UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS
ESCUELA DE INGENIERÍA EN INFORMÁTICA

TRABAJO FINAL DE GRADUACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN INGENIERÍA EN INFORMÁTICA

PROPUESTA DE UN PROCEDIMIENTO DE REVISIÓN Y CONTROL DE SEGURIDAD DE LOS DESARROLLOS WEB DEL DEPARTAMENTO DE MERCADEO, BASADO EN LA NORMATIVA ISO 27001 Y LA LEY DE PROTECCIÓN DE DATOS Nº8968 PARA LA COOPERATIVA DE PRODUCTORES DE LECHE DOS PINOS, EN ALAJUELA

JOHAN VEGA CÓRDOBA

FERNANDO RÍOS VARGAS
TUTOR

SEDE CENTRAL
ENERO, 2025

DEDICATORIA

El proyecto de graduación quiero dedicárselo en primer lugar a Dios, por darme la fortaleza y sabiduría para llevar a cabo todo este proceso. Cada jornada de esfuerzo y dedicación cobró sentido al saber que Él me acompañaba en este proceso desde el inicio.

En segunda instancia, a mi madre Mayra Córdoba Alpízar, una mujer imparable, guerrera y luchadora, que con su ejemplo me enseñó que nunca es tarde para estudiar y lograr metas profesionales. Esas ganas de salir adelante fue lo que nos marcó de forma muy positiva a mí y a mis hermanos y, este trabajo es una muestra de ese legado.

Finalmente, esta dedicatoria es para Johan Vega Córdoba, por haber transformado sus dudas en certezas, sus miedos en valentía y sus limitaciones en motivación. Este logro reafirma que sí es posible. Que el esfuerzo, la constancia y la fe en uno mismo son capaces de romper cualquier barrera mental. Que cada persona, sin excepción, puede alcanzar sus metas si decide creer en sí misma. Que este proyecto sea un recordatorio permanente de que somos capaces, somos suficientes y merecemos llegar hasta donde soñamos.

AGRADECIMIENTOS

Agradezco en primer lugar a Dios, por brindarme todas las herramientas, la fortaleza y la sabiduría necesarias para culminar este proyecto. Su guía ha sido fundamental en cada paso del camino.

A mi familia, en especial a mi madre y hermanos, por su apoyo incondicional, palabras de aliento y compañía constante. Gracias por impulsarme a seguir adelante incluso en los momentos más difíciles.

A mi gran amiga María José Herrera Ruíz, por su respaldo sincero, sus consejos oportunos y su disposición para acompañarme emocional y académicamente en este proceso.

A Jorge Eduardo Soto Mora, compañero y colega de la Cooperativa de Productores de Leche Dos Pinos, por ser pieza clave en la formulación de esta propuesta. Su orientación aportó claridad en este trabajo.

A la Máster Olda Bustillos Ortega, directora de carrera, por su compromiso con la excelencia académica y por su dedicación en fortalecer la calidad de las carreras de Informática en la Universidad. Su acompañamiento fue valioso desde un inicio.

A mi tutor de tesis, Fernando Ríos, por su guía, paciencia y acompañamiento constante durante estas semanas intensas de trabajo. Su apoyo fue detonante para lograr una propuesta clara y bien fundamentada, entregada en tiempo y forma.

Y, finalmente, a la Universidad Internacional de las Américas, por brindarme una experiencia académica enriquecedora. Guardo los mejores recuerdos de esta etapa: las clases, los compañeros que se convirtieron en amigos, las asignaciones que me desafiaron y formaron. Hoy me despido de esta etapa con la certeza de que salgo preparado para contribuir a la sociedad con soluciones prácticas, éticas y eficaces.

CONTENIDO

TABLAS

FIGURAS

RESUMEN EJECUTIVO

Este proyecto tiene como finalidad proponer un procedimiento de revisión y control de seguridad para los desarrollos web creados para el departamento de mercadeo de la Cooperativa de Productores de Leche Dos Pinos, con base en la normativa internacional ISO 27001 y la Ley de Protección de Datos Nº8968 de Costa Rica. Esta iniciativa surge como respuesta a la creciente necesidad de asegurar la confidencialidad, integridad y disponibilidad de los datos personales recolectados mediante plataformas digitales, en un contexto donde las estrategias de marketing digital dependen cada vez más del uso de first-party data y desarrollos externos.

Actualmente, los desarrollos web del departamento son tercerizados con agencias externas, lo que representa un riesgo ante la ausencia de estándares formales de revisión de código, encriptación, validación de accesos y auditorías de seguridad. En este sentido, el proyecto propone una solución estructurada compuesta por cinco elementos clave: proceso de validación del código fuente, directrices para evaluaciones de seguridad, normativa de verificación, políticas de actualización de estándares, y un protocolo de aprobación final antes del lanzamiento de nuevos desarrollos.

La propuesta es viable técnica, operativa, legal y económicamente, ya que no requiere de nuevas herramientas ni inversiones significativas. Se enfoca en aprovechar los recursos existentes mediante la implementación de procedimientos documentados, checklists de seguridad y alineación con normativas vigentes. Se aplicó una metodología cualitativa y descriptiva que permitió levantar insumos desde entrevistas, observaciones y revisión documental.

Como resultado, se presenta un procedimiento aplicable y adaptable que refuerza la protección de los datos personales, mejora la supervisión de las agencias externas y fortalece la reputación de la Cooperativa como una organización responsable y comprometida con la ciberseguridad. Esta propuesta no solo contribuye a la mitigación de riesgos legales y técnicos, sino que promueve una cultura digital ética, eficiente y alineada con los estándares internacionales.

CAPÍTULO I: INTRODUCCIÓN

Planteamiento del Problema

Dos Pinos es una cooperativa costarricense reconocida como líder en la industria láctea de Centroamérica y el Caribe. Con más de 76 años en el mercado, la empresa posee una gama superior a los 900 productos de consumo humano y una línea diversificada de agropecuarios, otorgándole el lugar de una de las marcas más queridas y confiables de la región. Actualmente, Dos Pinos mantiene una presencia considerable en países como Estados Unidos, República Dominicana y todos los países centroamericanos. Genera empleo para más de 5,000 personas y exporta a más de 10 mercados internacionales, bajo su lema “Siempre con Algo Mejor”.

Contexto

La pandemia mundial ha alterado drásticamente la forma en que las personas se comunican, interactúan, consumen productos y servicios, a cambio, aceleraron la transición hacia lo digital. Para Dos Pinos, la nueva realidad era: un consumidor cada vez más conectado. A raíz de ello, el Departamento de Mercadeo de Dos Pinos ha buscado y busca desarrollar estrategias digitales que le permitan la continua exposición de sus productos en un mercado altamente competitivo, donde la segmentación personalizada se vuele vital para sobresalir con propuestas cada vez más disruptivas que logren captar la atención del consumidor final.

Uno de los elementos clave en esta estrategia es la first-party data, definida como los datos que una organización recopila directamente de sus consumidores mediante sus propios canales digitales, como sitios web o aplicaciones móviles (Smith, 2020). Estos datos son esenciales para la toma de la decisión porque permiten a la empresa entender verdaderamente el comportamiento del consumidor, entender qué es lo que le gusta, con cuáles son aquellos productos más llamativos, y, por último, medir si la campaña de comunicación fue eficiente según el objetivo planteado inicialmente. Por lo que esta recolección de información se hace aún más valiosa y relevante para la evaluación final.

Es por esa razón que estas plataformas son esenciales para recopilar información que guie las estrategias digitales de la cooperativa para los siguientes años.

Problemas Identificados

Por lo tanto, en un marco como el indicado anteriormente, los problemas relacionados con la seguridad y la calidad de los desarrollos web hechos por agencias externas son los siguientes:

- Deficiencia en el control de calidad de los desarrollos web realizados por terceros, poniendo en riesgo la experiencia del usuario y la fiabilidad de las plataformas digitales de Dos Pinos.
- No existe un estándar formal para la revisión de seguridad, que incluya validación de código fuente, encriptación de datos y controles de acceso en los desarrollos web.
- Tampoco existen sensibilidades que señal el uso de pruebas de seguridad en los desarrollos entregados por las agencias externas, aumentando aún más el riesgo de las vulnerabilidades y la posibilidad de incumplimientos reglamentarios, que hagan más fácil un ataque.
- Por último, tampoco hay protocolos de aprobación final que garanticen que los sitios web u otros desarrollos web cumplan con los estándares establecidos antes de ser lanzados públicamente.

Objetivos

Objetivo general

Proponer un proceso de revisión y control de seguridad de los desarrollos web del Departamento de Mercadeo de la Cooperativa de Productores de Leche Dos Pinos, que impacte la confidencialidad, integridad, y disponibilidad de los datos personales procesados por estos medios en conformidad con lo que establece la normativa internacional ISO 27001, y la Ley Nº8968.

Objetivos específicos

Elaborar un proceso estándar para la validación del código fuente, el control de accesos y el cifrado de datos, asegurando la protección de los desarrollos web.

Desarrollar directrices para las evaluaciones de seguridad, estableciendo pruebas y criterios específicos que sea obligatorios para las agencias externas en la detección y mitigación de vulnerabilidades.

Formular una normativa que incluya una lista de verificación de seguridad obligatoria, estandarizando el proceso de comprobación de los desarrollos webs.

Crear políticas para la actualización periódica de los estándares de seguridad, integrando los cambios normativos y mejores prácticas de la industria.

Crear un protocolo de aprobación final que establezca los procedimientos para la verificación de los controles de seguridad y la validación de los desarrollos web antes de su lanzamiento.

Justificación

La realización de un proceso de revisión y control de seguridad para los desarrollos web del Departamento de Mercadeo, basado en la normativa ISO 27001 y la Ley de Protección de Datos Nº8968, tiene como objetivo fortalecer y mejorar el uso adecuado de las plataformas digitales, reduciendo todos los riesgos asociados con las vulnerabilidades que puedan suceder ante potenciales amenazas cibernéticas

El contexto de gestión y uso de datos requerido para las estrategias del área de mercadeo hace de la seguridad de estas plataformas un factor determinante para la competitividad de la Cooperativa y la buena imagen en los mercados donde actualmente ejecuta sus actividades.

La Ley Nº8968 exige a las empresas para implementar medidas para proteger los datos personales, mientras que la ISO 27001 se asegura de que los controles de seguridad garantizan la confidencialidad, integridad y disponibilidad de la información. Por lo tanto, este proyecto permitirá a la Cooperativa Dos Pinos a cumplir con dichos estándares.

Adicionalmente, la implementación de estándares y directrices de seguridad permitirá optimizar la revisión de desarrollos web, asegurando una reducción oportuna de tiempo y esfuerzo. La decisión de asegurar la calidad y la eliminación de vulnerabilidades de los desarrollos digitales refuerza la imagen de Dos Pinos como una empresa 100% confiable, alineada con las mejores prácticas internacionales. Se protege no solo a la cooperativa de costos legales, sino también a todos los usuarios que interactúan con estas plataformas, promoviendo un ecosistema digital mucho más ético y seguro.

Al final, la realización se centrará en la creación de las normativas para que el proyecto se lleve a cabo sin altos costos ni el desarrollo de tecnologías fuertemente técnicas y complicadas.

Viabilidad técnica

La propuesta es técnicamente viable debido a que su enfoque se basa en la creación de estándares, directrices y políticas que no requieren la creación de desarrollos tecnológicos complejos ni la adquisición de infraestructura adicional a la que cuenta la organización. Los principales factores que garantizan esta viabilidad son:

- **Marco Normativo Existente**: La propuesta se fundamenta en la norma ISO 27001, la cual proporciona lineamientos claros y detallados para la gestión de la seguridad de la información y la protección de datos personales. Estos estándares tienen un costo asociado, y su adquisición será gestionada a través del Instituto de Normas Técnicas de Costa Rica (INTECO)**,** mediante su página web, lo que facilita su compra de forma directa. A continuación, se detalla el desglose del costo:

Tabla 1
Costo de normativa ISO 27001 en Costa Rica

Normativa	Nombre	Precio con IVA ₡
INTE/ISO/IEC 27001:2023	Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.	₡31584.63

Fuente: *Vega, 2025.*

- **Recursos Disponibles**: El Departamento de Mercadeo de Dos Pinos cuenta con agencias que desarrollan sus plataformas web. La propuesta establecerá normativas para que estas agencias adopten procedimientos de seguridad claros y aplicables con los recursos tecnológicos y conocimientos con los que ya cuentan.
- **Herramientas y Técnicas**: El proyecto contempla el uso de herramientas prácticas, como checklist, procedimientos de validación de código fuente, y controles de encriptación. Estas herramientas están disponibles y no requieren de más desarrollos específicos.
- **Estructura Organizacional de Apoyo**: La cooperativa dispone de un sistema organizacional consolidado y personal capacitado en el área de mercadeo, lo que hace que

aún más práctica la implementación de los procedimientos y la supervisión de dichos estándares.

- **Enfoque Controlado**: La propuesta no incluye la creación o programación de nuevas aplicaciones, sino la estandarización de procesos y normas. Por lo tanto, garantiza que el proyecto sea ejecutable dentro del tiempo y recursos asignados, sin implicar dependencias técnicas adicionales.

De esta manera, todos estos elementos confirman la factibilidad técnica de la propuesta, con énfasis en la posibilidad de introducir normas de seguridad y legislación internacional en la operación del Departamento de Mercadeo. En este sentido, esto se traduce en que estas mismas operaciones diarias no se verán interrumpidas a corto plazo mientras se garantiza una protección de datos y calidad en el desarrollo de la web.

Viabilidad operativa

Según Asana (2023), la viabilidad operativa evalúa si una organización posee la capacidad para completar un proyecto, considerando la disponibilidad de personal adecuado, estructura organizativa y cumplimiento de requisitos legales. Así, el objetivo de esta propuesta es averiguar si la Cooperativa tiene las condiciones adecuadas para hacer cumplir las normas de seguridad en los desarrollos web realizados dentro del Departamento de Marketing.

Una vez analizada la estructura organizativa de la cooperativa y el funcionamiento del departamento involucrado, se puede decir que el proyecto cuenta con los requisitos operativos necesarios. Dos Pinos tiene una estructura bien establecida y una fuerza laboral capacitada para implementar las regulaciones planteadas. El Departamento de Marketing, una unidad con 16 colaboradores, es muy capaz en la gestión y supervisión de agencias externas para la creación de campañas digitales, por lo que están más abiertos a nuevas estrategias en materia de seguridad y calidad.

Además, la cooperativa ya dispone de procesos establecidos para la gestión de sus plataformas digitales, lo que permite la integración de los estándares definidos en la ISO 27001 y la Ley Nº8968 sin mayores inconvenientes.

Para garantizar el cumplimiento, se implementará un plan de concientización para que se obtenga una adecuada implementación.

Viabilidad económica

Debido a que esta propuesta data de una investigación, no implica mayores costos por los que no se tienen que incurrir en otros gastos como contratación de programadores, especialistas o ejecución de un programa como tal, esto hace que no se incurra en costos mayores.

La Cooperativa en este caso no tendrá que tampoco que asumir ningún costo extra para desarrollo de la propuesta de investigación, ya que se realizó un previo acuerdo entre la empresa y el estudiante, por tratarse de un proyecto de graduación.

Viabilidad legal

Para la propuesta se tomarán en cuenta las leyes y regulaciones vigentes en Costa Rica en materia de seguridad informática y protección de datos. Por lo que se procederá a mencionar cada una de ellas:

- ISO 27001: Norma internacional que establece los lineamientos para la gestión de la seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los datos.
- Ley 8968 sobre la Protección de la Persona Frente al Tratamiento de sus Datos Personales: se encarga de proteger los datos personales, bases de datos, datos de acceso restringido, sensibles y en el manejo de estos.
- Ley 8148 Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N°4573 para reprimir y sancionar los delitos informáticos de la Asamblea Legislativa de la República de Costa Rica del año 2001.
- Ley de Derechos de Autor 6683 por parte de la Asamblea Legislativa de la República de Costa Rica del año 1982

Por lo que el acatamiento de cada uno de estos lineamientos, concluimos que el proyecto es completamente viable en todos sus aspectos.

Proyecciones

Se espera que la implementación de esta propuesta genere un impacto positivo y permita que la Cooperativa Dos Pinos pueda ejecutar buenas prácticas en materia de la gestión en la seguridad en los desarrollos web. Que conforme se vayan adoptando las normativas y directrices

establecidas, la organización pueda fortalecer sus procesos digitales y optimizar la protección de los datos personales de los usuarios.

Además, se desea que esta propuesta sea tomada en cuenta no solo en Costa Rica, sino a toda la región, ya que actualmente hay una gran desconexión del equipo que trabaja en el exterior con todos los procesos que se ejecutan en casa matriz, y aún más con el departamento de tecnologías de la información.

A continuación, se detalla de cómo se desea implementar esta propuesta por plazos:

Corto Plazo (0-5 meses):

- Creación de un marco normativo interno basado en la ISO 27001 y la Ley Nº8968.
- Difusión de las nuevas políticas entre el personal del Departamento de Mercadeo y las agencias externas.
- Implementación de listas de verificación y protocolos de seguridad para validar los desarrollos web.
- Identificación de brechas en los procesos actuales y establecimiento de planes de mejora.

Mediano Plazo (5-8 meses):

- Integración de las operaciones de exterior: Cono Norte y República Dominicana.
- Aplicación efectiva de los estándares en los nuevos desarrollos web y seguimiento de su cumplimiento.
- Disminución de riesgos de vulnerabilidades en los sitios web de la cooperativa.
- Capacitación continua para el personal interno y colaboradores externos.

Largo Plazo (8 meses -1 año):

- Consolidación de una cultura organizacional enfocada en la seguridad de la información.
- Optimización de los procesos de revisión y control de seguridad, reduciendo tiempos y costos operativos.
- Posicionamiento de Dos Pinos como un referente en la implementación de normativas de seguridad digital en su sector.

En conjunto, esta proyección muestra que la implementación de la propuesta no solo es factible, sino también estratégica, ya que permitirá a la cooperativa adaptarse poco a poco a los nuevos procesos que buscan fortalecer la seguridad de sus plataformas.

Alcance funcional

Dentro de la Ingeniería en Informática, el alcance funcional en una propuesta de investigación define las funciones, características y limitaciones de la solución propuesta. Además, establece los requisitos que servirán como guía para su implementación.

En este sentido, la presente propuesta no conlleva el desarrollo de un sistema o software en particular, sino la formalización de un procedimiento estandarizado para la revisión y control de seguridad en los desarrollos web hechos a través de agencias para el Departamento de Mercadeo de Dos Pinos, dicha implementación velará para que cada uno de los desarrollos se encuentre conforme a los lineamientos de la ISO 27001 y de la Ley Nº8968, fortaleciendo de esta manera la protección de los datos personales y la integridad de las plataformas digitales de la cooperativa.

Tabla 2
Alcance funcional.

Nombre del apartado	Descripción del apartado
Proceso de validación de la calidad y seguridad de los desarrollos web administrados por agencias externas en campañas de mercadeo.	Este apartado tratará de la elaboración un proceso estándar para validar el código fuente, los controles de acceso y la encriptación de datos, garantizando la seguridad de los desarrollos web.
Directrices de seguridad y pruebas.	Este apartado tiene el propósito de desarrollar directrices para las evaluaciones de seguridad, estableciendo pruebas y criterios específicos que las agencias externas deben cumplir para detectar y mitigar vulnerabilidades.
Normativa de análisis y verificación de seguridad	Este apartado tiene la finalidad de formular una normativa que incluya una lista de verificación de seguridad obligatoria, estandarizando el proceso de comprobación de los desarrollos webs.

Políticas para el cumplimiento de la ley Nº8968 y la ISO 27001	Se crearán políticas para la actualización periódica de los estándares de seguridad, integrando los cambios normativos y mejores prácticas de la industria.
Protocolos de aprobación y validación final	Este apartado busca crear un protocolo de aprobación final que establezca los procedimientos para verificar los controles de seguridad y validar los desarrollos web antes de su lanzamiento.
Normativa de seguridad y calidad en el tratamiento de datos personales	En este apartado se desarrollará una normativa que contemple estándares sobre control de acceso, cifrado, validación de calidad y monitoreo de incidentes de seguridad, garantizando la protección de los datos personales procesados por los desarrollos web.
Normativa de análisis dinámico de seguridad para desarrollos web	Se establecerán lineamientos para realizar pruebas dinámicas de seguridad, documentar resultados, registrar riesgos y actualizar los criterios de evaluación frente a amenazas emergentes.
Normativa para el cumplimiento de la Ley Nº8968 y gestión de consentimiento de usuarios	En este apartado se creará un procedimiento para la obtención del consentimiento informado, gestión de cookies y atención de derechos de los usuarios sobre sus datos personales.
Normativa de gestión de incidentes de seguridad y monitoreo de actividades	Se desarrollará un proceso para la detección, respuesta y documentación de incidentes de seguridad, asegurando trazabilidad y mejora continua en la protección de los desarrollos.

Fuente: *Vega, 2025.*

Alcance metodológico

Dada la propuesta formulada, el presente estudio se clasificará como aplicado y descriptivo; lo anterior se debe, principalmente, a que su propósito es otorgar las herramientas para la formulación de un procedimiento estándar de revisión y control para asegurar los nuevos desarrollos web.

La propuesta, desde la metodología, también se inclina a un enfoque cualitativo, dado que las directrices y disposiciones planteadas están enfocadas a asegurar la seguridad de los desarrollos sin necesidad de ser garantizadas por algún sistema informático. A través de un análisis de normativas que involucren la ISO 27001 y la Ley Nº8968, se propondrán disposiciones específicas para garantizar la integridad, confidencialidad y disponibilidad de la información.

Por otro lado, considera, también, una propuesta de diseño documental, ya que estará basada en la interpretación y transcripción de lo encontrado en las normativas y recomendaciones de seguridad antes mencionadas, además de recurrir a fuentes secundarias, como artículos y normativa internacional, para sustentar la formulación de las disposiciones propuestas.

La propuesta delimita el ámbito temporal y organizacional a los procedimientos de Dos Pinos en el Departamento de Mercadeo y en la interacción con la agencia para el desarrollo de plataformas web durante el último año. De esta forma, la propuesta se ajusta a los procesos organizativos actuales y futuros, manifestando fortaleza en la propuesta.

Alcance tecnológico

Esta propuesta propone normativas, lineamientos y procedimientos en un modelo de revisión y control de seguridad para los desarrolladores web externos al área de TI del Departamento de Mercadeo de Dos Pinos. Aunque este proyecto no implica la creación y producción de software, incluye la utilización de herramientas en tecnología que permiten el soporte de la aplicación de las normas propuestas.

