objetivo tanto sancionar como promover el respeto de los derechos personales en el manejo de información personal, dentro de ellas se pueden mencionar la pérdida de confianza, reputación y credibilidad por parte de clientes y socios hacia la institución, lo que resultaría en problemas económicos serios a largo plazo.[32]

8. MEDIDAS PARA EL CUMPLIMIENTO DE LA "LPDP"

A manera de reducir estos riesgos, el Oficial de Cumplimiento debe ir más allá del simple cumplimiento de la Ley de Protección de Datos Personales, por lo que es fundamental que implemente reglas claras, políticas de privacidad, capacite al personal

[32] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de El Salvador, 2024; Ley de Ciberseguridad y Seguridad de la Información (El Salvador: Asamblea Legislativa, 2024.

constantemente e integre herramientas tecnológicas que protejan y supervisen la información de las personas.[33]

Es por ello que las políticas de privacidad deben ser accesibles y fáciles de entender, lo que permitirá a las personas ejercer sus derechos sin dificultad. Esta medida no solo cumple con lo establecido en la "Ley", sino que también fortalece la confianza y el respeto mutuo entre la institución financiera y sus clientes, generando un entorno de responsabilidad que beneficia a todos. La aplicación adecuada de estos métodos determina la relación entre la institución y los titulares, promoviendo una cultura organizacional dirigida a la protección y el manejo ético de la información personal.

También la inversión en tecnologías de seguridad avanzadas y la revisión constante de estos sistemas resulta fundamental para mantener la seguridad de la información y asegurar el cumplimiento normativo en el futuro.

Asimismo, para la capacitación del personal, se pueden realizar simulacros de problemas de seguridad, con la finalidad de preparar a los empleados ante los posibles riesgos, y a la vez, ayudaría a identificar las debilidades en los mecanismos de respuesta, mejorando el trabajo en equipo entre los diferentes departamentos de la institución.[34]

8.1 COLABORACIÓN CON EXPERTOS E IMPLEMENTACIÓN DE HERRAMIENTAS PARA EL FORTALECIMIENTO INSTITUCIONAL

Con la finalidad de asegurar la protección de los datos personales, los organismos e instituciones implementan medidas que, con la ayuda de profesionales externos en ciberseguridad, tienen como objetivo mejorar los procedimientos internos.[35]

Por ello, para promover la transparencia entre los titulares de los datos y las instituciones, es recomendable desarrollar una página web donde cada persona pueda acceder sin dificultad a sus datos personales y establecer su configuración de privacidad. También dentro de esta página se podría incluir un apartado con las preguntas más comunes sobre la protección de datos.[36]

---

[33] Guía para formular programas de cumplimiento en materia de competencia (El Salvador: Superintendencia de Competencia, 2022), página 30; 3. Pablo Contreras Vásquez, Marcelo Drago Aguirre y Pablo Viollier Bonvin, "*Compliance y protección de datos personales (*Chile: DER Ediciones, 2024), 119.

[34] Guía para formular programas de cumplimiento en materia de competencia (El Salvador: Superintendencia de Competencia, 2022), página 30.

[35] Guillermo Pacheco González, *Cultura de control: Cambios Transformacionales* (México: Editorial Mexicana, 2025), 11-13.

[36] Angely Valentina Montiel Zamora, "Un futuro de transparencia y protección en la era digital", *Revista*, (2025), https://revistas.umng.edu.col/article/download.

Es así que las instituciones a día de hoy establecen un canal de comunicación directo y eficiente para que las personas puedan reportar cualquier sospecha de violación de datos y así recibir una respuesta oportuna e inmediata sobre cualquier inconveniente o irregularidad que tengan.