Las tecnologías que hacen factible que el procedimiento propuesto se pueda llevar a cabo son:

- ISO 27001: Esta norma desarrolla los controles y mejores prácticas en la gestión de seguridad de la información en entornos digitales.
- Protocolos de encriptación: Son aquellos mecanismos de seguridad creados para proteger la información que se transmite y es almacenada en las plataformas web.
- Sistemas de gestión de accesos (IAM- Identity and Access Management): Este modelo de herramientas permite gestionar y limitar permisos de cada usuario web.
- Checklists de validación de seguridad: Son listas estructuradas con criterios con criterios técnicos para asegurar que los desarrollos cumplen con la seguridad antes de producción.

El alcance de esta propuesta se limitará a la definición y aplicación de los estándares antes descritos dentro del proceso de desarrollo web, sin incluir modificaciones en la infraestructura tecnológica de la Cooperativa ni la compra de nuevas herramientas digitales. Se usará exclusivamente los recursos tecnológicos ya que existentes dentro de la empresa y en las agencias externas encargadas de los desarrollos.

CAPÍTULO II: MARCO REFERENCIAL

Este capítulo tiene como finalidad de explicar de forma oportuna todos aquellos conceptos que tiene relación con la investigación. De esta forma, el lector podrá entender más a profundidad todos los temas que tienen relación con la propuesta de un proceso para identificar las vulnerabilidades de los desarrollos web, como el detectarlos y contrarrestarlos se convierte en parte fundamental para un manejo adecuado de la información, y de los datos que los usuarios proporcionan en las plataformas digitales hoy en día.

Ahora veamos, ¿qué beneficio tiene el identificar todas estas vulnerabilidades en un desarrollo?, ¿cuál es el beneficio tangible?; Primero, es importante el mencionar que, para las empresas, las plataformas digitales se han convertido en herramientas clave para sus estrategias de negocio. Estas plataformas facilitan la comunicación con los consumidores permitiendo que las compañías puedan fortalecer cada vez más su presencia de marca. Sin embargo, el creciente uso de estas plataformas ha traído también muchos desafíos en términos de seguridad, dado que la información que se manipula es de carácter sensible y debe ser protegida con los más altos estándares para evitar las filtraciones y salvaguardar siempre la integridad de cada usuario. Por ello, el beneficio más importante se transforma en asegurar que esos desarrollos estén protegidos ante cualquier amenaza cibernética y guardar la imagen tanto de la empresa, como de sus usuarios.

La Relevancia de la Seguridad en los Desarrollos Web para Dos Pinos

Dos Pinos fue fundada hace más de 76 años, ha demostrado ser una empresa que constantemente busca la innovación y la mejora en su portafolio de productos. Ahora bien, lograr posicionarse como una de las marcas más queridas de la región ha sido producto de su capacidad de adaptación y estrategias de mercadeo, que buscan generar siempre la conexión más efectiva con el consumidor.

Por otra parte, el departamento de mercadeo cumple un rol crucial en la comunicación de la cooperativa, ya que es su responsabilidad es asegurarse de que los mensajes, campañas y plataformas utilizadas, sean lo más eficaces posible. Cada año, se presenta el desafío de identificar cuáles son las mejores prácticas y plataformas digitales para innovar en la comunicación. En este proceso de búsqueda e innovación, los desarrollos web toman una participación relevante, ya que este activo tecnológico permite recolectar datos que pueden ser usados de forma estratégica.

Dicho lo anterior, toda esta información le permite al departamento personalizar las campañas de marketing con más precisión y de esa forma entregar un mensaje mucho más personalizado. Sin embargo, el obtener este tipo de datos también representa una responsabilidad significativa en términos de seguridad, de acuerdo con (Ryan, 2021) “Las empresas deben adoptar estrategias de ciberseguridad en sus plataformas digitales para evitar el robo de datos y asegurar la continuidad de sus operaciones en un entorno cada vez más digitalizado” (p.134), pues cualquier ataque en los desarrollos web puede exponer información sensible y comprometer la imagen de la compañía.

Fortalecimiento de la Infraestructura Digital de Dos Pinos

Si bien es cierto, Dos Pinos a lo largo de su trayectoria ha construido toda una infraestructura de TI robusta, pero, aún existen grandes oportunidades para seguir protegiendo y organizando todos los procesos tecnológicos dentro de la compañía. La ausencia de un proceso formal de revisión y control de seguridad en los desarrollos webs que hoy crean las agencias externas, representa una gran área de oportunidad.

El no contar con un estándar predefinido en términos de validación de código fuente, encriptación de los datos, controles de acceso y políticas de seguridad de la información, entre otras, incrementan el riesgo de vulnerabilidades y muy posibles incumplimientos normativos.

Por ende, en esta propuesta pretende reforzar estas falencias mediante procesos y normativas que garanticen que todos los desarrollos utilizados por el departamento de Mercadeo cumplan con los más altos estándares de seguridad. De esta manera, no solo se mitigarán todos los riesgos relacionados con la privacidad y protección de los datos, sino que además fortalecerá la imagen de la cooperativa como una empresa que se preocupa por la integridad de sus usuarios, respetando las normas internacionales, incluyendo la Ley Nº8968 sobre la protección de datos personales en Costa Rica.

Con este contexto, el marco referencial aborda en primer lugar la Gestión de Mercadeo de una Marca, explicando la evolución del marketing digital, el papel de las plataformas digitales en la estrategia comercial y la relevancia de la **first-party data** como un activo fundamental para la personalización de dichas estrategias. Posteriormente, se abordan aspectos técnicos de la

informática y los desarrollos web, para luego terminar el último tópico de la gestión, enfocado en la seguridad de la información y las normativas asociadas a esta investigación.

Gestión de Mercadeo de una Marca

Un dato importante para dar inicio en este punto lo resalta (Chaffey & Ellis-Chadwick, 2022): "Las estrategias de marketing digital permiten a las empresas no solo llegar a su público objetivo de manera más eficiente, sino también optimizar recursos y maximizar el retorno de inversión." (p.45). El éxito de una marca hoy en día depende de su gran capacidad para construir y gestionar estrategias de mercadeo que le permitan mantenerse relevante en la mente del consumidor.

Esta gestión no solo se enfoca en la promoción y posicionamiento de un producto o servicio, sino de entender el comportamiento del consumidor, el cómo desarrollar relaciones de valor con el público meta y cómo se optimiza los canales de comunicación para generar un alto impacto y fidelización.

A lo largo de los años, el mercadeo ha cambiado en respuesta a los cambios en la sociedad, el desarrollo tecnológico y la evolución en los hábitos de consumo. Según Kerin y Hartley (2023), “el proceso de marketing estratégico implica la asignación de recursos de la mezcla de marketing de la organización para alcanzar sus mercados meta y lograr una ventaja competitiva” (p. 42).

Este principio se ha convertido en una base para la mayoría de las empresas, ya que ayudan a cambiar sus modelos tradicionales basados en medios más impresos y televisivos a estrategias más dinámicas y personalizadas que se ajustan a la era digital.

A medida que las marcas adoptan estas nuevas tecnologías y plataformas para fortalecer su presencia en el mercado, es necesario entender cómo ha evolucionado el marketing digital y qué factores han impulsado esta transformación.

Marketing Digital y su Evolución

El marketing ha evolucionado de manera significativa a lo largo de los años, adaptándose a las nuevas tecnologías y hábitos de consumo de la población. El marketing digital, en particular,

ha transformado la manera en que las empresas se comunican con sus clientes y desarrollan estrategias de mercadeo. Según Sachdev (2024), “las tecnologías existentes, emergentes y futuristas afectan al marketing digital de muchas maneras. En particular, el marketing para dispositivos inteligentes da como resultado un marketing en un entorno inteligente, que está cambiando la forma en que se efectúa esta actividad” (p. 5). Esto ha servido de base para la evolución del marketing en la era digital, donde la interacción con los consumidores se ha vuelto más dinámica y medible en tiempo real.

Desde su surgimiento en la década de 1990, el marketing digital ha pasado por diferentes etapas. En sus inicios, el enfoque estaba centrado en la creación de sitios web y el uso del correo electrónico como herramienta de comunicación. Posteriormente, con el auge de los motores de búsqueda a principios de los años 2000, surgieron estrategias como **SEO (Search Engine Optimization) y SEM (Search Engine Marketing),** que permitieron a las empresas posicionarse en los resultados de búsqueda y atraer más tráfico relevante en sus plataformas digitales. En la década del 2010, las redes sociales transformaron la manera en que las marcas interactúan con sus consumidores, incentivando la creación de contenido atractivo. Como señala Sachdev (2024), “las marcas querrán aumentar el compromiso con los consumidores y clientes, y las redes sociales pueden ser una excelente manera de hacerlo” (p. 225).

A medida de toda esta evolución, las empresas poco a poco han incorporado tecnologías avanzadas para mejorar la eficiencia de sus estrategias. En la última década, el uso del **big data** y la inteligencia artificial ha permitido una personalización más profunda de los mensajes publicitarios.

El marketing digital se diferencia del marketing tradicional en varios aspectos clave, principalmente en la forma en que las marcas interactúan con los consumidores y en la capacidad de medición de los resultados.

Tabla 3
Diferencia entre marketing tradicional y digital

Característica	Marketing tradicional	Marketing Digital
Medios utilizados	TV, radio, prensa	RRSS, emails, blogs, Web
Segmentación	Amplia, sin personalización	Precisa, por intereses y datos
Interacción	Unidireccional	Bidireccional
Medición	Se requiere de estudios	En tiempo real, con KPIS

Fuente: *Vega, 2025.*

La adopción del marketing digital ha obligado a las empresas replantear sus estrategias comerciales, y esto lo explican claramente Fischer de la Vega y Espejo Callado (2024), quienes señalan que "hoy los usuarios pueden conectarse y mostrar en tiempo real lo que están haciendo mientras compran, se alimentan, caminan, viajan en vehículos, asisten a eventos o diversiones, etcétera" (p. 224).

Toda esta transformación digital ha venido a darle un giro completo a la comunicación, donde cada día las estrategias deben ser más dinámicas, personalizadas y centradas en la experiencia del usuario. Núñez Cudriz y Miranda Corrales (2020) enfatizan que: "la evolución del marketing digital ha llevado a que las empresas adopten modelos de negocio más ágiles, donde la recolección y análisis de datos juegan un papel fundamental en la toma de decisiones estratégicas" (p. 10). En este sentido, las empresas han tenido que reinventarse para mantenerse vigentes en un entorno digital que está en constante cambio.

Qué es el First Party Data y sus Fuentes

Tras comprender la importancia de la recolección de datos y su impacto en la estrategia de marca, es fundamental analizar el concepto de **First Party Data** y sus fuentes de origen. Este término hace referencia a la información que una empresa obtiene directamente de sus clientes a través de sus propias plataformas digitales, como sitios web, aplicaciones móviles, sistemas de gestión de relación con el cliente **(CRM)** y redes sociales. Al provenir de interacciones directas con los usuarios, estos datos permiten a las empresas conocer mejor a su público y diseñar estrategias de marketing más personalizadas y efectivas, esto lo refuerza Lotame (2022) donde

explica que: “Las marcas que utilizan First-Party Data desde canales propios pueden optimizar sus estrategias de fidelización y mejorar la experiencia del cliente mediante información más precisa y confiable” (p.54) para que el mensaje sea más preciso y atractivo.

Cómo se Utiliza la First Party Data en Mercadeo

El First party data es fundamental para las empresas, ya que proviene directamente de las interacciones del usuario con la marca, facilitando que las estrategias sean más efectivas y personalizadas (Juanjo Artero, 2023).

- Segmentación precisa: Permite segmentar las campañas basadas en la información que los mismos clientes proporcionan a la organización. Para crear anuncios y comunicación más personalizada según sus gustos y necesidades.
- Experiencia memorable: Al conocer las preferencias y comportamiento de sus clientes, las empresas pueden ofrecer experiencias únicas, con contenidos más relevantes, fortaleciendo aún más la satisfacción y fidelidad del cliente.
- **Retargeting** efectivo: Utilizando los datos propios, se pueden desarrollar campañas altamente personalizadas para todas esas personas que han interactuado previamente con la marca.

Por consecuente, al implementar estas prácticas, las empresas podrán mejorar la efectividad de sus estrategias, y como resultado obtener una mayor lealtad del cliente y optimar a su vez la toma de decisiones basados en datos reales, precisos y relevantes. Sin embargo, para que todas estas estrategias sean efectivas es fundamental comprender los principios tecnológicos que las sustentan. La informática y el desarrollo web constituyen la base sobre la cual se construyen las plataformas digitales utilizadas en mercadeo, desde sitios web hasta sistemas avanzados de gestión de datos.

En este sentido, el conocimiento de los fundamentos de la informática y el desarrollo web es clave para entender cómo se procesan, almacenan y protegen los datos en las estrategias digitales, tal como lo menciona Shelly & Vermaat (2021): “El dominio de la informática no solo mejora la eficiencia en la gestión de la información, sino que también es clave para la toma de decisiones estratégicas en un mundo digitalizado” (p.27). Además, este conocimiento facilita el aprovechamiento de herramientas tecnológicas y una mejor comprensión de los sistemas digitales que respaldan las estrategias empresariales.

Fundamentos de la Informática y Desarrollos Web

El crecimiento acelerado de la tecnología ha generado una dependencia cada vez mayor en los sistemas informáticos y el desarrollo web. En la actualidad, la informática no solo sustenta la operatividad de las empresas, sino que también se ha convertido en un elemento fundamental para garantizar la seguridad de la información y la optimización de procesos. Según Tanenbaum y Bos (2021): "todo sistema informático se compone de una interacción entre hardware, software y redes, donde cada uno desempeña un papel esencial en el procesamiento y la comunicación de datos dentro de una infraestructura digital" (p. 45). La interconexión entre hardware, software, redes y aplicaciones web ha transformado la manera en que las organizaciones gestionan su información y protegen sus activos digitales.

Conceptos Básicos de la Informática

La informática ha evolucionado de ser una disciplina centrada en cálculos y almacenamiento de datos a convertirse en el pilar de la gestión empresarial y digital. Según Tanenbaum y Wetherall (2021), "la informática moderna no solo se centra en el procesamiento de datos, sino en la eficiencia, seguridad y adaptabilidad de los sistemas computacionales" (p. 27). Esta evolución ha llevado a una mayor integración en los sistemas digitales, permitiendo que ahora sean más rápidos, eficientes y seguros.

Las redes han sido un componente crucial en esta transformación digital, permitiendo tener un mundo mucho más conectado y a su vez facilitando la comunicación en tiempo real. La confiabilidad de estos sistemas depende en gran medida de protocolos de seguridad que regulen el acceso y la transferencia de información entre dispositivos y usuarios validados.

El correcto funcionamiento de las soluciones digitales y plataformas en línea depende de estos tres elementos. La combinación de hardware potente, software optimizado y redes eficientes, permiten el desarrollo de plataformas robustas y seguras para la gestión de datos y la interacción con los usuarios. Como menciona Stallings (2022): "el rendimiento de un sistema informático está determinado por la sinergia entre su hardware, software y la infraestructura de red, ya que estos elementos deben estar diseñados para trabajar en conjunto y garantizar estabilidad y seguridad en la operación de las plataformas digitales" (p. 78). Esta integración asegura que los sistemas sean escalables, eficientes y adaptables a las necesidades del ecosistema digital actual.

La Importancia del Código Fuente en el Desarrollo de Aplicaciones

El código fuente es el elemento fundamental en la construcción de software, ya que define la lógica y el comportamiento de un sistema como tal. Estas instrucciones indican a la computadora los pasos a seguir para ejecutar tareas específicas. Ullman (2020) afirma que "el código fuente es la base sobre la cual se construyen las aplicaciones digitales, definiendo su estructura, funcionalidad y seguridad" (p. 88). Aunque el código fuente es comprensible para los programadores, las máquinas requieren que este sea traducido a lenguaje máquina mediante procesos de compilación o interpretación para su ejecución óptima.

Además de los programas de software tradicionales, el término "código fuente" también se aplica a otros tipos de documentos, como archivos HTML, CSS o XML, que, aunque no son lenguajes de programación en sentido estricto, definen la estructura y presentación de contenido en la web. Según Tanenbaum y Bos (2021):

> “El código fuente no se limita únicamente a lenguajes de programación como Java o Python. También abarca lenguajes de marcado como HTML y XML, los cuales definen la manera en que la información es presentada y estructurada en un entorno digital. Sin una adecuada gestión del código fuente, la funcionalidad y la estética de los sistemas web pueden verse afectadas” (p. 89).

Esto resalta la importancia de considerar la protección y optimización del código en diferentes ámbitos digitales para asegurar la protección del desarrollo en todos sus aspectos. La gestión y protección del código fuente son esenciales, ya que representa la propiedad intelectual de los desarrolladores y de las empresas.

El acceso no autorizado o la modificación indebida del código pueden comprometer la seguridad y funcionalidad de las aplicaciones. De acuerdo con Pressman y Maxim (2021): "la seguridad del código fuente es un factor crítico en el desarrollo de software, pues cualquier vulnerabilidad en su estructura puede convertirse en un punto de entrada para ataques cibernéticos" (p. 241). Esto evidencia la necesidad de implementar estrategias de resguardo y buenas prácticas en la gestión del código, asegurando su integridad y confiabilidad dentro de los sistemas informáticos. Todas estas estrategias juntas contribuyen a reducir riesgos de seguridad y mejorar la confiabilidad de los sistemas digitales.

Controles de Acceso y Protección de la Información

Los controles de acceso son mecanismos de seguridad diseñados para regular quién o qué puede visualizar o utilizar recursos en un entorno informático. En el contexto empresarial, garantizar que solo los usuarios autorizados accedan a información confidencial es crucial para la protección de datos. Según Sandhu y Samarati (2020), "los modelos de control de acceso juegan un papel fundamental en la seguridad de los sistemas, minimizando riesgos de intrusión y manipulación no autorizada" (p. 45). Su objetivo principal es garantizar la integridad y confidencialidad de la información. Estos controles se implementan a través de varios componentes clave:

- **Autenticación**: Proceso de verificar la identidad de un usuario o sistema, generalmente mediante credenciales como contraseñas, tokens o datos biométricos.
- **Autorización**: Determinación de los permisos o niveles de acceso que un usuario autenticado tiene dentro del sistema.
- **Auditoría**: Registro y análisis de las actividades de acceso para detectar y responder a posibles incidentes de seguridad.

Además, existen diferentes modelos de control de acceso, entre los cuales se destacan:

- **Control de Acceso Discrecional (DAC):** El propietario de los datos decide quién tiene acceso y qué tipo de privilegios se otorgan en el sistema.
- **Control de Acceso Obligatorio (MAC):** Las políticas de acceso son establecidas por una autoridad central, y los usuarios no pueden cambiar sus permisos.
- **Control de Acceso Basado en Roles (RBAC):** Los permisos se asignan según roles específicos dentro de una organización, facilitando la gestión de acceso en función de las responsabilidades laborales.

El modelo RBAC es ampliamente utilizado debido a su flexibilidad y capacidad de escalabilidad en entornos empresariales. Según Sandhu y Samarati (2020), este enfoque "ha demostrado ser uno de los más eficientes en la gestión de permisos dentro de grandes organizaciones, ya que reduce la complejidad administrativa y mejora la seguridad del sistema" (p. 155).

Además de su función en la seguridad informática, los controles de acceso contribuyen a mejorar la trazabilidad y la administración eficiente de los sistemas digitales. Como lo señalan Bishop y Snyder (2022), "los sistemas de control de acceso no solo protegen los datos, sino que también aseguran la trazabilidad y la detección oportuna de actividades maliciosas mediante auditorías constantes" (p. 67). Su correcta implementación en el marco de la gestión garantiza el cumplimiento de normativas de seguridad y refuerza la confianza en los sistemas digitales, facilitando la operatividad segura de las organizaciones.

Los Desarrollos Web y su impacto

El desarrollo web ha cambiado la forma en que se generan y administran las páginas digitales. A medida que ha evolucionado, ha brindado a las empresas y consumidores soluciones mucho más ágiles, interactivas y seguras, mejorando significativamente la experiencia. El desarrollo web ha pasado de páginas simples y estáticas a aplicaciones web interactivas que utilizan la mayoría de las tecnologías actuales. De acuerdo con Flanagan (2020) señala que: “En las últimas décadas, el desarrollo web ha experimentado cambios significativos, pasando de simples páginas estáticas hecha en HTML a aplicaciones interactivas y dinámicas con tecnologías como JavaScript, APIs, y bases de datos en la nube” (p. 88). A causa de estos cambios, el desarrollo web ahora incluye la programación no solo del lado del servidor y del cliente sino también la gestión de bases de datos y la ciberseguridad.

A lo largo de este proceso, es crucial que el balance entre funcionalidad, accesibilidad y usabilidad optimice la experiencia del usuario. Para crear páginas digitales efectivas, más allá de la programación, el diseño web es necesario. Como señala Fernández Casado (2024), “crear versiones de páginas web optimizadas para dispositivos móviles y asegurarse de que el sitio web cumple con un diseño receptivo o responsivo que haga que se adapte correctamente a diferentes tamaños de pantalla y dispositivos” (p. 157). Es decir, no es suficiente que un sitio funcione adecuadamente; lo vital es que sea intuitivo y eficiente para el usuario final.

En este contexto, Fernández Casado (2024) define el diseño de contenido web como “el proceso de planificación, creación y organización de todos los elementos visuales, auditivos y escritos que componen un sitio web, con el objetivo principal de crear una estructura visualmente

atractiva y funcional que guíe a los usuarios a través del sitio web de manera intuitiva y efectiva" (p. 18). Entre las tecnologías más utilizadas en el desarrollo web se encuentran:

- HTML (HyperText Markup Language): Define la estructura del contenido en la web.
- CSS (Cascading Style Sheets): Determina la apariencia y el diseño visual de los sitios.
- JavaScript: Permite la interactividad en las páginas web.
- Frameworks y bibliotecas: Como React, Angular o Vue.js, facilitan el desarrollo del lado del cliente.
- Lenguajes de backend: Como Python, Java, PHP o Node.js, utilizados para la lógica del servidor.
- Gestión de bases de datos: Mediante sistemas como MySQL, PostgreSQL o MongoDB.

El desarrollo web moderno también ha adoptado nuevas estrategias para garantizar que las plataformas sean accesibles desde cualquier dispositivo. En este sentido, Fernández Casado (2024) explica que "las páginas se deben diseñar dando prioridad a los dispositivos móviles, es decir, primero se tiene en cuenta el diseño para un dispositivo móvil y, si el escenario lo permite o es diferente, se le aplican una serie de reglas para su adecuado funcionamiento y correcta visualización" (p. 8). Este enfoque ha permitido que los sitios web hoy en día ofrezcan una experiencia más uniforme, sin importar el dispositivo desde el cual se está accediendo.

Por último, en el ámbito empresarial, el desarrollo web no se limita únicamente a la creación de sitios, sino que también implica la optimización de plataformas digitales, asegurando escalabilidad, seguridad y rendimiento óptimo, ya que esto permite a las empresas mejorar su competitividad al proporcionar experiencias digitales fluidas y accesibles para todos los usuarios.

Arquitectura de las Aplicaciones

El desarrollo de aplicaciones se basa en una arquitectura que separa responsabilidades en diferentes capas, lo que facilita su mantenimiento y escalabilidad. Estas capas principales son frontend, backend y bases de datos. Según Loyanes Aguilar (2020), el software de aplicación tiene como función principal asistir a los usuarios para ejecutar tareas específicas mediante programas desarrollados en distintos lenguajes y herramientas, permitiendo estructurar las soluciones de forma modular, escalable y reutilizable (p. 31). Así mismo esto lo refuerza (Patel, 2024) mencionando que,

> “La arquitectura de software proporciona una estructura clara para separar las responsabilidades del frontend y el backend. Esta división no solo mejora la organización del código, sino que también permite escalar sistemas con mayor facilidad, mantener la seguridad a lo largo del tiempo y asegurar que diferentes componentes puedan evolucionar independientemente sin comprometer el rendimiento general de la aplicación”. (párr. 3)

Esta separación estructural no solo optimiza el rendimiento de la aplicación, sino que también permite un desarrollo más eficiente y seguro, asegurando la correcta interacción entre las diferentes capas del sistema. Los principales componentes de la arquitectura de aplicaciones incluyen:

- **Fronted:** El frontend es la interfaz con la que los usuarios interactúan. Se encarga de presentar la información y manejar la experiencia visual dentro de una aplicación web. Esta capa se desarrolla con tecnologías como HTML, CSS y JavaScript, y puede incorporar frameworks como React, Vue.js o Angular para mejorar la experiencia de usuario. (Roberts, **2022**)

El principal reto del frontend es lograr una interfaz sea lo más intuitiva, accesible y compatible con distintos dispositivos, garantizando la mejor experiencia de usuario posible.

- **Backed:** Gestiona la lógica del negocio, la seguridad y el almacenamiento de datos. Esta capa interactúa con las bases de datos y responde a las solicitudes del frontend, asegurando que la información proporcionada sea precisa y procesada de manera eficiente (Amazon Web Services, 2023).

Las tecnologías utilizadas en el backend incluyen:

1. Lenguajes de programación: Python, Java, PHP, Ruby, Node.js.
2. Frameworks: Django, Spring Boot, Express.js, Laravel.
3. APIs (Interfaces de Programación de Aplicaciones): REST y GraphQL, utilizadas para la comunicación entre frontend y backend.

También es importante destacar que el backend cumple una función crítica en el desarrollo de aplicaciones web, al encargarse de procesar las solicitudes, ejecutar la lógica de negocio, interactuar con las bases de datos y asegurar que la información enviada al frontend sea precisa y oportuna. Este componente garantiza que la comunicación entre las diferentes capas del sistema

se realice de forma eficiente, lo que permite mantener la estabilidad, seguridad y rendimiento de las plataformas digitales (Arsys, 2024).

- **Bases de datos:** Las bases de datos permiten el almacenamiento, gestión y recuperación de información en una aplicación web. En este sentido, Fernández Casado (2024) destaca que: “una base de datos es esencial para organizar datos de forma estructurada, permitiendo su acceso eficiente y seguro, además de facilitar tareas como las consultas, actualizaciones y eliminación de registros dentro de una aplicación digital” (p. 25). Las bases de datos pueden ser relacionales (MySQL, PostgreSQL) o no relacionales (MongoDB, Firebase), dependiendo de las necesidades del sistema. Un diseño eficiente de bases de datos permite optimizar la velocidad de respuesta de una aplicación, asegurando que la información se almacene de manera estructurada y segura.

Una arquitectura bien estructurada garantiza que las aplicaciones sean seguras, eficientes y capaces de manejar grandes volúmenes de información sin comprometer su estabilidad o rendimiento.

Gestión de la Seguridad de la Información en una Empresa

En un entorno donde la digitalización y la interconectividad son esenciales para la competitividad empresarial, la seguridad de la información se ha convertido en una prioridad estratégica y de alta relevancia. Hoy en día, muchas organizaciones que no cuentan con mecanismos adecuados de protección corren el riesgo de enfrentar ataques cibernéticos, pérdida de datos y sanciones regulatorias. Según Rodríguez Zambrano y Moreno Tamayo (2024), "la ciberseguridad es un tema crucial en el siglo XXI, con diversos enfoques y desafíos planteados por los expertos" (p. 173). Además, Castillo Medina (2021) destaca que "la ciberseguridad y sus escenarios de aplicación son fundamentales para la protección de los sistemas de información en las organizaciones" (p. 165). La gestión de la seguridad de la información no solo protege los activos digitales de una empresa, sino que también fortalece la confianza de sus clientes y socios comerciales. Para Dos Pinos, el garantizar un entorno seguro es esencial para la protección de su infraestructura tecnológica y la integridad de los datos de sus consumidores.

Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI) proporciona un enfoque estructurado para la protección de datos dentro de una organización. Este sistema, basado en normativas internacionales como la ISO 27001, define políticas, procesos y controles para minimizar los riesgos de seguridad de la información. Según Whitman y Mattord (2021), "un SGSI no solo protege los activos digitales, sino que también permite a las empresas responder eficazmente a incidentes de seguridad y garantizar la continuidad del negocio" (p. 62). En Dos Pinos, la implementación de medidas para tener SGSI más optimizado permitiría mejorar la protección de sus sistemas digitales y estandarizar las medidas de seguridad en toda la organización y en este caso también para el departamento de mercadeo.

La adopción de este sistema contribuiría a reforzar la seguridad en el desarrollo web, asegurando que los datos de clientes y empleados sean tratados con los más altos estándares de confidencialidad. Además, permitiría establecer controles claros para la detección y mitigación de amenazas cibernéticas.

Gestión de Riesgos en los Desarrollos Web

Los desarrollos web, debido a su constante evolución y accesibilidad en línea, presentan diversas vulnerabilidades que pueden ser explotadas por atacantes. La gestión de riesgos en estos entornos se centra en la identificación de amenazas, el análisis de impacto y la implementación de estrategias de mitigación. De acuerdo con Stallings (2020), "la gestión de riesgos en el ámbito digital requiere un enfoque proactivo que contemple auditorías regulares, pruebas de seguridad y la actualización continua de las aplicaciones" (p. 88).

La gestión de riesgos en desarrollos web dentro de Dos Pinos es un aspecto fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos personales procesados en sus plataformas digitales. La falta de procesos de identificación de vulnerabilidades en los desarrollos web realizados por agencias externas puede representar un riesgo significativo, afectando no solo la seguridad de la información, sino también el cumplimiento normativo. Según lo establecido en la ISO 27001 y la Ley Nº8968, es indispensable que la empresa implemente un

proceso estandarizado de validación de código fuente, controles de acceso y encriptación de datos, asegurando que todas las plataformas cumplan con requisitos de seguridad adecuados.

En este sentido, la adopción de metodologías para la detección y mitigación de riesgos, como la implementación de auditorías de seguridad y pruebas de penetración, permitirá fortalecer la protección de los desarrollos web. Además, la creación de directrices para las evaluaciones de seguridad garantizará que las agencias externas cumplan con criterios claros en la detección y corrección de vulnerabilidades. Implementar herramientas de escaneo de seguridad, cifrado de datos y validaciones de entrada reducirá ataques, alineándose con el protocolo de aprobación final que establezca los procedimientos de seguridad antes del lanzamiento de nuevos desarrollos digitales en Dos Pinos.

Ciberseguridad Aplicada a Desarrollos Web

La ciberseguridad aplicada a desarrollos web abarca todas aquellas estrategias destinadas a proteger aplicaciones en línea frente a amenazas cibernéticas. A medida que las empresas dependen más de plataformas digitales, los ataques dirigidos a estas infraestructuras se han incrementado. Según Bishop (2021), "la ciberseguridad en entornos web debe incluir la autenticación robusta, la encriptación de datos sensibles y la detección temprana de anomalías para mitigar riesgos" (p. 110).

Para Dos Pinos, el aplicar principios de ciberseguridad en sus desarrollos web es esencial para garantizar la protección de sus consumidores y sus procesos internos. La integración de protocolos como HTTPS, la adopción de firewalls y la implementación de autenticación multifactor fortalecerían la seguridad en los sistemas digitales de la empresa. Asimismo, capacitar al personal en mejores prácticas y procedimientos reduciría el riesgo de incidentes por errores humanos, mejorando la postura de seguridad de la organización.

Identidad y Gestión de Accesos

La gestión de identidades y accesos es un componente clave dentro de la seguridad de la información, ya que regula quién tiene permiso para acceder a determinados recursos dentro de una organización. Según Sandhu y Samarati (2020), "los sistemas de gestión de identidades

permiten controlar y monitorear accesos en tiempo real, garantizando la seguridad de los sistemas y previniendo accesos no autorizados" (p. 45).

En Dos Pinos, fortalecer la gestión de accesos reduciría la exposición a amenazas internas y externas. La implementación de soluciones como el control de acceso en roles, permitiría restringir permisos según el cargo o función del usuario dentro o fuera de la empresa, en este caso, las agencias externas. Establecer políticas claras de acceso y monitoreo de actividad ayudaría a prevenir incidentes de seguridad y mejorar la trazabilidad en los sistemas de la organización y el departamento encargado.

Normativas y Regulaciones para la Gestión de la Información

La seguridad de la información es una preocupación global que ha llevado al desarrollo de marcos regulatorios y normativas que buscan estandarizar la protección de los datos dentro de las organizaciones. En este sentido, ISO/IEC 27001:2022 establece que: "las organizaciones deben implementar un sistema de gestión de seguridad de la información (SGSI) que garantice la confidencialidad, integridad y disponibilidad de los datos, asegurando el cumplimiento de normativas y la mitigación de riesgos asociados a la seguridad digital" (p. 3). Estas regulaciones proporcionan directrices para gestionar y reducir amenazas en el manejo de la información dentro del entorno empresarial.

La implementación de estándares internacionales es clave para fortalecer los mecanismos de protección digital. ISO/IEC 27001:2022 también menciona que: "el establecimiento de controles específicos dentro del SGSI permite a las organizaciones minimizar la exposición a riesgos, definir políticas claras de acceso y respuesta ante incidentes de seguridad" (p. 7). En este contexto, Dos Pinos al alinear sus políticas y procesos con estándares reconocidos, asegura el cumplimiento de estas normativas para fortalecer la seguridad digital y evitar sanciones legales.

Entre las principales regulaciones que impactan la gestión de la seguridad de la información se encuentran la ISO 27001 y la Ley Nº8968 de Protección de Datos Personales en Costa Rica, ambas fundamentales para garantizar la privacidad y protección de los datos dentro del entorno digital de la organización.

Estándar Internacional de Seguridad de la Información

La ISO 27001 es una norma internacional que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Su enfoque basado en la gestión de riesgos permite a las organizaciones identificar, evaluar y mitigar amenazas a la seguridad de los datos. Según Von Solms y Van Niekerk (2021), "la adopción de la ISO 27001 no solo mejora la seguridad de la información dentro de las organizaciones, sino que también eleva su reputación al demostrar compromiso con la protección de datos" (p. 104).

La implementación de la ISO 27001 dentro de Dos Pinos permitiría optimizar la gestión de riesgos en el desarrollo web y asegurar el cumplimiento de buenas prácticas internacionales. La norma establece un marco para la definición de políticas de seguridad, la evaluación de riesgos y la mejora continua en la protección de la información. Entre los beneficios clave de esta norma se incluyen:

- **Protección de datos sensibles:** Garantiza que la información empresarial y de clientes esté protegida frente a accesos no autorizados.
- **Cumplimiento legal y regulatorio:** Asegura que la empresa cumple con las normativas locales e internacionales sobre privacidad y seguridad de los datos.
- **Reducción del impacto de incidentes de seguridad:** Implementar controles basados en la ISO 27001 minimiza el impacto de ataques cibernéticos y fugas de datos.

En un entorno donde las amenazas digitales evolucionan constantemente, la adopción de esta normativa fortalecería la postura de seguridad de Dos Pinos y facilitaría la integración con otros estándares globales de seguridad.

Ley N.ª 8968: Regulación Costarricense de Protección de Datos

En Costa Rica, la Ley Nº8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales regula la recopilación, almacenamiento y uso de información personal. Su objetivo principal es garantizar el derecho a la privacidad y establecer directrices claras sobre la seguridad de los datos manejados por entidades públicas y privadas. Según González (2022), "la Ley 8968 busca equilibrar el derecho a la privacidad con el desarrollo tecnológico, estableciendo obligaciones precisas para quienes manejan información personal" (p. 37).

Para Dos Pinos, el cumplimiento de esta ley es fundamental para evitar sanciones y reforzar la confianza de los consumidores en la gestión de sus datos. Entre las disposiciones clave de la Ley 8968 destacan:

- **Consentimiento informado:** Las empresas deben obtener autorización expresa de los usuarios antes de recolectar o procesar sus datos personales.
- **Principio de finalidad:** La información solo puede ser utilizada para los fines específicos para los que fue recopilada.
- **Seguridad y confidencialidad:** Se exige la implementación de medidas para evitar los accesos no autorizados y garantizar la integridad de los datos.

El cumplimiento de esta regulación también implica la adopción de buenas prácticas en el almacenamiento y tratamiento de datos dentro de los sistemas informáticos de la empresa.

Impacto de las Normativas en la Estrategia de Seguridad de Dos Pinos

Tanto la ISO 27001 como la Ley Nº8968 ofrecen un marco sólido para mejorar la seguridad de la información dentro de la organización, como también del departamento en estudio, que para este contexto, hablamos del área de mercadeo. La combinación de estos estándares representa una oportunidad para fortalecer la confianza del consumidor, mejorar la resiliencia ante amenazas cibernéticas y evitar riesgos legales.

En la actualidad, muchas empresas han optado por la certificación en ISO 27001 como una estrategia para garantizar el cumplimiento normativo y demostrar un compromiso sólido con la seguridad de la información. Esto permite establecer un sistema de protección basado en la mejora continua, lo que reduce la vulnerabilidad ante ataques cibernéticos. Por su parte, la Ley Nº8968 refuerza la necesidad de que las empresas desarrollen medidas proactivas en la protección de datos personales, estableciendo sanciones en caso de incumplimiento. Implementar estos estándares en Dos Pinos permitiría optimizar la seguridad en los desarrollos web y mejorar la gestión de datos dentro de la organización. La alineación con regulaciones internacionales y locales fortalecería la posición de la empresa en el mercado, garantizando la confianza de sus clientes y el cumplimiento de los más altos estándares de seguridad de la información.

CAPÍTULO III: MARCO METODOLÓGICO

El marco metodológico es un elemento fundamental en una investigación, ya que brinda la estructura y el enfoque que se realizará para el proceso investigativo. En este apartado se definen el conjunto de métodos, técnicas y procedimientos que se utilizarán para recolectar y analizar los datos, así también como la forma en la que se interpretarán los resultados obtenidos.

Para el caso de Dos Pinos, se establecerá el enfoque metodológico adecuado para identificar de forma clara y precisa los desafíos en la gestión de la seguridad de la información enmarcada en sus desarrollos web para el departamento de mercado. Con ello, se obtendrán datos y evidencias puntuales de las vulnerabilidades presentes en sus procesos, los controles de acceso existentes y el nivel de cumplimiento de la normativa como ISO 27001/Ley No. 8.968. Asimismo, serán definidos los métodos de análisis y procesamiento de la información para evitar la subjetividad en la interpretación de los hallazgos, de manera que los resultados obtenidos estén alineados a las normas y estándares de protección que establece la organización.

Enfoques de Investigación

La selección de un enfoque de investigación es un aspecto clave para cualquier estudio académico o científico, ya que define la manera de cómo se analizará un fenómeno y los métodos a utilizar para la recolección y tratamiento de datos. Existen tres enfoques principales, los cuales se abordarán a continuación, dando una explicación más detallada de cada uno. Es importante mencionar que la elección del enfoque depende de la naturaleza del problema y los objetivos de la investigación, asegurando la validez y profundidad del estudio.

Enfoque Cuantitativo

El enfoque cuantitativo en la investigación se caracteriza por ser un proceso sistemático y secuencial que tiene como objetivo comprobar hipótesis previamente formuladas mediante el análisis numérico de datos. Parte de una idea que se delimita hasta convertirse en un problema de investigación concreto, del cual se derivan objetivos y preguntas específicas. Posteriormente, se revisa la literatura existente para construir un marco teórico sólido, a partir del cual se formulan hipótesis y se definen las variables a estudiar.

Este enfoque exige un diseño estructurado para recolectar los datos por medio de instrumentos de medición estandarizados, los cuales se analizan empleando métodos estadísticos. Su propósito es identificar patrones, establecer relaciones causales y, en muchos casos, generalizar los resultados a poblaciones más amplias. Según Hernández-Sampieri y Mendoza Torres (2023), esta ruta "parte de la teoría, de la cual se derivan las hipótesis que el investigador somete a prueba. Va de lo general a lo particular" (p. 7).

La precisión en la medición, el uso de técnicas estadísticas y el control riguroso sobre los procesos son fundamentales para garantizar la validez y confiabilidad de los resultados. Asimismo, este enfoque favorece la replicabilidad de los estudios y la predicción de fenómenos observables en diferentes contextos.

Enfoque Cualitativo

El enfoque cualitativo se orienta a la exploración profunda de significados, percepciones y experiencias humanas desde la perspectiva de los participantes. Este tipo de investigación no sigue una secuencia rígida, sino que adopta un proceso inductivo, flexible y emergente, ajustado a las particularidades del fenómeno estudiado. A diferencia del enfoque cuantitativo, no busca la generalización estadística, sino comprender la realidad desde el contexto natural en que ocurre, identificando los porqués de los hechos sociales y las relaciones entre categorías conceptuales.

Según Hernández-Sampieri y Mendoza Torres (2023), la ruta cualitativa "resulta apropiada cuando se desea conocer el significado de las experiencias y los valores humanos, el punto de vista interno e individual de las personas y el ambiente natural en que ocurre el fenómeno estudiado" (p.420). Este enfoque se apoya en métodos como entrevistas a profundidad, observación participante y grupos focales, que permiten captar la riqueza del entorno y las voces de quienes lo habitan.

El análisis cualitativo implica la interpretación de los datos, buscando patrones, significados y relaciones entre conceptos. La flexibilidad del diseño permite adaptar las técnicas en función de los hallazgos emergentes, generando un conocimiento más cercano a la realidad de los sujetos. En síntesis, este enfoque es valioso para explorar fenómenos complejos que no pueden

medirse numéricamente y para generar teorías fundamentadas en la experiencia vivida de los participantes.

Enfoque Mixto

El enfoque mixto combina estrategias de los enfoques cuantitativo y cualitativo para obtener una visión más completa del fenómeno estudiado. Hernández-Sampieri y Mendoza Torres (2023) explican que “los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio” (p. 634).

Este método permite validar hallazgos mediante la triangulación de datos, combinando mediciones numéricas con el análisis de percepciones y experiencias. Asimismo, los autores destacan que “el proceso de investigación y las estrategias utilizadas se adaptan a las necesidades, contexto, circunstancias, recursos, pero sobre todo al planteamiento del problema” (p. 634).

Su aplicación es útil en estudios donde se requiere tanto la medición objetiva de variables como el análisis interpretativo, siendo común en áreas como salud, educación y evaluación de impacto.

Tipo de Enfoque Seleccionado

Para esta investigación se ha seleccionado un enfoque cualitativo, ya que permite analizar la seguridad en los desarrollos web de Dos Pinos desde una perspectiva comprensiva y contextual. Este enfoque facilitará la exploración de los procesos, prácticas actuales del departamento de mercadeo y percepciones sobre la gestión de la seguridad de la información en la empresa.

Según Hernández-Sampieri, Fernández y Baptista (2023), “la investigación cualitativa te proporcionará un panorama completo y detallado de lo que piensan todos en la empresa y te facilitará que tus recomendaciones concretas sean más realistas y pertinentes" (p. 411). Por medio de este enfoque, se busca generar información detallada que contribuya a identificar áreas de mejora en la protección de los activos digitales de Dos Pinos para el departamento de mercadeo.

El enfoque cualitativo es adecuado para esta investigación, ya que permite recoger información de fuentes primarias como entrevistas y documentos internos, brindando un análisis

interpretativo que ayude a comprender los factores que inciden en la seguridad digital dentro de la organización. Además, este método facilita la identificación de patrones, desafíos y oportunidades en la gestión de riesgos de seguridad informática.

Tipos de Investigación

Como parte de este proceso de estructuración del marco metodológico, es esencial definir el tipo de investigación que mejor se adapte a los objetivos planteados en esta propuesta. La clasificación de los tipos de investigación permite seleccionar el enfoque metodológico adecuado, facilitando la recopilación y análisis de datos de manera efectiva.

Cada tipo de investigación posee características particulares que determinan su aplicación en distintos contextos. La elección correcta influye directamente en la manera en que se desarrollará el estudio, en la forma de abordar la problemática y en la interpretación de los resultados obtenidos. Con este contexto, se explicarán los principales tipos de investigación, sus particularidades y la importancia de su aplicación.

Investigación Exploratoria

Este tipo de investigación tiene como objetivo el examinar un problema poco estudiado o sobre el cual existe escasa información previa. Permite generar un panorama más general del fenómeno, identificando conceptos clave y sentar las bases para investigaciones futuras más estructuradas. Se caracteriza por su flexibilidad en la recopilación de datos, lo que facilita la adaptación a contextos con información limitada.