8.2 INCENTIVOS Y PROGRAMAS PARA LA FOMENTACIÓN DE UNA BUENA RESPONSABILIDAD INTERNA Y EXTERNA

Se reconoce que la responsabilidad interna es un desafío constante que poseen todas las instituciones, sin embargo, esto se podría fortalecer a través de un programa de incentivos que premie al personal por su esfuerzo y dedicación a la protección de datos. Dentro de estos incentivos se pueden brindar recompensas o reconocimientos a las personas que demuestren un uso responsable de la protección misma.[37]

De igual forma las instituciones tienen la potestad de implementar medidas disciplinarias para fortalecer la responsabilidad interna y con el propósito de enfatizar en cumplir la normativa propia de la institución como la legislación pertinente. Estas medidas o procedimientos a seguir deben ser claras y transparentes con todos los involucrados desde los trabajadores de poco rango hasta los altos directivos. Como, por ejemplo, se puede implementar una política de cero tolerancias hacia las infracciones de datos, en la que se estén monitoreando cada cierto tiempo que se cumpla efectivamente todos los lineamientos; en un dado caso que esta política se llegue a incumplir el que cometiere dicha infracción pudiera contraer desde multas hasta despidos.[38]

Es un hecho que tanto el Oficial de Cumplimiento como el resto del personal de la institución deben recibir una formación constante. Para ello, se pueden implementar distintas actividades, que pueden ser tanto internas como externas.[39]

Entre las actividades internas, se pudieran impartir capacitaciones o foros diseñados a medida de las necesidades de la institución. Estas pueden ser impartidas por el propio

[37] Guía para formular programas de cumplimiento en materia de competencia (El Salvador: Superintendencia de Competencia, 2022), páginas 40-42.
[38] Guía para formular programas de cumplimiento en materia de competencia (El Salvador: Superintendencia de Competencia, 2022), página 42.
[39] Ignacio Danvila del Valle, *La valoración y formación de las personas en las organizaciones* (Madrid: Netbiblo, 2011), 120-122.

personal con conocimientos especializados, en donde abordarían temas específicos relacionados con la privacidad y la seguridad de la información.[40]

Y como actividades externas, se pudieran organizar seminarios especializados en temas concretos sobre la privacidad y la seguridad que debe poseer toda institución. También se pudieran obtener certificaciones internacionales reconocidas, que garanticen que poseen cierto nivel de conocimiento en el ámbito de privacidad y seguridad. Dentro de estas certificaciones, se pueden encontrar las normas ISO, las cuales son estándares internacionales elaborados por expertos, que establecen lineamientos o requisitos para distintos tipos de productos o servicios con la finalidad de garantizar que dicha institución o empresa cumpla con una calidad, seguridad y eficiencia adecuada. [41]

Estas normas ISO van encaminadas a la gestión, implementación y protección de la seguridad en la información personal. Por ejemplo, la norma ISO 27001 se centra en ayudar a las organizaciones a establecer sistemas de gestión de seguridad de la información para proteger sus datos y evitar riesgos. Adicionalmente esta norma proporciona un marco de referencia para identificar, evaluar y gestionar los riesgos de seguridad de la información, y establece los requisitos para implementar un sistema de gestión de seguridad de la información eficaz.

También se puede encontrar la norma ISO 27002, la cual ofrece una guía práctica para implementar controles de seguridad de la información, es decir, esta norma proporciona recomendaciones sobre cómo seleccionar, implementar y gestionar los controles de seguridad de la información, y además ayuda a las organizaciones a proteger los datos confidenciales de manera eficaz.

Igualmente se encuentra la norma ISO 27701, que es una norma que establece los requisitos para establecer un sistema de gestión de información de privacidad, es decir, se centra en la protección de datos personales. También se dice que, esta norma sirve como extensión a las ISO 27001 y la ISO 27002, ya que, amplían los requisitos para establecer una mejor gestión de privacidad, dando como fin ayudar a las organizaciones a cumplir con las leyes y regulaciones de protección de datos personales.[42]

---

[40] Gabriela Guiñazú. *Capacitación efectiva en la empresa* (Argentina: Invenio, 2004), 111.

[41] Ibíd. 112.

[42] Duban Oswaldo Palacios Portilla, "Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el área de informática de la cooperativa del Magisterio de Túquerres bajo la norma ISO 27001" (Tesis de grado, Universidad Nacional Abierta y a Distancia, 2015), 25-27.