En este sentido, Hernández-Sampieri, Fernández y Baptista (2023) mencionan que “los estudios exploratorios se llevan a cabo cuando el propósito es examinar un fenómeno o problema de investigación nuevo o poco estudiado, sobre el cual se tienen muchas dudas o no se ha abordado antes; es decir, cuando la revisión de la literatura reveló que tan solo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si deseamos indagar sobre temas y áreas desde perspectivas innovadoras”. (p. 107)

Dado que los estudios exploratorios no buscan probar hipótesis, sino descubrir patrones y tendencias, suelen emplear metodologías flexibles como entrevistas a expertos, revisión de documentales y estudios de caso. Hernández-Sampieri et al. (2023) explican que: "estos estudios

pueden ayudar a establecer prioridades en la investigación, sugiriendo hipótesis o identificando variables relevantes para estudios posteriores" (p. 108). Estos métodos permiten al investigador ampliar su conocimiento sobre el problema y definir estrategias más adecuadas para su análisis.

Investigación Descriptiva

Por su parte, la investigación descriptiva se centra en analizar y detallar las características de un fenómeno sin manipular variables, permitiendo obtener una visión aún más clara y organizada del problema por resolver. Este tipo de estudio busca medir conceptos y definir variables de manera precisa.

Según Hernández-Sampieri et al., (2023) explican que: “los estudios descriptivos pretenden especificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, miden o recolectan datos y reportan información sobre diversos conceptos, variables, aspectos o dimensiones del fenómeno o problema a investigar” (p. 109).

A diferencia de los estudios exploratorios, que buscan una primera aproximación al fenómeno, la investigación descriptiva profundiza en sus elementos y los mide de forma estructurada. Esta clase de estudios es útil para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso o contexto específico. Como afirman Hernández-Sampieri et al., (2023), “la descripción puede ser más o menos profunda, aunque en cualquier caso se basa en la medición de uno o más atributos del fenómeno o problema de interés” (p. 109).

Estos estudios permiten obtener información organizada que puede servir como base para investigaciones posteriores, facilitando la toma de decisiones o la formulación de estrategias en distintos ámbitos académicos y profesionales.

Investigación Explicativa

Por último, este tipo de investigación busca identificar las causas de un fenómeno o problema, y establecer relaciones de causalidad entre variables. Su propósito es responder a preguntas sobre el por qué y el cómo ocurren ciertos eventos, proporcionando un mayor grado de comprensión del objeto de estudio. A diferencia de los estudios descriptivos y exploratorios, este enfoque permite analizar la interacción entre variables y sus efectos.

Según Hernández-Sampieri et al., (2023), “los estudios explicativos van más allá de la descripción de fenómenos, conceptos o variables, o del establecimiento de relaciones entre estas; están dirigidos a responder por las causas de los eventos y fenómenos de cualquier índole” (p. 112). Su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables.

Este tipo de estudio requiere un diseño metodológico estructurado que permita demostrar relaciones de causa y efecto. Para ello, es necesario evaluar variables en diferentes contextos y analizar sus posibles influencias mutuas. Hernández-Sampieri, Fernández y Baptista (2023) afirman que “el determinar las causas de una problemática es un paso indispensable para resolverla” (p. 113).

Tipo de Investigación Seleccionado

Para esta investigación, se ha seleccionado la investigación descriptiva, ya que permite analizar y documentar de manera detallada las características y procesos relacionados con la seguridad en los desarrollos web del Departamento de Mercadeo de Dos Pinos. Este tipo de investigación facilita la identificación de patrones y la estructuración de información sobre la gestión de la seguridad informática, sin intervenir en las variables del estudio.

La elección de este enfoque se alinea con la necesidad de comprender cómo se aplican las normativas ISO 27001 y la Ley Nº8968 de Protección de Datos Personales en los desarrollos web de la empresa. A través de la investigación descriptiva, se podrá evaluar la implementación de controles de acceso, creaciones de normativas y validaciones de seguridad dentro del departamento, proporcionando un marco de referencia claro para futuras mejoras en la gestión de la seguridad de la información.

Fuentes de Información

Las fuentes de información son aquellos medios utilizados para obtener datos relevantes sobre un tema específico. A partir de estas fuentes, se recopilan datos que permiten profundizar en el tema de interés o completar detalles con aportes adicionales de otros autores hayan hecho alguna investigación al respecto.

Es fundamental tener en cuenta que, dependiendo del tipo de investigación y su propósito, es necesario realizar una búsqueda previa, ya que existen numerosos formatos y tipos de fuentes. Estas pueden incluir libros, artículos de periódicos, encuestas, documentos emitidos por instituciones públicas, entrevistas, videos, entre otros.

Cada fuente debe ser evaluada según su confiabilidad, considerando la precisión de la información y su grado de comprobación. Por esa razón, se recomienda contrastar los datos obtenidos con diferentes fuentes y analizar su trayectoria o reputación, para garantizar la validez de la información.

Fuentes de Información Primaria

Las fuentes primarias constituyen el primer contacto con los datos originales, obtenidos de manera directa por el investigador sin intermediarios. Se recolectan a través de herramientas como encuestas, entrevistas, observaciones directas o pruebas, permitiendo obtener información específica y contextualizada sobre el objeto de estudio. Según el portal Concepto.de, "proporcionan datos nuevos, directos, sin alterar ni interpretar, como registros, documentos, encuestas o entrevistas" (Concepto.de, 2024, párr. 6).

En el contexto de la investigación en Dos Pinos, la recopilación de información primaria será fundamental para evaluar directamente la percepción de los responsables de TI y mercadeo sobre la gestión de seguridad en los desarrollos web. Este tipo de datos permitirá obtener una visión clara de los procesos internos, identificar vulnerabilidades específicas y proponer soluciones adecuadas a las necesidades reales de la organización.

Fuentes de Información Secundaria

La información secundaria se refiere a los datos que ya han sido recolectados, procesados y publicados por otras fuentes. Este tipo de información se obtiene a partir de documentos como artículos académicos, informes, bases de datos, registros institucionales o estadísticas gubernamentales. Según Concepto.de (2024), "este tipo de fuente recopila, analiza o interpreta información procedente de otras fuentes, organizándola de forma accesible para distintos fines informativos o investigativos" (párr. 10).

Dicho lo anterior, esta información será útil para analizar estudios previos relacionados con la seguridad de la información, así como para evaluar el cumplimiento de normativas como la ISO

27001 y la Ley Nº8968 de Protección de Datos Personales en Costa Rica. Este tipo de información complementará los datos primarios, proporcionando una base sólida para validar hallazgos y generar recomendaciones fundamentadas en evidencia previamente recopilada.

Fuentes de Información Terciaria

Las fuentes de información terciaria recopilan, organizan y presentan datos provenientes de fuentes primarias y secundarias. Su función principal es ofrecer resúmenes, índices o guías de contenidos que faciliten el acceso a la información ya existente. Este tipo de fuentes es útil cuando se busca obtener una visión general de un tema o identificar documentos relevantes que profundicen en áreas específicas.

De acuerdo con la Universidad de Puerto Rico, Recinto de Río Piedras (2022), "las fuentes terciarias identifican, recopilan o indizan fuentes sobre una disciplina o tema. Muchas sirven para encontrar fuentes secundarias y primarias" (párr. 3).

Ejemplos comunes de fuentes terciarias incluyen:

- Enciclopedias: Resúmenes organizados de información general.
- Índices bibliográficos: Herramientas que permiten ubicar rápidamente artículos o libros en diferentes bases de datos.
- Directorios: Listados organizados de instituciones o especialistas en un campo.
- Bases de datos temáticas: Recopilaciones de documentos categorizados por áreas de conocimiento.

Este tipo de fuente es particularmente útil al inicio de un proyecto de investigación, ya que permite estructurar una base sólida a partir de la cual desarrollar un análisis más profundo.

Variables

Las variables son elementos esenciales en toda investigación, ya que permiten observar, medir y analizar fenómenos específicos. En este sentido, Arroyo Valenciano (2022) destaca lo siguiente:

> "La comunidad científica coincide en que tanto el problema como la hipótesis comparten un elemento común y sustancial: las variables. El éxito y la precisión de una investigación dependen de la rigurosidad con que cada una de ellas sea definida, ya que constituyen la

base sobre la cual se construyen la formulación del problema, las hipótesis y el análisis de datos" (p. 2).

En esta investigación, las variables seleccionadas permitirán abordar de manera precisa el problema planteado, facilitando el análisis de los datos recolectados.

Variables Conceptuales

La definición conceptual establece como el significado teórico de una variable, basado en definiciones reconocidas por la comunidad científica. Estas definiciones, consideradas técnicas y específicas, permiten comprender el concepto desde una perspectiva académica y profesional.

Arroyo Valenciano (2022) menciona que,

"La definición conceptual se construye mediante la revisión teórica de fuentes documentales y representa el acuerdo existente entre investigadores y expertos sobre cómo debe entenderse una variable dentro de un marco de referencia específico" (p. 4).

Esta formulación orienta la comprensión de la variable a lo largo del proceso investigativo, asegurando coherencia en su aplicación y respaldo en fuentes confiables.

Variables Operacionales

Para el caso de las variables operacionales, podemos definir como la transformación de conceptos abstractos en elementos observables y medibles. de modo que puedan ser evaluados.

Este proceso permite descomponer la variable en dimensiones e indicadores, facilitando su evaluación y asegurando la coherencia en la recolección de datos. Como señala Arroyo Valenciano (2022), la definición operacional "traduce los conceptos teóricos en procedimientos que permiten medirlos o valorarlos en el contexto del estudio" (p. 4).

De este modo, se garantiza que la medición esté alineada con los objetivos de la investigación.

Variables Instrumentales

Los instrumentos permiten recolectar información de manera precisa y coherente con los objetivos del estudio. La elección del instrumento dependerá de la naturaleza de la variable y del

tipo de datos que se necesiten obtener. Según Arroyo Valenciano (2022), los instrumentos “constituyen el mecanismo mediante el cual se asignan valores o categorías observables a una variable” (p. 4).

La elección del instrumento dependerá de la naturaleza de la variable y del tipo de datos que se necesiten obtener. Entre los más utilizados se encuentran cuestionarios, entrevistas, listas de verificación y guías de observación, los cuales facilitan la obtención de datos confiables para el análisis.

Tabla 4
Unidades de análisis (variables)

Objetivos específicos	Variable	Variable conceptual	Variable operacional	Variable instrumental
Elaborar un proceso estándar para la validación del código fuente, control de accesos y cifrado de datos.	Proceso de validación de seguridad en los desarrollos	Según ComplianceQuest (2022), la validación de software es la "confirmación mediante examen y provisión de evidencia objetiva de que las especificaciones del software se ajustan a las necesidades del usuario y usos previstos, y que los requisitos particulares implementados a través del software pueden cumplirse de manera consistente" (párr. 2). Este proceso implica la realización de pruebas y auditorías para identificar y corregir posibles vulnerabilidades antes de la implementación del sistema.	Entrevista Encuesta	Guía de entrevista. Cuestionario.
Desarrollar directrices para evaluaciones de seguridad en desarrollos web.	Directrices para evaluación	La ISO/IEC 27001:2022 establece que "las directrices de seguridad permiten evaluar la efectividad de los controles en sistemas, mediante auditorías y pruebas técnicas" (p. 134).	Entrevista Encuesta	Guía de entrevista. Cuestionario.

Formular una normativa de verificación de seguridad obligatoria.	Normativa de verificación de la seguridad	Según la ISO/IEC 27001:2022, "un SGSI permite gestionar los riesgos de seguridad de manera efectiva, garantizando la protección de la información" (p. 85).	Entrevista Encuesta	Guía de entrevista. Cuestionario.
Crear políticas para la actualización periódica de los estándares de seguridad.	Políticas de cumplimento de estándares nacionales e internacionales	Según SafetyCulture (2023), "las auditorías de cumplimiento ayudan a las empresas a cumplir las leyes, reglamentos y normas del sector" (párr. 5).	Entrevista Encuesta	Guía de entrevista. Cuestionario.
Crear un protocolo de aprobación final para verificación de seguridad antes del lanzamiento.	Protocolo de aprobación final de la Web	La ISO/IEC 27001:2022 establece que "antes de la puesta en producción, los sistemas deben someterse a procesos de evaluación de seguridad, incluyendo pruebas de vulnerabilidad y auditorías, para garantizar el cumplimiento de los controles establecidos" (p. 190).	Entrevista Encuesta	Guía de entrevista. Cuestionario.

Fuente: *Vega, 2025.*

Instrumentos de Recolección de Datos

Los instrumentos de recolección de datos están diseñados para obtener información de manera sistemática y estructurada. Hernández-Sampieri, Fernández y Baptista (2023), mencionan que: “para recolectar datos disponemos de una gran variedad de instrumentos o técnicas, tanto cuantitativas como cualitativas; y en un mismo estudio podemos utilizar ambos tipos” (p. 234).

Su función principal es garantizar que los datos obtenidos sean válidos y confiables, facilitando el análisis posterior. La elección del instrumento adecuado dependerá de la naturaleza de la investigación, las variables definidas y el enfoque metodológico adoptado.

Cuestionario

Se define como el instrumento encargado de recolectar datos por medio de un conjunto estructurado de preguntas, diseñado para obtener información específica sobre un tema o problema determinado. De acuerdo con Hernández-Sampieri, Fernández y Baptista (2023), un cuestionario:

> "es un conjunto organizado y estandarizado de preguntas respecto de una o más variables a medir. Debe ser congruente con el planteamiento del problema e hipótesis. Los cuestionarios se utilizan en encuestas de todo tipo, por ejemplo, para calificar el desempeño de un gobierno, conocer las necesidades de hábitat de futuros compradores de viviendas y evaluar la percepción ciudadana sobre ciertos problemas como la inseguridad. Pero también se implementan en otros campos. Por ejemplo, un ingeniero en minas usó un cuestionario como herramienta para que expertos de diversas partes del mundo aportaran opiniones calificadas con el fin de resolver ciertas problemáticas de producción en la industria". (p. 259)

Los cuestionarios son ampliamente utilizados en investigaciones cuantitativas, ya que permiten recopilar datos de manera eficiente, estandarizada y en función de las variables previamente definidas. Además, facilitan el análisis estadístico de las respuestas, garantizando la comparabilidad de los resultados.

Entrevista

La entrevista es una técnica cualitativa de recolección de datos utilizada para obtener información detallada directamente de los participantes. Según Hernández-Sampieri, Fernández y Baptista (2023), "la entrevista cualitativa es más íntima, flexible y abierta que la cuantitativa y permite la construcción conjunta de significados respecto a un tema" (p. 469).

Hoy en día existen diferentes tipos de entrevistas: la estructurada, la semiestructurada y la no estructurada. La entrevista estructurada se caracteriza por seguir un guion rígido de preguntas previamente definidas, mientras que la semiestructurada permite mayor flexibilidad, adaptando las preguntas según las respuestas del entrevistado. Finalmente, la entrevista no estructurada se desarrolla como una conversación libre, guiada por el criterio del investigador.

La utilidad de la entrevista radica en su capacidad para profundizar en las experiencias y percepciones de los entrevistados. Hernández-Sampieri, Fernández y Baptista (2023) destacan que este instrumento permite lograr "una comunicación y la construcción conjunta de significados

respecto a un tema" (p. 469) y se desarrolla especialmente cuando el problema de estudio no puede observarse directamente o se requiere conocer más perspectivas.

La Observación

La observación es una técnica de recolección de datos que consiste en el registro sistemático, válido y confiable de comportamientos o eventos tal como ocurren en su contexto natural. En la investigación cualitativa, observar va más allá de simplemente ver: implica involucrar todos los sentidos, interpretar lo que se presencia y registrarlo con propósito investigativo. Según Hernández-Sampieri, Fernández y Baptista (2023), "la observación investigativa no se limita al sentido de la vista, sino a todos los sentidos" (p. 465), permitiendo comprender a profundidad el entorno y las interacciones sociales en su forma más natural.

Existen diferentes tipos de observación según el grado de participación del investigador y el nivel de estructuración del proceso:

Según la participación del observador:

- **Observación participante:** El investigador se integra en el grupo o situación que estudia, interactuando directamente con los sujetos de investigación.
- **Observación no participante:** El investigador se mantiene al margen, sin intervenir ni interactuar con el entorno observado.

Según la estructuración:

- **Observación estructurada:** Se realiza siguiendo un esquema previamente definido, donde se identifican las categorías de análisis y los aspectos específicos que se observarán.
- **Observación no estructurada**: No sigue un esquema rígido; el investigador registra los eventos conforme surgen, permitiendo mayor flexibilidad.

Según el grado de sistematización:

- **Observación directa:** El investigador presencia los hechos directamente en el momento en que ocurren.
- **Observación indirecta:** Se realiza a partir de registros, como videos o grabaciones previas.

La observación permite obtener información detallada y contextualizada sobre los fenómenos estudiados, facilitando la comprensión de comportamientos, procesos o interacciones que otros instrumentos no pueden captar de manera tan directa.

Proceso para la Recolección y Análisis de Datos

El proceso de recolección y análisis de datos de esta investigación es de tipo cualitativo, con la finalidad de lograr una comprensión detallada acerca del manejo de la seguridad en los desarrollos web del Departamento de Mercadeo de Dos Pinos. Bajo este enfoque, se implementarán dos técnicas principales: la entrevista semiestructurada y el cuestionario.

Por un lado, las entrevistas semiestructuradas se aplicarán a los responsables del área del departamento de mercadeo y de seguridad informática dentro de Dos Pinos, así como los representantes de las agencias externas para los desarrollos web. Este instrumento permitirá saber cuáles son las prácticas actuales del manejo de seguridad, la implementación de las regulaciones, y los retos que enfrentan para cumplir con los estándares IS0 27001 y la Ley Nº8968.

En complemento, se utilizarán cuestionarios para obtener información más amplia sobre el cumplimiento de controles de seguridad en los desarrollos web. Para ello, se emplearán formularios de Microsoft Forms para el caso de los funcionarios que trabajan en Dos Pinos, garantizando que la información recolectada quede almacenada dentro del entorno digital de la empresa, asegurando su accesibilidad y seguridad. En el caso de las agencias externas, se utilizarán formularios de Google Forms, permitiendo un acceso más flexible a los encuestados.

La información recolectada se organizará por medio de un análisis de contenido en el cual se utilizará y se categorizará a través de patrones y temáticas en las respuestas de los participantes. En complemento con todo lo mencionado, se realizará una revisión documental de las políticas internas, procedimientos de seguridad y lineamientos normativos vigentes dentro de la cooperativa, con el fin de contrastar los datos obtenidos en la investigación.

Finalmente, los resultados serán documentados y analizados en función de su relación con los objetivos planteados, permitiendo la formulación de recomendaciones estratégicas orientadas a fortalecer la seguridad de los desarrollos web en el departamento. Este enfoque garantizará un análisis integral y descriptivo, alineado con la metodología establecida en este estudio.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

El presente capítulo tiene como propósito exponer y analizar los resultados obtenidos mediante la aplicación de los instrumentos de recolección de información definidos en el proyecto: un cuestionario dirigido al personal del Departamento de Mercadeo y a proveedores externos vinculados con el desarrollo de sitios web, así como una entrevista aplicada a dos colaboradores del Departamento de Tecnologías de Información de la Cooperativa de Productores de Leche Dos Pinos.

Ambos instrumentos fueron diseñados para identificar prácticas, vacíos y oportunidades de mejora relacionados con todo el proceso de la seguridad de los desarrollos web utilizados en campañas digitales por parte del Departamento de Mercadeo, con énfasis en aspectos como la validación previa de los sitios, los controles de acceso, la protección de datos personales, el uso de listas de verificación, la existencia de procesos de aprobación formal, la capacitación del personal y el monitoreo posterior al lanzamiento.

Los resultados expuestos a continuación permiten evidenciar el nivel de cumplimiento actual con los principios establecidos en la norma ISO/IEC 27001:2022 y con los requerimientos de la Ley Nº8968, así como sustentar técnicamente la necesidad de establecer procedimientos, normas y directrices formales que regule la revisión y control de seguridad de los desarrollos web.

Cuestionario

Con el objetivo de obtener una visión más clara sobre las prácticas actuales en torno a la seguridad de los desarrollos web impulsados desde el Departamento de Mercadeo, se aplicó un cuestionario estructurado dirigido tanto a colaboradores internos del departamento como a proveedores externos que han estado actualmente involucrados en la creación de sitios, micrositios o formularios digitales utilizados en campañas de comunicación.

El cuestionario fue conformado por quince preguntas cerradas y una pregunta abierta, distribuidas en cinco bloques temáticos: validación previa, revisión de seguridad y requisitos para agencias, uso de listas de verificación, actualización de medidas de seguridad, y seguimiento posterior al lanzamiento. La estructura de las preguntas fue diseñada para explorar el cumplimiento de buenas prácticas alineadas con la norma ISO/IEC 27001:2022 y los principios establecidos por la Ley Nº8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.

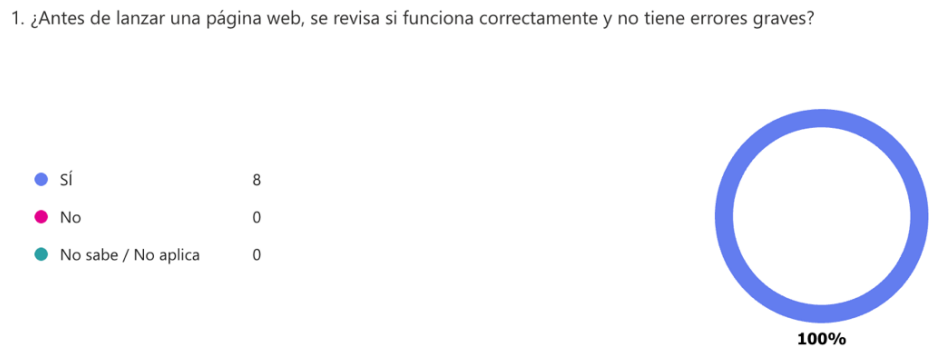
La participación fue totalmente voluntaria y anónima, y la recolección se realizó por medio de un formulario de la suite de Microsoft. Los datos obtenidos a partir de las respuestas permitieron identificar patrones comunes, debilidades en los procesos y oportunidades de mejora en las prácticas de validación, supervisión y seguimiento de los desarrollos web.

Bloque 1: Validación de funcionamiento, accesos y protección de datos.

En este bloque se exploraron prácticas relacionadas con la revisión técnica previa, los controles de acceso y la protección de datos personales.

Figura 1

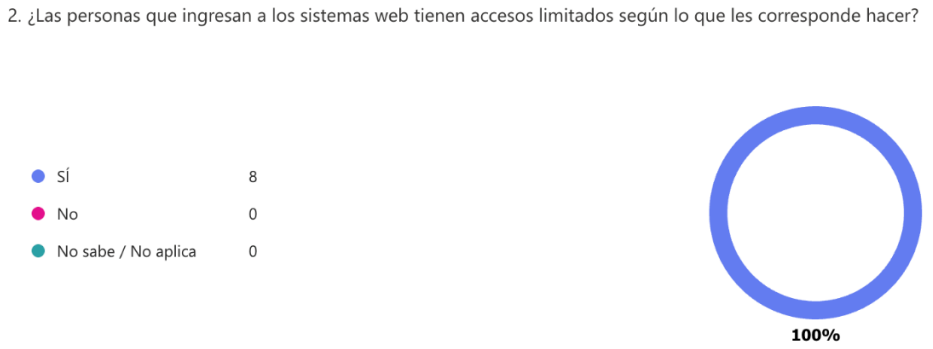
Pregunta: Funcionamiento del Desarrollo web.



Fuente: *Vega, 2025.*

Figura 2

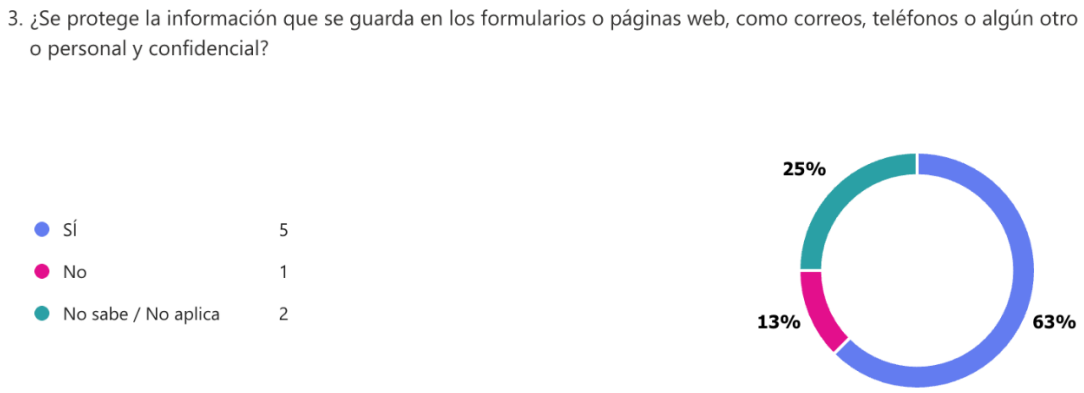
Pregunta: Accesos limitados según rol de usuario.



Fuente: *Vega, 2025.*

El 100 % de las personas encuestadas indicó que se revisa el funcionamiento del sitio antes de lanzarlo y que los accesos están limitados según el rol del usuario, lo cual evidencia una práctica básica de control previo.

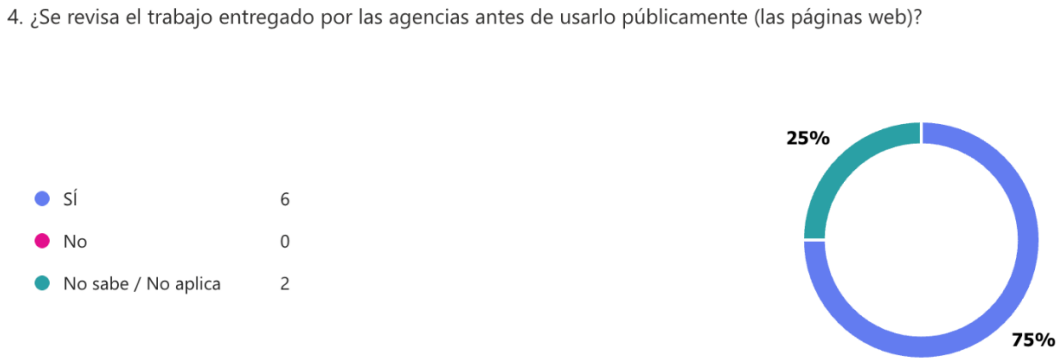
Figura 3
Pregunta: Protección de datos personales.



Fuente: *Vega, 2025.*

En cuanto a la protección de datos personales, solo el 62 % afirmó que sí se aplican medidas. El restante 38 % (sumando respuestas negativas o de desconocimiento) refleja una falta de claridad o estandarización en este tema.

Figura 4
Pregunta: Revisión previa a lanzamientos



Fuente: *Vega, 2025.*

Finalmente, el 75 % señaló que sí se revisa lo entregado por las agencias antes de publicarlo, aunque un 25 % indicó no tener conocimiento al respecto, lo cual sugiere una debilidad en la trazabilidad del proceso.

- **Hallazgos clave:**

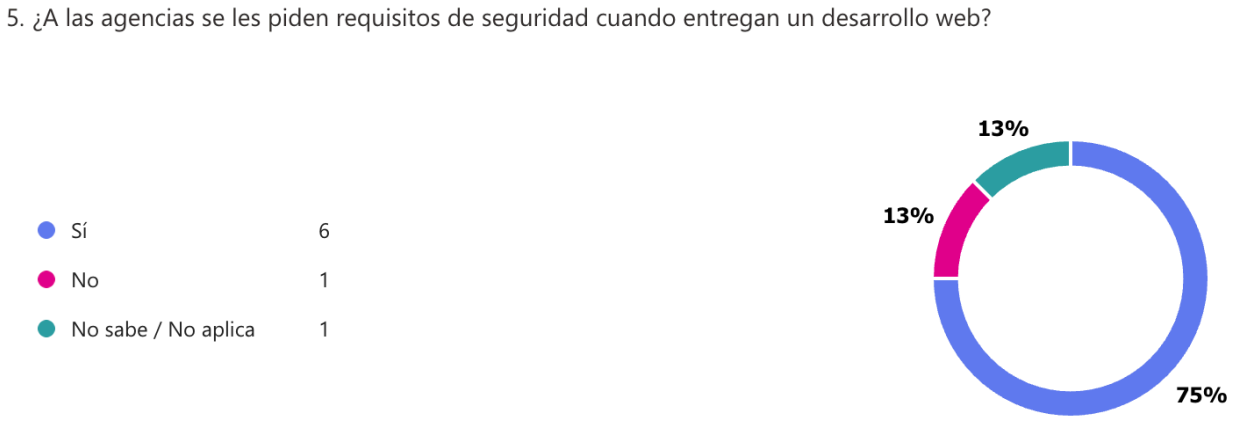
- Hay revisión funcional y control de accesos, pero la protección de datos no es consistente en el proceso.
- No todos los involucrados en estos proyectos tienen claridad sobre la revisión del trabajo de las agencias, lo que puede afectar el control de calidad.

Bloque 2: Revisión de seguridad y requisitos para agencias externas.

Se abordó las condiciones de seguridad exigidas a las agencias externas y el tratamiento de entregables que no cumplen con los requisitos.

Figura 5

Pregunta: Requisitos de seguridad

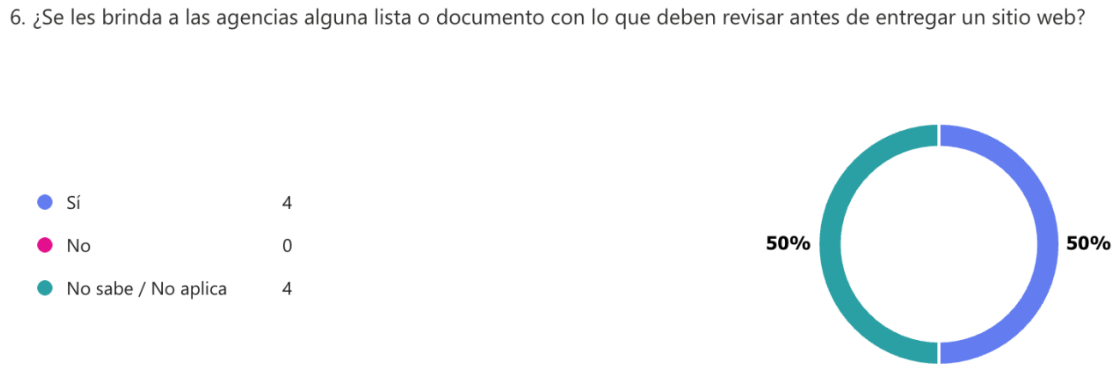


Fuente: *Vega, 2025.*

El 75 % de las personas encuestadas indicó que sí se solicitan requisitos de seguridad a las agencias, aunque un 12 % respondió que no, y otro 12 % dijo no saber, lo cual refleja una falta de comunicación en esta práctica.

Figura 6

Pregunta: Listas o documentos de verificación.

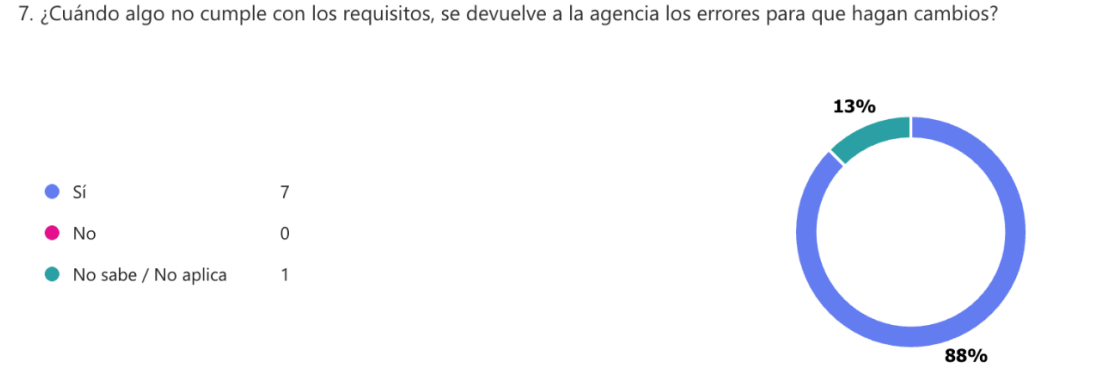


Fuente: *Vega, 2025.*

En cuanto a la entrega de listas o documentos de verificación por parte del departamento, solo el 50 % confirmó que sí se proporciona esta guía, mientras que el otro 50 % manifestó desconocerlo, lo que sugiere que no existe un mecanismo estandarizado y visible para todos los involucrados en el proceso.

Figura 7

Pregunta: Cumplimiento de requisitos y evaluación de errores



Fuente: *Vega, 2025.*

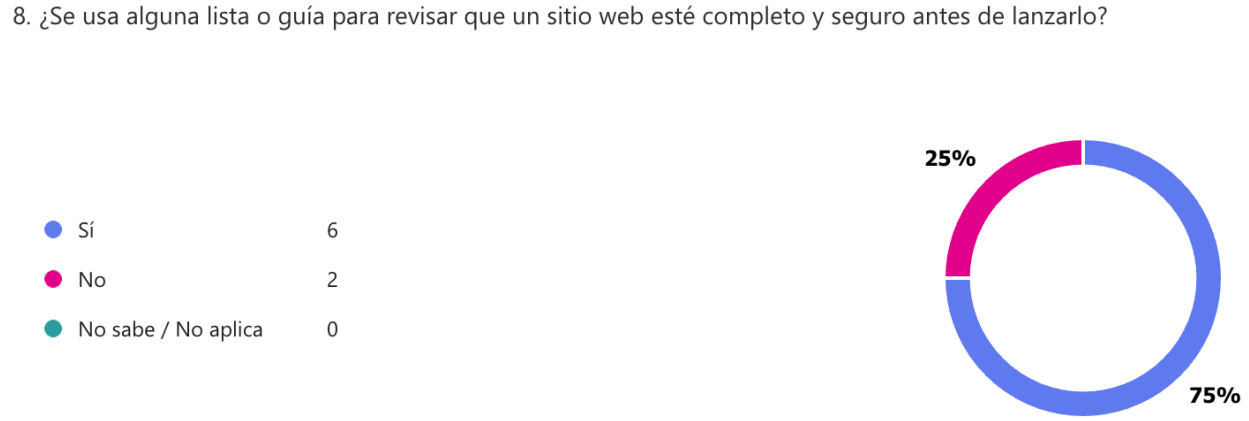
Finalmente, el 88% señaló que, si un desarrollo no cumple con los requisitos, sí se devuelve a la agencia para realizar correcciones, aunque el 12% indicó no estar seguro, lo cual podría deberse a una falta de trazabilidad o formalización del proceso de devolución.

- **Hallazgos clave:**
- Aunque se exigen ciertos requisitos de seguridad, la entrega de guías o listas formales no está clara para todo el equipo.
- La gestión de errores por parte de las agencias funciona, pero no todos los involucrados conocen el procedimiento correcto o lo ejecutan al pie de la letra.

Bloque 3: Uso de listas de verificación o control previo al lanzamiento.

Este segmento evaluó la existencia de herramientas de control antes de publicar un sitio web, como listas de verificación y procesos de aprobación formal.

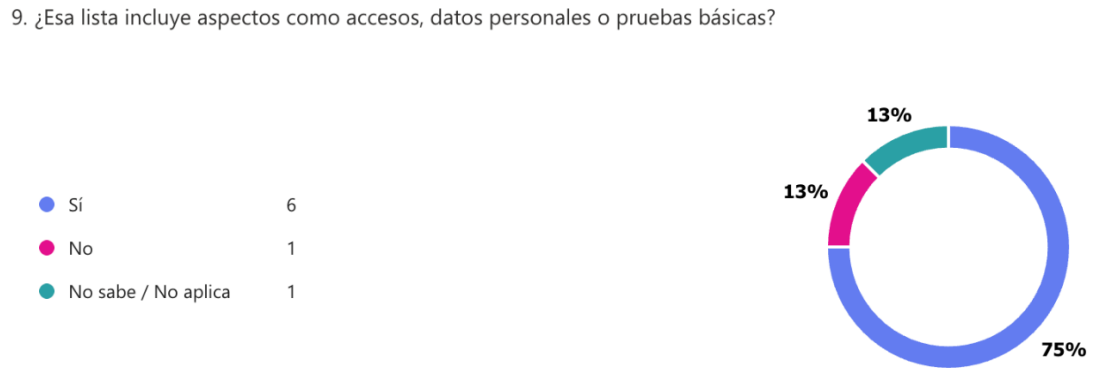
Figura 8
Pregunta: Guía de verificación



Fuente: *Vega, 2025.*

El 75 % de los encuestados afirmó que sí se utiliza una lista o guía para verificar que un sitio esté completo y seguro antes de su lanzamiento. Sin embargo, el 25 % respondió que no, lo que evidencia una aplicación parcial de esta práctica.

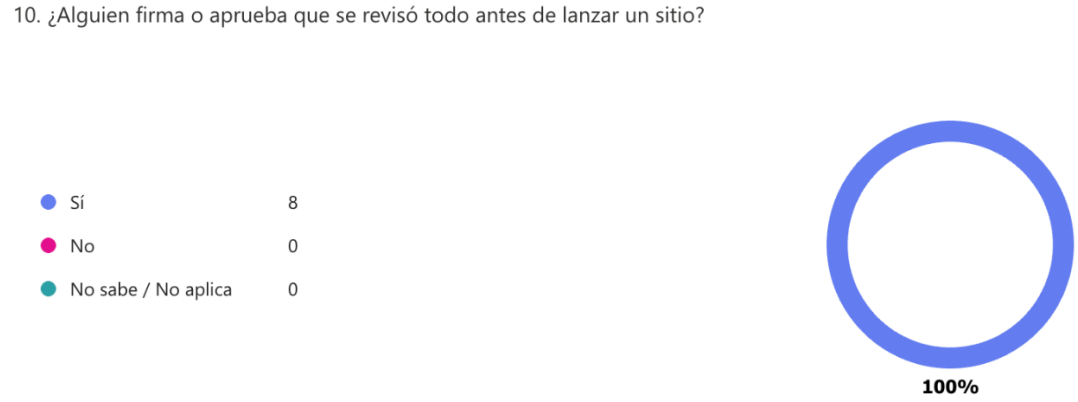
Figura 9
Pregunta: Contenido de listas de verificación



Fuente: *Vega, 2025.*

Respecto al contenido de dicha lista, el 75 % indicó que incluye aspectos como accesos, datos personales o pruebas básicas, aunque un 12 % respondió que no y otro 12 % dijo no saber, lo cual sugiere que no todos conocen con claridad el alcance de lo que se revisa de cara al lanzamiento del desarrollo.

Figura 10
Pregunta: Aprobación pre lanzamiento



Fuente: *Vega, 2025.*

Finalmente, el 100 % señaló que sí existe una firma o aprobación previa al lanzamiento, lo cual indica un proceso de validación formal, al menos en apariencia.

- **Hallazgos clave:**

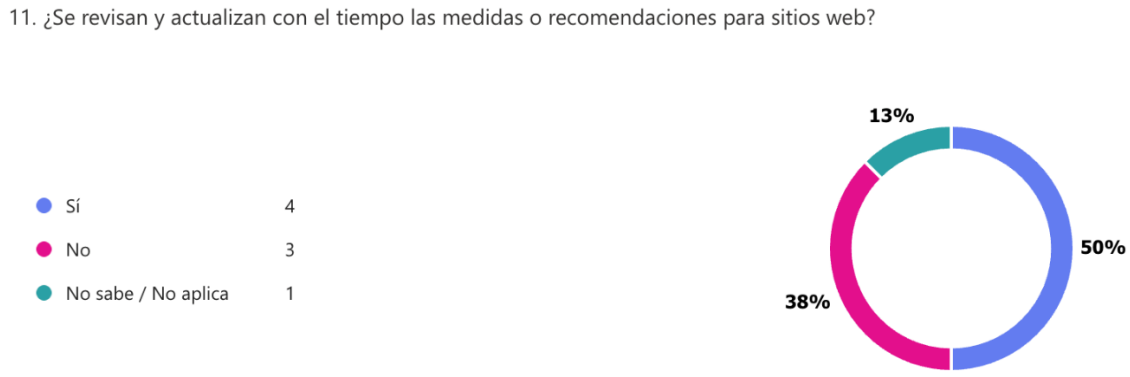
- Aunque la mayoría afirma usar una lista de verificación, una cuarta parte no aplica esta herramienta, lo que evidencia inconsistencias en su adopción.
- La existencia de una firma de aprobación es reconocida por todos, pero el contenido y uso de las listas aún no está estandarizado en el proceso.

Bloque 4: Actualización de prácticas o medidas de seguridad.

Este bloque se centró en identificar si existen procesos activos de actualización, formación y adaptación a nuevas normativas.

Figura 11

Pregunta: Actualización de medidas de seguridad

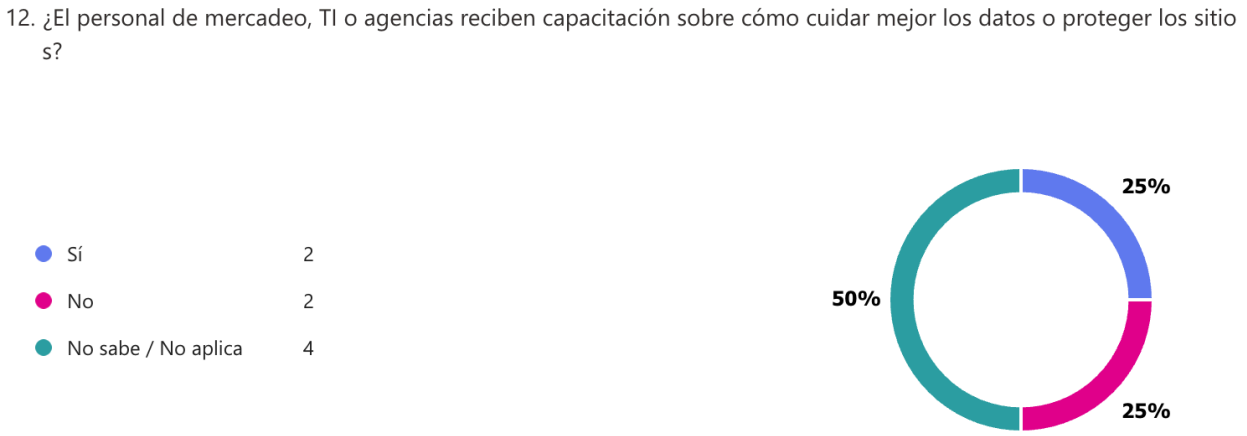


Fuente: *Vega, 2025.*

El 50 % de los encuestados indicó que sí se revisan y actualizan las medidas de seguridad con el tiempo, pero un 38 % dijo que no y un 12 % no sabe. Esto refleja que no hay un proceso continuo y claro de actualización en todos los casos.

Figura 12

Pregunta: Capacitación del personal ejecutor

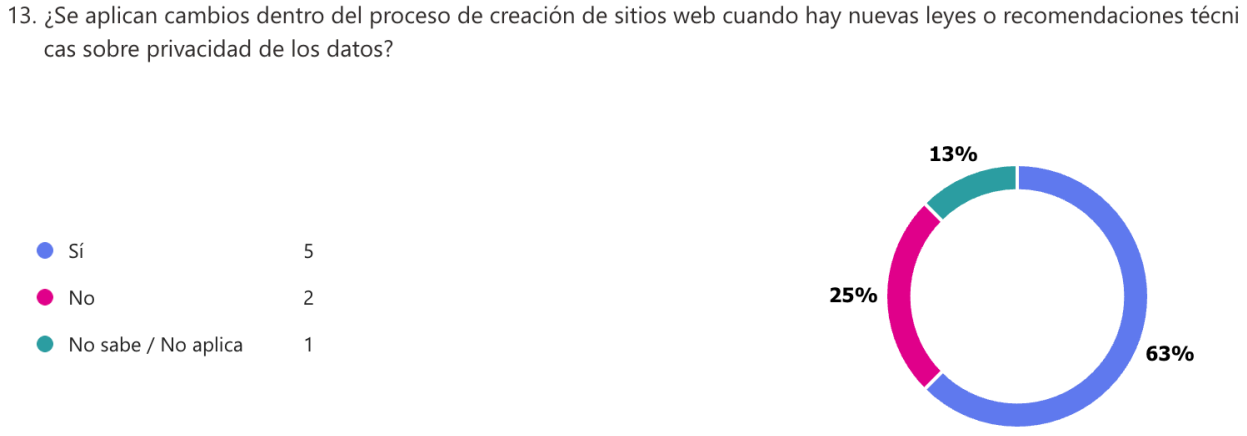


Fuente: *Vega, 2025.*

Respecto a la capacitación del personal en temas de protección de datos y seguridad, solo el 25 % confirmó recibirla. El 50 % respondió que no sabe y un 25 % que no, lo que evidencia una clara debilidad en la formación continua del equipo interno y externo.