9. CASO QUE EVIDENCIA LA PROBLEMÁTICA

Considerando que las instituciones y organizaciones están constantemente expuestas a peligros por una supervisión inadecuada en la protección de datos personales, es fundamental analizar las consecuencias de estas fallas. Es por ello que a continuación, se mostrará un caso que demuestra de qué manera la falta de una buena gestión en este ámbito puede causar problemas serios para una institución.

Una institución financiera, que estaba bajo la supervisión de la Superintendencia del Sistema Financiero, sufrió un problema de seguridad informática que resultó en la filtración de datos personales de sus clientes. El ataque fue llevado a cabo por un grupo de hackers autodenominado RansomHub, el cual consiguió infiltrarse en la infraestructura interna de la institución y extraer información personal de los usuarios, dentro de esta información se encuentran nombres completos, números de identificación personal y detalles sobre los ingresos de los clientes.

El problema se volvió grave cuando el grupo delictivo al no recibir el pago del dinero exigido por la información extraída, decidió divulgar la información en la dark web. Este hecho convirtió el problema en uno de los más serios que ha enfrentado una institución financiera no bancaria en el país. En un inicio, la institución comunicó que sus sistemas se encontraban controlados y que la información de sus clientes no había sido filtrada. Sin embargo, días después, varios medios de comunicación a nivel nacional confirmaron el acceso de los archivos en línea, lo que provocó cuestionamientos acerca de cómo dicha institución manejó el problema desde el inicio.[43]

Este problema demostró dos aspectos clave: en primer lugar, que hasta las instituciones de tamaño medio o que parecen estar protegidas pueden ser objeto de ataques complicados; y, en segundo lugar, que la reacción de una institución ante una situación crítica tiene que ser técnica y rápida.

---

https://repository.unad.edu.co/bitstream/handle/10596/3817/1085255001.pdf?sequence=1&isAllowed=y; Luis Enrique Giraldo Cepeda, "Análisis para la implementación de un Sistema de Gestión de la Seguridad de la Información según la norma ISO 27001en la empresa Servidoc s.a." (Tesis de grado, Universidad Nacional Abierta y a Distancia, 2016), 20. https://repository.unad.edu.co/bitstream/handle/10596/6341/16453917.pdf?sequence=1&isAllowed=y

[43] David Bernal, "Hackers exponen datos de clientes de la Sociedad de Ahorro y Crédito Constelación S.A. de C.V.", *La Prensa Gráfica* (26 de abril de 2024).

Es por ello que, el rol del Oficial de Cumplimiento es fundamental, ya que, en primer momento debe informar a las autoridades pertinentes como la "ACE" y la "SSF", y en ese mismo momento igual informar a los titulares de los datos sobre el problema; y, en segundo lugar, poner en marcha los procedimientos para intentar solventar el problema en colaboración con los departamentos técnicos y jurídicos.

Sin embargo, la falta de transparencia en la comunicación pública también afectó la confianza de los clientes y provocó sospechas sobre la integridad y credibilidad de la institución. En estos conflictos, el Oficial de Cumplimiento no solo debe actuar según la Ley de Protección de Datos Personales (LPDP), sino también asegurar de la integridad de la institución, garantizando que se respeten los principios de legalidad, transparencia y seguridad, principalmente cuando los derechos fundamentales de los usuarios se han visto perjudicados.

En ese sentido, es fundamental mencionar que el rol del Oficial de Cumplimiento no puede limitarse a funciones reactivas, es decir, solo actuar cuando ocurra un problema, sino, que debe estar en constante preparación para prevenir, actuar y sobre todo comunicar a las entidades correspondientes. Es por ello que fortalecer su rol no es solo una cuestión de formalismo, sino también tener un compromiso con una gestión más experimentada, accesible, eficaz y sobre todo ética.

En relación a lo antes mencionado, existen distintas recomendaciones prácticas que se pueden implementar para mejorar el desempeño sobre el cumplimiento tanto operacional como jurídico. Uno de los pasos más importantes para fortalecer el rol del Oficial de Cumplimiento es invertir en una capacitación continua, es decir, no simplemente adquirir conocimientos generales acerca de las operaciones o de la legislación vigente, sino también mantenerse al día en temas fundamentales como la protección de datos personales, la ciberseguridad y la legislación financiera, ello con el fin de anticipar los riesgos y poder tomar decisiones más responsables e informadas.