Figura 13

Pregunta: Actualización de las normativas en los procesos.



Fuente: *Vega, 2025.*

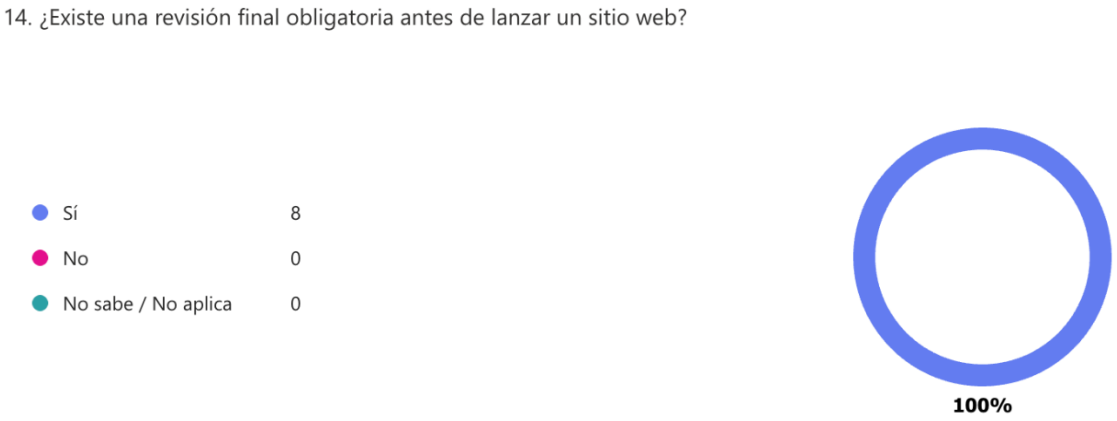
Finalmente, el 62 % afirmó que sí se aplican cambios cuando hay nuevas leyes o recomendaciones técnicas, pero un 25 % dijo que no y un 12 % no tiene conocimiento, lo que sugiere una implementación parcial y poco documentada de estos ajustes.

- **Hallazgos clave:**
- La actualización de medidas y procesos de seguridad no se realiza de forma periódica.
- La falta de capacitación es evidente, lo que limita la capacidad del equipo para aplicar buenas prácticas y entender la importancia de estas medidas de seguridad.

Bloque 5: Revisión final y seguimiento después del lanzamiento.

Se examinó si existen procesos formales para la revisión final antes del lanzamiento y si se realiza monitoreo posterior para detectar fallos.

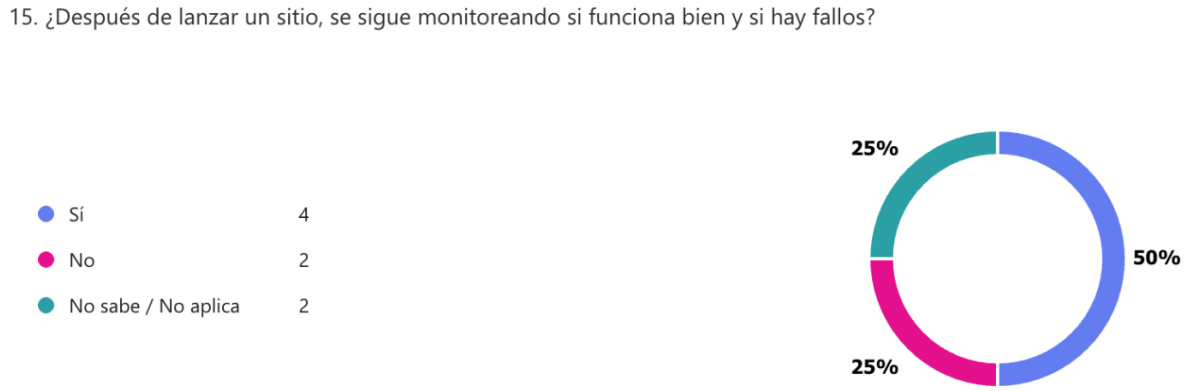
Figura 14
Pregunta: Revisión final de desarrollo



Fuente: *Vega, 2025.*

El 100 % de los encuestados indicó que sí existe una revisión final obligatoria antes de lanzar un sitio web, lo que refleja la presencia de un paso formal previo a la publicación.

Figura 15
Pregunta: Monitoreo de los desarrollos web



Fuente: *Vega, 2025.*

Sin embargo, solo el 50 % afirmó que sí se realiza monitoreo posterior al lanzamiento para verificar el funcionamiento del sitio o detectar errores, mientras que el 25 % respondió que no, y otro 25 % dijo no saber. Esto indica una falta de seguimiento estandarizado una vez que los desarrollos están en producción.

- **Hallazgos clave:**

- La revisión final previa al lanzamiento está plenamente implementada.
- El seguimiento posterior no está claramente definido ni aplicado por todos los actores, lo que puede limitar la detección oportuna de vulnerabilidades.

Los resultados del cuestionario evidencian que, si bien existen prácticas básicas de control como la revisión funcional previa al lanzamiento y la firma de aprobación, no hay una estandarización transversal ni visibilidad compartida sobre los procesos de seguridad aplicados a los desarrollos web. Elementos clave como la protección de datos personales, el uso efectivo de listas de verificación, la capacitación continua y el monitoreo posterior presentan inconsistencias entre los distintos colaboradores involucrados.

Esto demuestra que muchas decisiones se toman según el criterio de cada persona o con acuerdos informales entre el equipo y las agencias, sin que exista un procedimiento claro que garantice el cumplimiento de buenas prácticas en seguridad. Al no contar con reglas escritas y

conocidas por todos, se dificulta dar seguimiento correcto, asumir responsabilidades y mejorar continuamente la forma en que se gestionan los desarrollos web.

Entrevista

Con el fin de complementar los resultados obtenidos mediante el cuestionario y profundizar en aspectos técnicos relacionados con la seguridad de los desarrollos web, se realizó una entrevista semiestructurada a dos colaboradores del Departamento de Tecnologías de Información de la Cooperativa de Productores de Leche Dos Pinos.

La entrevista se desarrolló con base en una guía organizada en cuatro bloques temáticos: seguridad en los desarrollos web, controles de seguridad y normativas, validación y aprobación, y por último, monitoreo y mejora continua. Esta división permitió abordar de forma integral temas clave. Los insumos obtenidos a partir de estas entrevistas permitieron contrastar la percepción desde el área técnica con las prácticas declaradas por los equipos de mercadeo y los proveedores, reforzando así el diagnóstico general del proyecto.

Bloque 1: Seguridad en los desarrollos web.

Este bloque se centró en conocer cómo se gestiona actualmente la seguridad en los desarrollos digitales dentro del Departamento de Mercadeo de Dos Pinos y cuál es el rol del área de TI en ese proceso.

Ambos entrevistados coincidieron en que no existe un proceso establecido desde Mercadeo para validar la seguridad de los desarrollos web. Uno de ellos señaló:

"Para el departamento de Mercadeo no hay un proceso fijo para eso. Normalmente lo vemos con los encargados cuando logramos identificar una nueva solicitud de un desarrollo web y si algo nos genera duda, lo consultamos, para seguir brindando apoyo".

Desde el área de TI se indica que, si los desarrollos no pasan por sus manos, no pueden garantizar ningún tipo de validación de seguridad: *"Sí, hoy por hoy hay un procedimiento de análisis de vulnerabilidad, pero si esto no pasa por el área de TI, que ya nos ha pasado, muy difícilmente tengamos visibilidad para poder hacer esas verificaciones*".

También se remarcó que no hay una persona responsable de seguridad dentro de Mercadeo y que ese aspecto recae enteramente en TI, que a su vez enfrenta limitaciones de recursos:

"Desde Mercadeo como tal, no, temas de seguridad, eso ya le corresponde a TI, pero no hay alguien dentro del equipo que vea eso directamente".

- **Hallazgo clave:** Existe una desconexión entre las áreas Mercadeo y TI en cuanto a la validación de seguridad de los desarrollos web. La falta de un protocolo compartido y la escasa visibilidad generan riesgos para la organización al permitir la publicación de sitios sin control técnico formal.

Bloque 2: Controles de seguridad y normativas.

Este segmento se abordó el conocimiento y aplicación de normativas de seguridad, así como los controles actualmente implementados en los desarrollos web relacionados con el Departamento de Mercadeo.

Ambos entrevistados reconocieron que no existe un cumplimiento total de la norma ISO/IEC 27001 ni de la Ley Nº8968 en los procesos actuales. Uno de ellos comentó: *"Sé que algunos compañeros hablan de la ISO, que es un marco y que algunas cosas se trabajan en pro de esto, pero que cumplamos esta norma al 100 % no".*

En cuanto a la Ley Nº8968, otro colaborador expresó que la revisión técnica y el cumplimiento legal dependen de si el sitio llega a TI: *"Si el sitio o formulario no pasa por TI, no podemos garantizar que tenga controles o revisiones".*

También se mencionó que no hay una estructura formal que aplique estas normativas desde el diseño del desarrollo. La gestión de accesos o protección de datos se da solo en ciertos casos, y la participación de TI suele ser reactiva o a solicitud del área de Mercadeo.

- **Hallazgo clave:** El cumplimiento de normativas como la ISO 27001 y la Ley N°8968 no está estandarizado ni incorporado formalmente al proceso. La verificación depende de si los desarrollos llegan al área técnica, lo que genera vacíos importantes en seguridad y protección de datos.

. **Bloque 3: Controles de seguridad y normativas.**

Este bloque explora si existe algún procedimiento formal de aprobación técnica o de seguridad previo al lanzamiento de sitios web desarrollados por agencias externas.

Uno de los entrevistados indica sobre pruebas de seguridad: *"Sé que se han pruebas de código, pero en aplicativos, pero no en desarrollos web. Creo que no"*.

Cuando se les consulta si existe un procedimiento de aprobación final antes de publicar los desarrollos, la respuesta fue directa: *"No, actualmente no se realiza"*.

Otro entrevistado comentó que existen procedimientos dentro del área técnica de TI, pero no siempre se aplican porque algunos sitios se publican sin pasar por esta área: *"Sí, hoy por hoy hay un procedimiento de análisis de vulnerabilidad este sobre desarrollos y bueno sobre aplicaciones, infraestructura, ya se ejecuta, se valida y forma parte de lo que es una salida a producción de un nuevo sitio. Esto dentro de TI, pero si esto no pasa por el área de TI, que ya nos ha pasado, muy difícilmente tengamos visibilidad para poder hacer esas verificaciones. Tenemos un servicio de protección de marca, y muchas veces hemos visto sitios que nunca hemos aprobado o que no pasaron por nuestra dirección, y esto pasa generalmente ya después de su producción"*.

- **Hallazgo clave:** Aunque TI cuenta con procedimientos de validación, no hay un protocolo formal que obligue a que todos los desarrollos pasen por revisión antes de su publicación, y en la práctica sí se han lanzado sitios sin aprobación técnica previa.

. **Bloque 4: Monitoreo y mejora continua.**

Este bloque indaga sobre el seguimiento que se realiza a los desarrollos web después de su publicación, las capacitaciones brindadas al personal, oportunidades de mejora en la seguridad digital y el cumplimiento por parte de las agencias externas.

Cuando se consultó sobre las prácticas actuales de monitoreo, se respondió: *"Se hace a través de un escaneo que se hacen los compañeros, para verificar qué webs están a nombre de Dos Pinos, de momento, solo eso"*.

Respecto a la formación del personal en materia de seguridad web y normativas, el entrevistado afirmó: *"No, a Mercadeo no lo involucramos, esto lo dejamos solo al departamento de seguridad de TI"*.

En cuanto a posibles mejoras para fortalecer la seguridad en los desarrollos, se propuso: *"Que se aseguren que todo lo que hagan lo pasen por TI, porque muchas veces gestionan Desarrollos y no nos involucran, y esto hace que no tengamos visibilidad de nada".*

Finalmente, sobre la percepción del cumplimiento de las agencias externas: *"De momento bien, porque solo he tenido contacto con un solo proveedor".*

- **Hallazgo clave:** El monitoreo actual es limitado y reactivo. No se capacita al personal de Mercadeo y TI actúa de forma aislada. A pesar de contar con un proveedor, no existe una estrategia consolidada de seguimiento post lanzamiento ni control sobre el cumplimiento de estándares de seguridad.

Resumen de análisis

El análisis de los instrumentos aplicados permitió evidenciar de forma clara las debilidades importantes en los procesos actuales de validación y control de seguridad de los desarrollos web impulsados desde el Departamento de Mercadeo. Si bien existe una revisión funcional antes de lanzar los sitios, así como una aprobación desde el área responsable, no se cuenta con procedimientos formalizados ni estandarizados que aseguren el cumplimiento de buenas prácticas en seguridad de la información.

En el cuestionario se identificaron vacíos relacionados con la protección de datos, la entrega de listas de verificación a las agencias y la capacitación del personal. Además, el monitoreo posterior al lanzamiento no es una práctica consistente entre los distintos actores involucrados.

Por su parte, las entrevistas al personal técnico de TI confirmaron que, aunque existen procedimientos como análisis de vulnerabilidades y verificaciones técnicas, estos solo se aplican si los desarrollos son gestionados directamente por el área de TI. En los casos donde Mercadeo no involucra a esta área desde el inicio, se pierde visibilidad y control sobre lo que se publica, lo que impide realizar validaciones oportunas.

Tampoco existe una firma técnica o protocolo formal que documente la aprobación de seguridad antes del lanzamiento, ni procesos sistemáticos de formación sobre normativa vigente. Estos hallazgos refuerzan la necesidad de establecer un procedimiento estructurado, compartido y alineado con los controles definidos en la norma ISO/IEC 27001:2022 y los principios de la Ley Nº8968 sobre protección de datos personales.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

El presente capítulo expone las principales conclusiones derivadas del diagnóstico realizado al proceso de desarrollos webs subcontratados por el Departamento de Mercadeo, así como de la propuesta normativa planteada para mitigar los riesgos identificados en dicho entorno. Estas conclusiones responden directamente a los objetivos específicos formulados y reflejan tanto los hallazgos como los aportes técnicos del proyecto. Posteriormente, se presentan recomendaciones orientadas a facilitar la aplicación efectiva de las normativas propuestas y su sostenibilidad en el tiempo, considerando las condiciones operativas reales del entorno de la Cooperativa.

Conclusiones

El diagnóstico realizado evidenció la ausencia de lineamientos normativos y procedimientos técnicos que permitan al Departamento de Mercadeo gestionar de manera segura y estructurada los desarrollos web subcontratados. Esta carencia ha impedido que el Departamento cuente con un marco de control propio sobre los aspectos técnicos de seguridad, lo cual ha dejado en manos de los proveedores externos la aplicación de buenas prácticas esenciales para la protección de la información. Como resultado, se incrementa el riesgo de errores, filtraciones o incumplimientos legales en aspectos críticos como la validación del código fuente, el control de accesos, el tratamiento de datos personales y la obtención del consentimiento de los usuarios.

Como resultado del análisis realizado y del marco normativo aplicable, se logró estructurar un procedimiento técnico y documental que permite revisar, validar y controlar todos los desarrollos web subcontratados por el Departamento de Mercadeo. Este procedimiento fue diseñado con base en los principios y controles establecidos en la norma ISO/IEC 27001:2022 y en los artículos clave de la Ley Nº8968. La propuesta se compone de apartados operativos independientes, ajustados a las condiciones reales de las campañas digitales, con formatos y criterios aplicables sin requerir infraestructura adicional ni alterar la dinámica funcional del equipo de Mercadeo.

Integra de forma precisa los controles de seguridad establecidos en la norma ISO/IEC 27001:2022 y los principios legales definidos en la Ley Nº8968. Cada apartado responde directamente a las debilidades detectadas en el diagnóstico, como la falta de revisión estructurada

del código fuente, la ausencia de controles sobre los accesos administrativos a los sitios o formularios digitales, la falta de procedimientos de cifrado de datos y la inexistencia de mecanismos formales para el consentimiento informado. Esta integración normativa no solo fortalece la seguridad de los desarrollos web, sino que también contribuye a una gestión más transparente, documentada y coherente con los marcos regulatorios vigentes.

La propuesta fue diseñada considerando las condiciones operativas reales del Departamento de Mercadeo, caracterizadas por la subcontratación frecuente de desarrollos web, la alta rotación de campañas y la limitada duración de los sitios implementados. Bajo este contexto, se priorizó la definición de lineamientos claros, formatos reutilizables y procedimientos técnicamente viables, evitando requerimientos complejos como el monitoreo post-campaña o el uso de infraestructura adicional. Esta orientación garantiza la aplicabilidad efectiva de la normativa, manteniendo la agilidad operativa y fortaleciendo al mismo tiempo el control institucional sobre los desarrollos digitales.

La implementación de esta propuesta permitiría al Departamento de Mercadeo contar con un mayor control sobre los desarrollos web subcontratados, reduciendo riesgos técnicos, legales y reputacionales asociados al manejo de información personal en campañas digitales. Asimismo, contribuiría a fortalecer la trazabilidad, la documentación técnica y la responsabilidad compartida con los proveedores externos. Esta propuesta representa una mejora sustancial en la gestión de la seguridad sin requerir grandes inversiones ni alterar el flujo operativo actual, promoviendo una cultura de seguridad aplicable y coherente con la operación.

Recomendaciones

Se recomienda aplicar de forma integral la propuesta desarrollada como un estándar mínimo para la gestión de seguridad en los desarrollos web subcontratados por el Departamento de Mercadeo. Cada apartado debe ser implementado según su naturaleza operativa, asegurando que las agencias proveedoras, el equipo de Mercadeo y el personal técnico de la Cooperativa comprendan su contenido, apliquen los procedimientos correspondientes y conserven la documentación como parte del expediente de cada campaña digital.

Al Departamento de Mercadeo le corresponde integrar formalmente los procedimientos propuestos en el flujo operativo de gestión de las campañas digitales. Para ello, se recomienda:

- Aplicar cada procedimiento desde la etapa de planificación del proyecto, por parte del ejecutivo responsable del desarrollo. Esta incorporación permite velar por las buenas prácticas de seguridad.
- Incluir en el brief inicial la solicitud del cumplimiento de los lineamientos normativos establecidos en los apartados ***PR-VCS-001, DR-EADS-001, NTV-STDP-001, NTV-CDS-001 y PTC-AVF-001***. Esta solicitud debe ser verificada al cierre del proyecto, asegurando la integración de las medidas de seguridad de principio a fin.
- Integrar el checklist de verificación (***NTV-CDS-001***) y el formulario de incidentes (***NTV-GISMA-001***) como parte del expediente técnico de cada campaña. Ambos deben ser completados por la agencia y archivados por Mercadeo antes del lanzamiento del desarrollo, con el fin de garantizar trazabilidad y cumplimiento normativo.
- Asignar un ejecutivo responsable por proyecto, desde el inicio de la campaña, con la función de supervisar la correcta ejecución de cada uno de los procedimientos, coordinar con TI en caso necesario y consolidar toda la documentación de seguridad. Esta figura asegura continuidad, control y responsabilidad institucional.

Al Departamento de TI le corresponde brindar acompañamiento al Departamento de Mercadeo durante todo el proceso de desarrollo. Para ello, se recomienda:

- Revisar técnicamente el código fuente, la configuración de accesos y el cifrado de datos en tránsito y en reposo, según lo establecido en el procedimiento ***PR-VCS-001***. Esta revisión debe realizarse antes de la aprobación final del desarrollo, garantizando que los entregables cumplan con los criterios técnicos definidos.
- Colaborar en la ejecución e interpretación de las pruebas dinámicas de seguridad contempladas en el apartado ***DR-EADS-001***. Esta participación debe darse durante la etapa de validación técnica, con el fin de asegurar que cualquier vulnerabilidad detectada sea corregida antes del despliegue del desarrollo.
- Verificar que el desarrollo cumpla con los criterios establecidos en el protocolo de aprobación final (***PTC-AVF-001)*** antes de autorizar su publicación. Esta revisión técnica debe realizarse en conjunto con el equipo de Mercadeo para asegurar una validación cruzada.

- Atender los incidentes de seguridad reportados por agencias o Mercadeo, conforme a lo establecido en la normativa ***NTV-GISMA-001***. Esto implica validar técnicamente el incidente, aplicar las medidas de contención necesarias, conservar la evidencia técnica y cerrar formalmente el expediente en coordinación con el equipo de Mercadeo. Esta atención debe realizarse de forma inmediata tras la notificación, para minimizar el impacto del incidente.
- Aprobar previamente las herramientas de escaneo técnico de seguridad utilizadas por los proveedores, aunque no se indique una herramienta específica en la normativa. Esta aprobación debe realizarse al momento de iniciar cada proyecto, garantizando que las soluciones elegidas sean confiables, compatibles y alineadas con los criterios del Departamento de TI.
- Brindar sesiones de capacitación técnica específicas al equipo de Mercadeo, cuando sea requerido, para facilitar la comprensión y correcta aplicación de los lineamientos normativos, especialmente en el uso de plantillas, formularios y criterios técnicos. Estas sesiones pueden organizarse una vez al año o cuando se identifiquen brechas de conocimiento.

A las agencias externas se les recomienda cumplir con los requisitos establecidos en cada uno de los apartados normativos como parte integral de la contratación para el desarrollo. Para ello, se sugiere lo siguiente:

- Aplicar controles técnicos desde el inicio del proyecto, especialmente en relación con el código fuente, los accesos administrativos y el cifrado de datos en tránsito y en reposo (***PR-VCS-001***). Estas acciones deben realizarse durante la etapa de desarrollo y ser verificables mediante evidencia técnica al momento de la entrega. Su cumplimiento previene vulnerabilidades que podrían comprometer la seguridad de los usuarios y de la organización.
- Ejecutar las pruebas dinámicas de seguridad conforme a los lineamientos establecidos en la directriz ***DR-EADS-001***, utilizando herramientas previamente aprobadas por el Departamento de TI. Estas pruebas deben ser realizadas antes de la entrega final del proyecto y sus resultados deberán integrarse en el expediente técnico correspondiente, como respaldo de calidad y seguridad.

- Completar el checklist de verificación de seguridad (***NTV-CDS-001***) y remitirlo junto con los entregables del desarrollo web. Este documento debe ser gestionado al cierre del desarrollo y permite asegurar que se ha cumplido con todos los criterios definidos por la Cooperativa.
- Gestionar el consentimiento informado de los usuarios mediante los formularios o sitios web desarrollados, conforme a los requisitos establecidos en la normativa ***NTV-STDP-001***. La evidencia del consentimiento debe ser recolectada y presentada al finalizar el desarrollo, con el fin de asegurar la legalidad del tratamiento de datos personales.
- Notificar de inmediato cualquier incidente de seguridad detectado, completando el formulario técnico de ***NTV-GISMA-001*** y colaborando en el proceso de análisis y mitigación. Esta notificación debe hacerse en cuanto se detecte el incidente, garantizando una respuesta oportuna y minimizando el impacto de la afectación.
- Cumplir con todas las etapas definidas en el protocolo de aprobación y validación final (***PTC-AVF-001***) antes de considerar un proyecto como finalizado. Esto incluye la entrega documental, revisión funcional y validación técnica. Su cumplimiento asegura que el desarrollo cumpla con los criterios de calidad, trazabilidad y seguridad requeridos por la Cooperativa.

Para asegurar la sostenibilidad, actualización y efectividad de la propuesta normativa en el tiempo, se recomienda establecer un proceso de mejora continua liderado por el Departamento de Mercadeo, con apoyo del Departamento de TI. Este proceso debe contemplar:

- Revisar periódicamente el contenido de cada apartado normativo, tomando como insumo los incidentes registrados, retroalimentación de las agencias, nuevas necesidades operativas y cambios en la normativa vigente. Esta revisión puede ser realizada cada seis meses por el equipo de Mercadeo con acompañamiento de TI, con el fin de mantener la vigencia técnica y legal de los procedimientos aplicados.
- Actualizar los formatos, formularios y checklists utilizados, en especial aquellos definidos en los apartados ***PR-VCS-001, NTV-CDS-001, NTV-GISMA-001 y PTC-AVF-001***. Esta actualización debe hacerse anualmente, o cuando se detecten cambios importantes en las plataformas tecnológicas utilizadas por las agencias o por la Cooperativa.
- Aplicar la política ***PL-CNAE-001*** como base institucional para el seguimiento de estándares de seguridad y normativas aplicables, permitiendo consolidar una cultura de

cumplimiento alineada con marcos nacionales e internacionales. Esta política debe revisarse una vez al año, y su aplicación debe ser gestionada por Mercadeo, validada por del departamento de TI.

- Promover espacios de revisión conjunta entre Mercadeo, TI y proveedores externos, al cierre de cada proyecto o campaña relevante, para discutir buenas prácticas, lecciones aprendidas y oportunidades de mejora. Esta práctica favorece la evolución gradual de los controles sin comprometer la agilidad operativa del área.

CAPÍTULO VI: LA PROPUESTA

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

PROPUESTA DE UN PROCEDIMIENTO DE REVISIÓN Y CONTROL DE SEGURIDAD DE LOS DESARROLLOS WEB DEL DEPARTAMENTO DE MERCADEO, BASADO EN LA NORMATIVA ISO 27001 Y LA LEY DE PROTECCIÓN DE DATOS Nº8968 PARA LA COOPERATIVA DE PRODUCTORES DE LECHE DOS PINOS, EN ALAJUELA.

JOHAN VEGA CÓRDOBA

SAN JOSÉ, JULIO, 2025

Introducción

En la actualidad, los desarrollos web se han convertido en un recurso esencial dentro de las estrategias digitales de las organizaciones, especialmente a partir de la aceleración en los procesos de digitalización posterior a la pandemia. Su uso ha cobrado especial relevancia en entornos de mercadeo, donde cumplen un rol central en la recopilación de datos, la segmentación de audiencias y la ejecución de campañas personalizadas para el consumidor final. Sin embargo, la rapidez con la que se implementan estos desarrollos, junto con la presión por reducir tiempos de entrega, puede comprometer la calidad técnica y la seguridad de la información si no existen lineamientos normativos claros que orienten su correcta construcción, validación y puesta en marcha.

En respuesta a los crecientes desafíos en materia de ciberseguridad y cumplimiento normativo, han surgido marcos internacionales como la norma ISO/IEC 27001:2022 y leyes nacionales como la Ley Nº8968, los cuales ofrecen principios y controles que permiten robustecer la seguridad en los desarrollos tecnológicos. Si bien su implementación integral suele asociarse a entornos con sistemas de gestión formalizados, esta propuesta busca adaptar dichos lineamientos a un entorno operativo ágil, como el del Departamento de Mercadeo, brindando una base normativa aplicable.

En el caso de la Cooperativa de Productores de Leche Dos Pinos, y en particular del Departamento de Mercadeo, los desarrollos web se caracterizan por ser ejecutados por agencias de publicidad o proveedores externos, en contextos de alta rotación y bajo esquemas de duración limitada, como ocurre en la mayoría de las campañas digitales. Esta dinámica operativa, aunque eficiente desde el punto de vista de ejecución de Mercadeo, ha evidenciado una ausencia de lineamientos técnicos y normativos que permitan asegurar la calidad y seguridad de los productos entregados.

La presente propuesta normativa busca dar respuesta a esa necesidad mediante la definición de procedimientos, normativas y procesos prácticos que puedan ser implementados directamente desde el área de Mercadeo, en coordinación con el Departamento de Tecnologías de la Información, sin requerir inversiones adicionales ni una infraestructura compleja. Su diseño se apoya en los principios de la norma ISO/IEC 27001:2022 y en los artículos clave de la Ley Nº8968, y se adapta a la naturaleza temporal y subcontratada de los desarrollos digitales ejecutados para las campañas institucionales.

Esta propuesta no pretende sustituir procesos existentes, sino complementarlos mediante la incorporación de criterios de control y validación, de forma que la gestión de proyectos web se fortalezca con herramientas normativas claras, alineadas con prácticas ampliamente adoptadas por otras organizaciones. Su implementación permitirá al Departamento de Mercadeo contar con mayor trazabilidad, mejores controles y una base normativa defendible ante cualquier revisión técnica o legal.

En la sección siguiente se detallan el objetivo, el alcance de la propuesta y una descripción breve de cada normativa incluida. Posteriormente, se presenta el desarrollo completo y estructurado de cada uno de los siete apartados normativos que componen esta propuesta.

Objetivos

Objetivo General:

Proponer un proceso de revisión y control de seguridad de los desarrollos web del Departamento de Mercadeo de la Cooperativa de Productores de Leche Dos Pinos, que impacte la confidencialidad, integridad, y disponibilidad de los datos personales procesados por estos medios en conformidad con lo que establece la normativa internacional ISO 27001, y la Ley Nº8968.

Objetivos específicos:

- Elaborar un proceso estándar para la validación del código fuente, el control de accesos y el cifrado de datos, asegurando la protección de los desarrollos web.
- Desarrollar directrices para las evaluaciones de seguridad, estableciendo pruebas y criterios específicos que sea obligatorios para las agencias externas en la detección y mitigación de vulnerabilidades.
- Formular una normativa que incluya una lista de verificación de seguridad obligatoria, estandarizando el proceso de comprobación de los desarrollos webs.
- Crear políticas para la actualización periódica de los estándares de seguridad, integrando los cambios normativos y mejores prácticas de la industria.

- Crear un protocolo de aprobación final que establezca los procedimientos para la verificación de los controles de seguridad y la validación de los desarrollos web antes de su lanzamiento.

Alcance de la propuesta

La presente propuesta aplica para todos los desarrollos web subcontratados por el Departamento de Mercadeo de la Cooperativa de Productores de Leche Dos Pinos, incluyendo landing pages, micrositios y formularios digitales vinculados a campañas publicitarias. Su aplicación es obligatoria en los proyectos que involucren el manejo de datos personales, la recopilación de información de usuarios o la publicación de plataformas digitales accesibles al público externo.

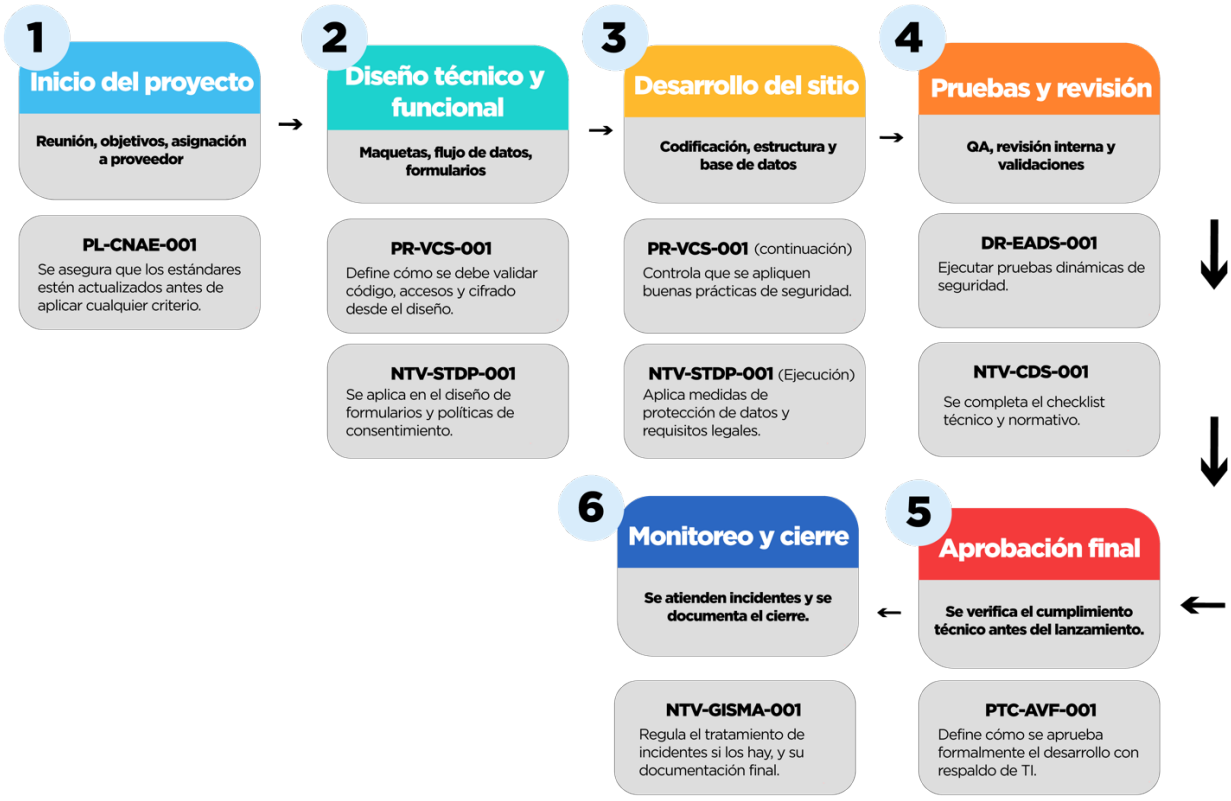
Las normativas propuestas deben ser consideradas desde el momento de la planificación del proyecto, continuando durante su desarrollo técnico, revisión funcional, aprobación final y eventual cierre. Cada apartado normativo establece lineamientos específicos que deberán ser implementados por las agencias proveedoras, supervisados por el Departamento de Mercadeo y validados, cuando corresponda, por el personal técnico del Departamento de Tecnologías de la Información.

Este conjunto normativo no sustituye los controles existentes dentro de la infraestructura interna de TI, ni implica la adopción de un sistema de gestión integral de seguridad de la información (SGSI), sino que actúa como un refuerzo operativo para garantizar la trazabilidad, seguridad y cumplimiento en desarrollos temporales y subcontratados. Su alcance está limitado al ciclo de vida activo de los proyectos web asociados a campañas, sin requerir monitoreo continuo una vez concluida su vigencia.

La siguiente imagen resume gráficamente cómo se integra cada una de las normativas propuestas dentro del ciclo operativo de los desarrollos web subcontratados por el Departamento de Mercadeo. Este flujo ilustra en qué momento específico se aplica cada apartado, permitiendo una cobertura completa desde la planificación inicial hasta el cierre técnico del proyecto.

Figura 16

Flujo normativo por etapa en el desarrollo o proyecto digital



Fuente: *Vega, 2025.*

Estos son cada uno de los apartados que integran la propuesta y que a continuación describiremos cuál es su función dentro de cada etapa del ciclo de desarrollo:

- PL-CNAE-001 – Política de cumplimiento normativo y actualización de estándares.
- PR-VCS-001 – Proceso de validación de la calidad y seguridad de los desarrollos web
- NTV-STDP-001 – Normativa sobre tratamiento de datos personales y consentimiento.
- DR-EADS-001 – Directriz de evaluación y análisis de seguridad.
- NTV-CDS-001 – Normativa de verificación mediante checklist de seguridad.
- PTC-AVF-001 – Protocolo de aprobación y validación final de los desarrollos web.
- NTV-GISMA-001 – Normativa de gestión de incidentes de seguridad y monitoreo de actividades.

Política de cumplimiento normativo y actualización de estándares

Este apartado establece una política que define los criterios para asegurar el cumplimiento de las normativas vigentes en materia de seguridad de la información y protección de datos personales, así como para mantener actualizados los estándares técnicos aplicables a los desarrollos web subcontratados. Su función es actuar como marco de referencia inicial para todo el ciclo del proyecto, garantizando que las directrices utilizadas estén alineadas con los marcos regulatorios nacionales e internacionales más recientes.

Su aplicación inicia en la etapa de planificación del desarrollo, antes de definir requerimientos funcionales o técnicos. Desde este punto, la política orienta la adopción de criterios, formatos y controles basados en los principios establecidos en la norma ISO/IEC 27001:2022 y en la Ley Nº8968, promoviendo una cultura de cumplimiento desde el inicio del proyecto.

Además de fijar una base normativa clara, este apartado define un mecanismo de actualización continua, mediante el cual las directrices técnicas podrán ser revisadas periódicamente por el Departamento de Tecnologías de la Información, en conjunto con el Departamento de Mercadeo. Esta revisión podrá responder a lecciones aprendidas, incidentes de seguridad previos, cambios en el marco legal o mejoras operativas identificadas durante la ejecución de otras campañas digitales.

El propósito de esta política es evitar que los desarrollos web se ejecuten con criterios obsoletos o desalineados con los requisitos legales actuales. Asimismo, permite asegurar que las normativas definidas en esta propuesta permanezcan vigentes y funcionales a lo largo del tiempo, sin necesidad de reiniciar el proceso de validación ante cada nuevo desarrollo.

Proceso de validación de la calidad y seguridad de los desarrollos web

Este apartado establece un procedimiento normativo para asegurar la calidad técnica y la protección de la información en los desarrollos web. Su alcance comprende la validación del código fuente, la gestión de accesos administrativos y el cifrado de los datos tanto en tránsito como

en reposo. Se trata de un proceso transversal que inicia en la fase de diseño y se mantiene activo durante todo el desarrollo técnico, hasta su revisión final.

El objetivo principal es garantizar que las agencias externas o proveedores apliquen las mejores prácticas de seguridad desde la construcción inicial del sitio, evitando errores comunes como configuraciones inseguras, credenciales expuestas o falta de protección de la información sensible. La normativa contempla también la exigencia de utilizar HTTPS con certificado SSL/TLS, así como mecanismos de revisión estructurada del código, que pueden realizarse de forma manual o asistida, siempre con aprobación del Departamento de TI.

Dentro de este proceso se incluyen requisitos específicos que deben cumplir las agencias proveedoras, tales como la documentación del repositorio de código, la implementación de controles de acceso diferenciados por rol y el uso de técnicas de cifrado adecuadas. Además, se prohíbe el uso de datos reales en ambientes de prueba sin autorización previa, y se establecen técnicas obligatorias de enmascaramiento u ofuscación de datos cuando sea necesario.

El cumplimiento de este proceso debe ser verificado por el Departamento de Tecnologías de la Información, como parte del control de calidad previo a la publicación del desarrollo. Los hallazgos y revisiones técnicas deben formar parte del expediente documental del proyecto, reforzando la trazabilidad del proceso y el cumplimiento normativo en materia de seguridad de la información.

Normativa sobre tratamiento de datos personales y consentimiento de usuarios

Con el fin de garantizar el correcto cumplimiento legal en el manejo de datos personales, este apartado define los lineamientos específicos que deben ser aplicados en los desarrollos web que recopilen, almacenen o procesen información de carácter personal. La normativa se fundamenta en los principios establecidos por la Ley Nº8968 y busca asegurar que todas las acciones relacionadas con el tratamiento de datos se realicen de manera informada, segura y conforme a los derechos que tienen cada uno de los usuarios.

La aplicación de estos lineamientos inicia desde la etapa de planificación del proyecto, en la cual se debe determinar si el sitio o formulario recolectará datos personales. A partir de ese momento, se exige que el diseño incorpore mecanismos de consentimiento informado, políticas

claras de privacidad, criterios de proporcionalidad en la solicitud de información, y el uso adecuado de cookies.

En entornos de prueba o desarrollo, queda estrictamente prohibido el uso de datos reales sin autorización previa del Departamento Legal y del Departamento de Tecnologías de la Información. En caso de requerirse, el proveedor deberá aplicar técnicas de enmascaramiento u ofuscación de datos personales. Dicho proceso debe documentarse mediante un informe técnico que incluya el método utilizado, fecha de ejecución, responsable, y evidencia visual que respalde su correcta implementación.

Se establece también la obligatoriedad del uso de HTTPS con certificado SSL/TLS como medio seguro para la transmisión de información sensible. Además, se exige la realización de un escaneo técnico de seguridad previo al lanzamiento de la plataforma, con herramientas que, aunque no son impuestas por esta normativa, deben contar con la aprobación previa del Departamento de TI.

Finalmente, se contempla un procedimiento para la atención de solicitudes relacionadas con los datos personales recolectados. Los desarrollos deben habilitar canales claros para que los usuarios puedan ejercer sus derechos, como acceder, rectificar o eliminar su información, y garantizar que dichas solicitudes sean gestionadas de manera oportuna y documentada.

Esta normativa le permite al Departamento de Mercadeo cumplir con los principios de legalidad, finalidad, proporcionalidad, veracidad, confidencialidad y seguridad en el tratamiento de datos personales, fortaleciendo así la protección del usuario final y la integridad institucional de la Cooperativa.

Directriz de evaluación y análisis de seguridad

Esta directriz establece los lineamientos para realizar pruebas dinámicas de seguridad en los desarrollos web del Departamento de Mercadeo. Su propósito es identificar vulnerabilidades técnicas que podrían comprometer la integridad, disponibilidad o confidencialidad de la información gestionada por los sitios o formularios implementados, antes de su publicación.

La aplicación de esta normativa debe realizarse una vez que el desarrollo ha alcanzado un nivel funcional operativo, preferiblemente en un ambiente de pruebas. Las evaluaciones se centran en detectar fallas como inyecciones de código, errores de validación de entradas, configuraciones

inseguras o exposición de datos sensibles. Como referencia técnica, se adopta el estándar internacional OWASP Top Ten como base para definir las áreas prioritarias de revisión.

El proveedor podrá utilizar herramientas automatizadas, técnicas manuales u otras metodologías equivalentes, siempre que los resultados se documenten formalmente. El informe técnico debe incluir el nombre de la herramienta utilizada, fecha de ejecución, hallazgos identificados, acciones correctivas aplicadas y evidencia técnica del proceso. Aunque la herramienta no se impone desde esta propuesta, su uso deberá ser previamente validado por el Departamento de Tecnologías de la Información para asegurar su idoneidad.

El Departamento de TI podrá brindar acompañamiento técnico en la interpretación de los hallazgos, así como en la verificación de la eficacia de las medidas correctivas implementadas. La responsabilidad de ejecutar las pruebas recae sobre la agencia desarrolladora, mientras que el resguardo del informe técnico corresponde al equipo de Mercadeo como parte del expediente normativo del proyecto.

Esta directriz busca reforzar el principio de prevención en la seguridad de la información, asegurando que los errores o vulnerabilidades técnicas sean identificados y corregidos antes de que el sitio entre en producción, disminuyendo con ello altos riesgos operativos, legales y reputacionales para la Cooperativa.

Normativa de verificación mediante checklist de seguridad

Esta normativa establece una lista de verificación estructurada que debe ser completada antes de la aprobación funcional de cualquier desarrollo web subcontratado. Su función es estandarizar la validación de los requisitos técnicos, normativos y de seguridad aplicables, facilitando la trazabilidad y el cumplimiento documental en los proyectos digitales del Departamento de Mercadeo.

La lista de verificación debe ser utilizada una vez concluido el desarrollo funcional y técnico del sitio, antes de su publicación. En ella se consolidan los principales controles definidos en los apartados anteriores, como la revisión del código fuente, la implementación de HTTPS, la gestión de consentimientos, el resultado de las pruebas de seguridad dinámica, y la existencia de mecanismos adecuados para la atención de solicitudes de los usuarios, entre otros.

Este checklist debe ser completado por la agencia proveedora, validado por el equipo de Mercadeo y, en los casos aplicables, revisado por el Departamento de TI. Se trata de un documento obligatorio para considerar un desarrollo como técnicamente cerrado, y debe archivarse como parte del expediente normativo de cada campaña.

El formato propuesto busca facilitar su uso mediante un diseño claro, con campos para marcar cumplimiento, observaciones, evidencias técnicas y responsables. Además, se prevé que el checklist pueda ser actualizado conforme evolucionen los estándares de seguridad o se incorporen nuevas exigencias legales, tal como lo contempla la política de actualización de estándares (***PL-CNAE-001***).

Con esta normativa se formaliza un mecanismo de control objetivo y reutilizable que evita la subjetividad en la evaluación técnica de los desarrollos, promueve la documentación institucional y fortalece la rendición de cuentas ante cualquier eventualidad relacionada con la seguridad o el tratamiento de datos.

Protocolo de aprobación y validación final de los desarrollos web

Este apartado define el procedimiento obligatorio para validar técnica y documentalmente cualquier desarrollo web antes de su lanzamiento. Su propósito es asegurar que los sitios o formularios digitales utilizados en campañas del Departamento de Mercadeo cumplan con todos los requisitos de seguridad, calidad y cumplimiento normativo establecidos en la presente propuesta.

La aplicación de este protocolo se activa una vez que el desarrollo ha sido concluido por parte de la agencia proveedora y ha superado las etapas de validación técnica y revisión mediante checklist. El proceso contempla cuatro etapas: entrega técnica por parte del proveedor, revisión funcional por parte del equipo de Mercadeo, validación técnica por parte del Departamento de TI (cuando corresponda) y comunicación formal de aprobación.

El protocolo exige que toda la documentación asociada incluyendo checklist, resultados de pruebas, formularios de consentimiento y reportes técnicos, se encuentre debidamente archivados como parte del expediente del proyecto. Asimismo, establece que ningún sitio puede ser publicado sin la aprobación expresa del equipo de Mercadeo y, en su caso, del Departamento de TI, conforme a las responsabilidades descritas.