También es importante valorar que las instituciones financieras deben contar con los procedimientos internos claros y correspondientes a la "LPDP". Dentro de estos procedimientos se deben definir quién es el responsable en actuar ante cualquier problema,

además de cómo se gestionarán dichos problemas y cómo se protegerán los derechos de los titulares de los datos ante cualquier problema.[44]

Es por ello que, el Banco Central de Reserva estableció unas regulaciones técnicas que no pueden ignorarse y deben incorporarse a los procesos diarios que implementar las instituciones, dentro de ellas se encuentran las NRP-23 y NRP-24, las cuales establecen requisitos de seguridad tecnológica.

La norma NRP-23 establece la forma en que las instituciones están obligadas a ordenar y analizar sus mecanismos internos, con el fin de evitar equivocaciones o estafas, asegurando trámites claros y eficaces. Y con respecto a la norma NRP-24, esta se enfoca en la identificación y gestión de riesgos, ayudando a las organizaciones en la prevención y reducción de posibles amenazas, ya sean operativas o de seguridad. Por ello se afirma que estas normas son fundamentales para resguardar correctamente de datos personales, ya que establecen un sistema que garantiza que los datos confidenciales de los titulares se administren con la máxima protección.[45]

Como se ha mencionado anteriormente, es fundamental optar por la mejora continua del Oficial de cumplimiento, poner en práctica los procedimientos brindados por las distintas entidades conocedoras y contraloras, también es importante crear una cultura institucional que vele por el respeto a la privacidad, el respeto a los derechos de las personas y además que posea una ética institucional sólida. A partir de ahí es en donde al Oficial se le atribuye otra responsabilidad, la cual es convertirse en un agente de cambio dentro de la institución, es decir, que promueva buenas prácticas, dando el ejemplo de cómo se debe actuar y sobre todo asegurarse que todo el personal entienda que tan importante es proteger los datos personales de las personas.

10. IMPLEMENTACIÓN DE SISTEMAS PARA FORTALECER LA CAPACIDAD INSTITUCIONAL

También los organismos o instituciones nacionales pueden ser partícipes en esto, porque pueden promover una red nacional de Oficiales de Cumplimiento normativo, en la cual les permitiría compartir vivencias, experiencias, recibir alertas, recibir reportes, brindar

[44] Ley de Protección de Datos Personales (El Salvador: Asamblea Legislativa de El Salvador, 2024), artículo 50.

[45] Normas técnicas para la gestión de la seguridad de la información (NRP-23), (El Salvador: Banco Central de Reserva de El Salvador, 2020).; Normas técnicas para el sistema de gestión de la continuidad del negocio (NRP-24) (El Salvador: Banco Central de Reserva de El Salvador, 2020).

medidas preventivas y coordinar acciones para responder ante cualquier tipo de riesgo de forma rápida y eficaz. Igualmente, dentro de esta red, se puede compartir experiencias no solo a nivel nacional sino a nivel internacional, acerca de los problemas que han tenido instituciones de otros países y cómo han logrado solventarlos, todo ello para el fortalecimiento de las capacidades de respuesta institucional, a la mejora continua de los mecanismos de cumplimiento normativo y al forjamiento de una confianza sólida entre los participantes.

11. CONCLUSIÓN

Si bien el cargo de un Oficial de Cumplimiento y un Delegado de Protección de Datos no son los mismos, porque cada uno posee un grado de dificultad, una alta dedicación, y además contraen obligaciones específicas. Para el caso del oficial, también es obligatorio que cuente con una acreditación en prevención de lavado de dinero y activos y contra el financiamiento del terrorismo, proporcionado por una institución extranjera certificada en dicha materia. Sin embargo, estos roles podrían ser asumidos por una sola persona, siempre y cuando se compruebe que este cumpla con los requisitos mínimos para desempeñar dicho cargo, dentro de ellos están que tenga un conocimiento amplio sobre las normativas y los procedimientos que posea la institución, también esta persona no debe que poseer ningún tipo de conflicto de intereses con la institución.

Sin embargo, esta fusión podría conllevar a una sobrecarga laboral, ya que cada uno de los cargos requiere el cumplimiento de obligaciones específicas, como informes, auditorías y asesoramientos. También esta unificación pudiera afectar a la propia independencia, objetividad, pero sobre todo a la calidad de trabajo, lo que conlleva a la posibilidad de cometer errores o tener retrasos en los resultados. Por lo tanto, si una institución decide combinar ambos cargos, debe asegurar que la persona designada tenga una correcta preparación, cuente con los recursos institucionales y además que le aseguren que tiene un tiempo necesario para cumplir con sus obligaciones adecuadamente, ello con la finalidad de no poner en riesgo la protección de datos ni el cumplimiento normativo.

Es así en donde el cumplimiento de la Ley de Protección de Datos Personales en el sector financiero, no solo tiene que verse como una obligación jurídica formal, sino como una necesidad para generar credibilidad, sinceridad, confidencialidad y responsabilidad institucional. Es por eso que, los Oficiales de Cumplimiento no son únicamente expertos

que analizan las normativas y realizan reportes, sino que también son profesionales integrales, que pueden garantizar la protección de los derechos de las personas y las actividades relacionadas con la prevención del lavado de dinero y activos.

Es evidente que cuando las instituciones no invierten en estos profesionales ni les ofrecen independencia ni seguridad, las filtraciones de datos, las conductas deshonestas o la falta de respuestas correctas pueden afectar significativamente la reputación y la credibilidad ante las personas. Esto demuestra que el cumplimiento de las normas no debe ser solo una formalidad; sino como una necesidad y a la vez una obligación que poseen las instituciones para que cuenten con sistemas y procedimientos bien establecidos, personal capacitado y el compromiso de todo el personal.

Es así que, fortalecer la función de los Oficiales de Cumplimiento también puede ayudar a las instituciones financieras a cumplir aún más con sus obligaciones legales, al comportamiento ético y la protección de la información privada del titular. Es sí que la capacitación del Oficial y del propio personal no se tiene que ver como un gasto, sino como una inversión en sostenibilidad, transparencia y seguridad jurídica; ya que, con esta inversión igualmente les permitiría a las instituciones a reducir riesgos, prevenir infracciones, garantizar sus ingresos económicos provienen de actividades lícitas y a la vez fortalecer la imagen de la institución.

BIBLIOGRAFÍA

"Asamblea Legislativa: Transferencia de recursos permitirá funcionar la Agencia de Ciberseguridad del Estado", Asamblea Legislativa, acceso el 21 de octubre de 2025, https://www.asamblea.gob.sv/node/13555.

"ALTA Legal: Protección de datos en El Salvador", ALTA, acceso el 14 de octubre de 2025, https://altalegal.com/comunicacion/proteccion-de-datos-en-el-salvador/.

"BLP Legal: Ley para la Protección de Datos Personales en El Salvador", BLP Legal, acceso el 13 de octubre de 2025, https://blplegal.com/es/ley-para-la-proteccion-de-datos-personales-en-el-salvador/.

Bernal, David. “Hackers exponen datos de clientes de la Sociedad de Ahorro y Crédito Constelación S.A. de C.V.”, *La Prensa Gráfica* (26 de abril de 2024).

Constitución de la República de El Salvador. El Salvador: Asamblea Legislativa de El Salvador, 1983.

Contreras Vásquez, Pablo, Marcelo Drago Aguirre y Pablo Viollier Bonvin. *Compliance y protección de datos personales.* Chile: DER Ediciones, 2024.

Danvila del Valle, Ignacio. *La valoración y formación de las personas en las organizaciones*. Madrid: Netbiblo, 2011.

“Estrategia y Negocios (E&N): Retos y claves ante nuevas leyes de ciberseguridad y protección de datos en El Salvador”, acceso el 10 de octubre de 2025, https://www.revistaeyn.com/tecnologia-cultura-digital/retos-y-claves-ante-nuevas-leyes-de-ciberseguridad-y-proteccion-de-datos-en-el-salvador-KL25486419.

“Grupo de Trabajo sobre Protección de Datos: Directrices sobre los delegados de protección de datos”, acceso el 22 de octubre de 2025, https://www.aepd.es/documento/wp243rev01-es.pdf.

Guía para formular programas de cumplimiento en materia de competencia. El Salvador: Superintendencia de Competencia, 2022.

“García & Bodán: Ley para la Protección de Datos Personales: Un avance para el ecosistema digital de El Salvador”, García & Bodán, acceso el 10 de octubre de 2025, https://garciabodan.com/ley-para-la-proteccion-de-datos-personales-un-avance-para-el-ecosistema-digital-de-el-salvador/.

Guiñazú, Gabriela. Capacitación efectiva en la empresa. Argentina: Invenio, 2004.

Giraldo Cepeda, Luis Enrique. “Análisis para la implementación de un Sistema de Gestión de la Seguridad de la Información según la norma ISO 27001 en la empresa Servidoc s.a.”. Tesis de grado, Universidad Nacional Abierta y a Distancia, 2016. https://repository.unad.edu.co/bitstream/handle/10596/6341/16453917.pdf?sequence=1&isAllowed=y

“Instituto de Auditores Internos: Certificación AMLCA” IAI, acceso 31 de octubre de 2025, https://www.iaielsalvador.org/certificacion-amlca/.

Ley de Protección de Datos Personales. El Salvador: Asamblea Legislativa de El Salvador, 2024.

Ley de Ciberseguridad y Seguridad de la Información. El Salvador: Asamblea Legislativa de El Salvador, 2024.

Ley Especial contra los Delitos Informáticos y Conexos. El Salvador: Asamblea Legislativa de El Salvador, 2015.

Ley Contra el Lavado de Dinero y de Activos. El Salvador: Asamblea Legislativa de El Salvador, 2015.

Ley de Supervisión y Regulación del Sistema Financiero. El Salvador: Superintendencia del Sistema Financiero, 2024.

Montiel Zamora, Angely Valentina. "Un futuro de transparencia y protección en la era digital", *Revista*, (2025), https://revistas.umng.edu.col/article/download.

Normas para la gestión del riesgo operacional de las entidades financieras NPB4-50. El Salvador: Superintendencia del Sistema Financiero, 2022.

Normas técnicas para la gestión de la seguridad de la información (NRP-23). El Salvador: Banco Central de Reserva de El Salvador, 2020.

Normas técnicas para el sistema de gestión de la continuidad del negocio (NRP-24). El Salvador: Banco Central de Reserva de El Salvador, 2020.

Pacheco González, Guillermo. *Cultura de control: Cambios Transformacionales*. México: Editorial Mexicana, 2025.

Palacios Portilla, Duban Oswaldo. "Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el área de informática de la cooperativa del Magisterio de Túquerres bajo la norma ISO 27001". Tesis de grado, Universidad Nacional Abierta y a Distancia,2015.https://repository.unad.edu.co/bitstream/handle/10596/3817/1085255001.pdf?sequence=1&isAllowed=y

Rodríguez Ayuso, Juan Francisco: "Requisitos para ser Delegado de Protección de Datos", *Revista Derecho*, (2020), https://www.unir.net/revista/derecho/requisitos-para-ser-delegado-de-proteccion-de-datos/.

Santamaría Ramos, Francisco José. "El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano". *Revista Derecho*, (2020).

"Unidad de Investigación Financiera, Fiscalía General de la República: Preguntas frecuentes – oficiales/encargados de cumplimiento titulares y suplentes", UIF/FGR, acceso

el 22 de octubre de 2025, https://www.uif.gob.sv/preguntas-oficiales-y encargados/#:~:text=Respuesta%3A%20Los%20oficiales%20de%20cumplimiento,los%20que%20se%20encuentran%2C%20las.

Viguri Cordero, Jorge Agustín. “Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos”. *Revista de Internet*, Derecho y Política, (2021), https://dialnet.unirioja.es/metricas/documentos/ARTREV/8222608.