Este apartado garantiza que la publicación de los desarrollos no dependa únicamente de criterios operativos o urgencias de campaña, sino que pase por un proceso de cierre técnico normativo que fortalezca la seguridad. Además, promueve la trazabilidad de las decisiones tomadas, la conservación de evidencias técnicas y la responsabilidad compartida entre proveedores, Mercadeo y TI.

El cumplimiento de este protocolo representa la fase final del ciclo de desarrollo web subcontratado y marca el punto de partida para la ejecución operativa de la campaña, bajo condiciones controladas y documentadas.

Normativa de gestión de incidentes de seguridad y monitoreo de actividades

Esta normativa establece el procedimiento para la gestión de incidentes de seguridad en los desarrollos web contratados por el Departamento de Mercadeo, así como los mecanismos mínimos de monitoreo que deben aplicarse durante el ciclo de vida activo de las campañas digitales. Su objetivo es garantizar una respuesta oportuna ante eventos que puedan afectar la información manejada por los sitios implementados.

El procedimiento se activa cuando se detecta o reporta una anomalía que comprometa el funcionamiento del sitio, la protección de datos personales o el cumplimiento normativo. La normativa contempla las siguientes fases: detección y registro del incidente, notificación y comunicación interna, evaluación y contención, recuperación y cierre del incidente, por último, la actualización y mejora de criterios de seguridad.

Para facilitar la aplicación de esta normativa, se incluye un formato estandarizado de reporte de incidentes, que debe ser utilizado por las agencias proveedoras y el equipo de Mercadeo ante cualquier evento relevante. Este reporte debe incluir una descripción detallada del incidente, fecha, responsable, acciones tomadas, medidas correctivas aplicadas y evidencia técnica correspondiente.

El Departamento de TI será el encargado de brindar soporte técnico en la investigación y contención del incidente, así como de validar las acciones correctivas aplicadas. El informe final debe ser archivado como parte del expediente del proyecto y revisado en sesiones posteriores de evaluación, para retroalimentar los procesos normativos internos y promover mejoras operativas.

En cuanto al monitoreo, la normativa establece que, debido al carácter temporal de los sitios implementados para campañas digitales, no se requiere monitoreo continuo. Sin embargo, durante el periodo de vigencia activa del sitio, se deberán aplicar mecanismos mínimos de supervisión sobre el comportamiento técnico, accesos y funcionamiento general.

Con este apartado, se refuerza la capacidad institucional de reacción ante incidentes, se formaliza el canal de reporte y documentación, y se promueve una cultura de mejora continua.

Proceso de implementación de la propuesta

La propuesta normativa ha sido diseñada para su implementación en tres etapas, según la complejidad operativa y el impacto esperado:

- **Corto plazo (0 a 5 meses):** Aplicación inicial de las normativas operativas más urgentes y de menor complejidad técnica, como el checklist de verificación de seguridad (NTV-CDS-001), el formulario de reporte de incidentes (NTV-GISMA-001) y el protocolo de aprobación final (PTC-AVF-001). Estas pueden integrarse de forma inmediata al flujo operativo del Departamento de Mercadeo mediante briefs, entregables y capacitaciones internas.
- **Mediano plazo (6 a 8 meses):** Incorporación de procedimientos que requieren coordinación técnica con el Departamento de TI, tales como la validación del código fuente, los accesos y el cifrado de datos (PR-VCS-001), y la ejecución de pruebas dinámicas de seguridad (DR-EADS-001). Esta fase contempla también la consolidación documental de evidencias y el establecimiento de responsabilidades por proyecto.
- **Largo plazo (9 a 12 meses):** Establecimiento de la política de actualización de estándares (PL-CNAE-001) como mecanismo formal de mejora continua, así como el fortalecimiento institucional del enfoque de seguridad en el tratamiento de datos personales (NTV-STDP-001). Esta etapa dependerá del proceso de maduración de las capacidades internas y de la articulación estratégica con otras áreas de la Cooperativa.

Detalles complementarios para la implementación:

Si bien la propuesta ha priorizado una redacción clara y operativa sin necesidad de glosarios o matrices aisladas, se integran los siguientes recursos como complemento:

- **Matriz de responsabilidades integrada por normativa:** Cada normativa establece claramente los responsables de su aplicación (Mercadeo, TI, agencias), asignando funciones específicas según el tipo de acción (revisión, validación, ejecución, archivo). Esta información se encuentra detallada dentro de cada apartado, evitando duplicidad.
- **Flujo normativo visual:** Para facilitar la comprensión del proceso integral, se incluyó un diagrama (*Flujo normativo por etapa en el desarrollo o proyecto digital*) en la sección de propuesta que ilustra cómo cada apartado se inserta dentro del flujo operativo de desarrollo web subcontratado. Esta herramienta visual cumple la función de flujograma y permite al lector ubicar de forma rápida la secuencia operativa por etapa.
- **Términos técnicos y referencias:** Todos los términos utilizados en la propuesta están alineados con los controles de la norma ISO/IEC 27001:2022 y la Ley N.º 8968. Al no incluir un SGSI formal ni generar un documento jurídico, se optó por explicar directamente los conceptos en el cuerpo del texto, especialmente en los apartados que abordan cifrado, consentimiento, incidentes o pruebas técnicas.

Mecanismos de cumplimiento y seguimiento con proveedores:

Actualmente, la Cooperativa no contempla la modificación de los contratos marco con las agencias para establecer sanciones económicas o cláusulas explícitas por incumplimientos en los desarrollos web. Sin embargo, la entrada en vigencia de esta propuesta normativa habilita un mecanismo operativo que permite incluir el cumplimiento de los lineamientos técnicos y documentales como parte de los criterios de evaluación institucional.

Dos Pinos cuenta con un sistema de evaluación trimestral de agencias proveedoras, en el cual se califican diversos aspectos del servicio prestado, incluyendo la calidad técnica, la gestión de proyectos y el cumplimiento de requerimientos establecidos por el Departamento de Mercadeo. A partir de la implementación de esta propuesta, el cumplimiento de las normativas de seguridad y calidad (como la entrega del checklist, el consentimiento informado o la evidencia del cifrado) podrá formar parte de los rubros a calificar, sin necesidad de renegociar contratos.

Cuando una agencia omite reiteradamente estas entregas, o incumple los lineamientos definidos en esta propuesta, su calificación institucional puede verse afectada. Esto puede derivar en observaciones formales y, en casos graves, en la pérdida de elegibilidad como proveedor activo de la Cooperativa. Este enfoque permite aplicar consecuencias prácticas sin necesidad de implementar sanciones contractuales, fortaleciendo al mismo tiempo el control sobre los desarrollos subcontratados.

Integración con procedimientos existentes del Departamento de TI:

Esta propuesta no busca sustituir ni duplicar los procedimientos existentes definidos por el Departamento de Tecnologías de la Información (TI), sino complementarlos desde el contexto operativo del Departamento de Mercadeo. En Dos Pinos, el Departamento de TI mantiene protocolos institucionales para proyectos de alto alcance, desarrollos internos o soluciones integradas dentro del ecosistema tecnológico de la Cooperativa. Sin embargo, los desarrollos subcontratados por Mercadeo, como landing pages, micrositios o formularios para campañas digitales, suelen tener una naturaleza distinta: son temporales, gestionados por agencias externas y no siempre forman parte del portafolio técnico centralizado de TI.

Por ello, esta propuesta se desarrolla como una herramienta de enlace entre ambos departamentos, permitiendo que Mercadeo pueda asumir un rol más activo en la gestión técnica y documental de estos desarrollos sin depender exclusivamente del acompañamiento continuo de TI. Cada normativa incluida fue diseñada para que sus entregables puedan ser fácilmente revisados, validados y archivados por TI en los puntos críticos del proceso, como el momento de la aprobación final o la atención de un incidente.

Además, se recomienda que las normativas propuestas, especialmente aquellas relacionadas con seguridad (PR-VCS-001), consentimiento (NTV-STDP-001) e incidentes (NTV-GISMA-001), sean compartidas formalmente con el Departamento de TI, de forma que puedan ser consideradas en futuras actualizaciones de los procedimientos técnicos institucionales, promoviendo una mayor armonía operativa entre áreas.

APÉNDICE A

Política de cumplimiento normativo y actualización de estándares

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

POLÍTICA DE CUMPLIMIENTO NORMATIVO Y ACTUALIZACIÓN DE ESTÁNDARES

JOHAN VEGA CÓRDOBA

JUNIO, 2025

INTRODUCCIÓN

La subcontratación de desarrollos web por parte del Departamento de Mercadeo implica la creación de plataformas que, en muchos casos, gestionan información personal proporcionada por usuarios. Aunque estos proyectos cumplen funciones estratégicas dentro del área, su crecimiento no ha estado acompañado por una política formal que regule de forma clara la actualización de estándares técnicos ni el tratamiento seguro de todos los datos recolectados en cada uno desarrollos.

En ausencia de estos lineamientos específicos, existe el riesgo de que se mantengan prácticas desactualizadas o incompatibles con los requerimientos legales vigentes, lo que podría comprometer tanto la seguridad de la información como el correcto cumplimiento normativo. Además, sin una guía estructurada, las decisiones técnicas suelen quedar al criterio del proveedor, lo que reduce aún más la trazabilidad de todas las acciones realizadas en estos proyectos.

Esta política responde a esa necesidad. Su propósito es fortalecer y formalizar criterios para mantener actualizados los estándares de seguridad, e integrar una normativa aplicable al tratamiento responsable de datos personales en los desarrollos digitales. Todo ello en conformidad con la Ley N.º 8968 y con los controles pertinentes establecidos por la norma ISO/IEC 27001.

OBJETIVO

Establecer una política que oriente la correcta actualización periódica de los estándares técnicos aplicables a los desarrollos web subcontratados por el Departamento de Mercadeo, garantizando que estos mantengan su vigencia frente a los cambios normativos, tecnológicos y operativos que afectan la seguridad de la información.

Además, definir un marco normativo para el tratamiento de datos personales dentro de estos desarrollos, incluyendo principios de seguridad, calidad, trazabilidad y confidencialidad. Esta política busca asegurar que los sitios web y plataformas digitales gestionados por terceros operen bajo prácticas que respeten la legislación vigente, en especial la Ley Nº8968, y los controles establecidos por la norma ISO/IEC 27001, promoviendo así una gestión responsable, auditable y alineada con los valores institucionales de la Cooperativa.

ALCANCE

La presente política aplica a todos los desarrollos web que sean subcontratados por el Departamento de Mercadeo que impliquen la recolección, procesamiento o almacenamiento de datos personales. Su aplicación es obligatoria tanto para proveedores externos como para el personal interno que participe en la gestión, validación o aprobación de dichos proyectos.

También será de cumplimiento para cualquier micrositio, landing page, formulario digital diseñado para interacción con usuarios finales, independientemente de su duración, complejidad o medio de publicación. Los lineamientos definidos en este documento deberán ser considerados desde la etapa de planificación del proyecto hasta su cierre y documentación final.

El Departamento de Tecnologías de Información juntamente con la Dirección de Experiencia al Consumidor serán las instancias encargadas de verificar que los estándares y protocolos descritos en esta política sean aplicados correctamente en cada uno de los desarrollos para el área, como condición previa para autorizar el despliegue en entornos productivos.

FUNDAMENTO NORMATIVO

Esta política se basa en el marco legal costarricense y en estándar internacional ISO 27001:2002, con el propósito de asegurar el cumplimiento en el tratamiento de datos personales y en la gestión de seguridad de la información.

Ley No. 8968 – Protección de la Persona frente al Tratamiento de sus Datos Personales

- Artículo 6: Establece que los datos personales deben ser exactos, veraces y adecuados, lo que exige limitar la recolección de información a lo estrictamente necesario.
- Artículo 11: Impone el deber de confidencialidad a todas las personas involucradas en el tratamiento de datos, reforzando la necesidad de controles de acceso.
- Artículo 12: Permite emitir protocolos de actuación para gestionar adecuadamente los datos personales, los cuales deben ser aplicados por las organizaciones como parte de su deber de diligencia y cumplimiento interno.

Normativa internacional aplicable: Norma ISO/IEC 27001:2022

- Control A.5.1 – Políticas de seguridad de la información: Exige que la organización defina, apruebe y mantenga políticas que establezcan los objetivos de seguridad, alineadas con el marco legal y los riesgos identificados. Este control respalda la creación de esta política como instrumento formal de dirección.
- Control A.5.36 – Cumplimiento con normas y políticas: Señala la necesidad de asegurar que las actividades organizacionales estén alineadas con políticas, reglas y estándares vigentes. En el caso de Dos Pinos, esto implica garantizar que proveedores y personal interno trabajen conforme a los estándares definidos y actualizados periódicamente.
- Control A.5.15 – Control de acceso: Establece que deben definirse y aplicarse reglas que limiten el acceso físico y lógico a los activos de información según roles y responsabilidades. Esto es fundamental cuando los desarrollos web manejan datos personales, ya que evita accesos no autorizados o fugas de información.
- Control A.8.10 – Eliminación de información: Requiere que los datos almacenados se eliminen de forma segura cuando ya no sean necesarios. Esto implica definir criterios para

la eliminación de datos recolectados en formularios de campañas y asegurar que esta acción esté documentada y controlada por los proveedores.

LINEAMIENTO PARA LA ACTUALIZACIÓN DE LOS ESTÁNDARES

La vigencia y eficacia de los estándares técnicos aplicables a los desarrollos web dependen de una constante revisión frente a cambios normativos, tecnológicos y operativos que puedan existir con el avance del tiempo. Por ello, la presente política establece los siguientes lineamientos para garantizar su debida actualización periódica:

- **Frecuencia mínima:** Los estándares deberán revisarse al menos una vez al año, o cuando ocurra un cambio significativo en la legislación, normativas internacionales o infraestructura tecnológica institucional.
- **Responsables:** La unidad de Tecnologías de Información será el área técnica encargada de proponer ajustes a los estándares. El Departamento de Mercadeo, como área solicitante, deberá participar en la validación de los cambios aplicables a los proyectos bajo su gestión y entender cuáles son los cambios para que estos nuevos ajustes entren a regir de la forma correcta.
- **Fuentes de actualización:** Toda revisión deberá considerar nuevas versiones de la Ley Nº8968, actualizaciones a la norma ISO/IEC 27001, así como alertas de seguridad, vulnerabilidades emergentes o cualquier cambio en las plataformas tecnológicas utilizadas por la Cooperativa.
- **Mecanismo de control:** Cada actualización deberá documentarse en un historial de versiones con fecha, describir cuáles fueron los cambios introducidos, áreas involucradas y responsable del ajuste. El nuevo estándar entrará a regir tras su comunicación oficial a las partes interesadas y difundidas por el departamento de comunicación interna de la Cooperativa.

Todos estos lineamientos permiten mantener una base técnica vigente, reducir el riesgo de obsolescencia normativa y asegurar que los desarrollos se construyan bajo criterios actuales, seguros y auditables. Como parte de este enfoque, a continuación, se resumen las

responsabilidades asignadas a cada actor institucional involucrado en el proceso de actualización de estándares:

Tabla 5
Tabla de responsabilidades en la actualización de estándares.

Rol	Responsabilidades clave
Departamento de TI	• Identificar cambios normativos y tecnológicos. • Proponer ajustes a los estándares vigentes. • Documentar las versiones actualizadas. • Comunicar cambios a las áreas implicadas en el proceso.
Departamento de Mercadeo	• Participar en la validación de los ajustes propuestos. • Asegurar que, los proveedores apliquen los nuevos lineamientos de forma correcta. • Incluir los estándares actualizados en los debidos repositorios del SharePoint del Departamento.
Proveedores externos	• Aplicar los estándares vigentes en cada desarrollo. • Incorporar las modificaciones en sus entregables. • Documentar el cumplimiento técnico en cada fase del proyecto.

Fuente: *Vega, 2025.*

NORMATIVA DE TRATAMIENTO DE DATOS PERSONALES EN LOS DESARROLLOS WEB

Propósito:

Regular el tratamiento de los datos personales recolectados o procesados en los desarrollos web subcontratados por el Departamento de Mercadeo, estableciendo criterios mínimos de seguridad, confidencialidad y calidad. Esta normativa busca prevenir riesgos legales, operativos y reputacionales mediante la aplicación de controles técnicos alineados con la Ley Nº8968 y la norma ISO/IEC 27001, asegurando que toda plataforma digital gestionada por terceros cumpla con los principios de protección de datos.

Principios rectores:

La presente normativa se fundamenta en los principios esenciales que garantizan el tratamiento adecuado de los datos personales, conforme al marco legal costarricense y los estándares internacionales de seguridad de la información. Los siguientes principios deben ser aplicados de forma obligatoria en cualquier desarrollo web que recolecte o procese datos personales:

- **Calidad de la información:** Según el Artículo 6 de la Ley Nº8968, los datos personales deben ser exactos, actualizados, veraces y pertinentes. Esto implica que los formularios y sistemas utilizados en desarrollos web solamente deben recolectar únicamente la información estrictamente necesaria para el propósito específico del proyecto, evitando campos genéricos o innecesarios.
- **Confidencialidad:** De acuerdo con el Artículo 11 de la misma ley, toda persona que intervenga en el tratamiento de datos personales tiene el deber de guardar secreto profesional o funcional, incluso después de finalizada su relación contractual. Esto exige que los proveedores implementen controles de acceso, separación de entornos y protección lógica de la información para evitar filtraciones, manipulaciones o accesos no autorizados.
- **Necesidad y minimización:** Este principio complementa los anteriores y exige que todo dato recolectado tenga una justificación operativa o legal clara. La recolección excesiva de datos constituye una práctica contraria a la normativa vigente y debe ser evitada desde la fase de diseño del desarrollo.

- **Trazabilidad:** Cada acción relacionada con los datos personales debe ser documentada o registrable. Esto permite identificar quién accedió a la información, cuándo, desde qué canal, en qué condiciones, asegurando así la capacidad de auditoría y control posterior.
- **Legalidad y responsabilidad:** Todo tratamiento debe sustentarse en una base legal válida y verificable. La organización debe estar preparada para demostrar que los procesos técnicos y administrativos cumplen con lo exigido por la Ley Nº8968 y los controles aplicables de la norma ISO/IEC 27001.

Controles mínimos requeridos:

Todo desarrollo web que recolecte o procese datos personales deberá cumplir con los siguientes controles técnicos y operativos, como condición para su aprobación:

- **Control de acceso basado en roles:** El sistema debe permitir la gestión de privilegios diferenciados según funciones. El acceso a información personal debe limitarse únicamente a personal autorizado, y todo acceso debe estar autenticado y registrado.
- **Transmisión segura de datos (HTTPS):** Todo formulario o interfaz de recolección debe operar bajo protocolo HTTPS, asegurando la encriptación de los datos en tránsito y previniendo su interceptación.
- **Validación de formularios:** Deben implementarse filtros en el lado cliente y servidor para validar el tipo y formato de los datos ingresados. Además, los formularios deben limitarse a recolectar únicamente los campos estrictamente necesarios, evitando datos sensibles no justificados.
- **Política visible de privacidad:** Todo desarrollo debe incluir un enlace visible a una política de privacidad que informe al usuario sobre el uso, finalidad, derechos y responsable del tratamiento de los datos personales.
- **Eliminación segura de datos:** Cuando los datos recolectados ya no sean necesarios, deberán eliminarse de forma definitiva mediante procesos que impidan su recuperación o exposición posterior. El proveedor deberá asegurar este proceso y registrarlo como parte del expediente técnico.
- **Documentación de consentimiento (cuando aplique):** En los casos donde se requiera consentimiento del usuario, este debe ser recolectado de forma explícita, con registros que permitan verificarlo en caso de auditoría.

Estos controles forman parte del cumplimiento mínimo requerido y deberán reflejarse en los entregables técnicos del proveedor, así como en los informes de revisión del Departamento de Mercadeo y de Tecnologías de Información.

Aplicación obligatoria:

El cumplimiento de esta normativa es de carácter obligatorio para todos los desarrollos web subcontratados por el Departamento de Mercadeo que recolecten o procesen datos personales. La aplicación de los controles aquí definidos será una condición indispensable para la aprobación y puesta en producción de cualquier plataforma digital.

Para garantizar su cumplimiento, se establecen los siguientes mecanismos:

- **Checklist de verificación institucional:** El proveedor deberá completar el formulario oficial definido en la ***Normativa de verificación mediante checklist de seguridad (NTV-CDS-001)***, que incluye un apartado específico sobre tratamiento de datos personales. Además, deberá adjuntar evidencia técnica que respalde la implementación de cada control declarado.
- **Validación técnica por el Departamento de TI:** El checklist y sus evidencias serán revisados por el área de Tecnologías de Información, como parte del flujo descrito en el ***Proceso técnico para la validación del código fuente, accesos y cifrado (PR-VCS-001)***. Ningún desarrollo podrá ser publicado sin la aprobación técnica correspondiente.
- **Inclusión en el expediente de campaña:** Toda documentación generada (checklist, evidencias y validaciones) deberá ser archivada en el expediente técnico de la campaña, bajo la custodia del Departamento de Mercadeo. Esto garantiza trazabilidad, cumplimiento normativo y respaldo ante auditorías internas o externas.

Es importante recalcar que ***La Directriz de evaluación y análisis dinámica de seguridad (DR-EADS-001***) también deberá considerarse como insumo complementario para validar la robustez técnica del desarrollo, en especial en proyectos con formularios o procesamiento activo de datos personales.

Aplicación obligatoria:

Esta normativa se implementa en conjunto con los lineamientos técnicos ya establecidos por la Cooperativa, fortaleciendo el enfoque integral de seguridad en los desarrollos web subcontratados. En particular, se vincula directamente con:

- PR-VCS-001: Proceso técnico para la validación del código fuente, accesos y cifrado.
- DR-EADS-001: Directriz de evaluación y análisis dinámica de seguridad.
- NTV-CDS-001: Normativa de verificación mediante checklist de seguridad.

Cada uno de estos documentos contribuye desde una dimensión técnica específica, mientras que esta normativa asegura la correcta aplicación de criterios legales y operativos para el tratamiento responsable de los datos personales.

MECANISMO DE VALIDACIÓN Y MEJORA CONTINUA

La presente política será objeto de revisión periódica con el fin de asegurar su vigencia, aplicabilidad y coherencia con el entorno normativo y operativo de la Cooperativa. A diferencia de los estándares técnicos definidos en otros apartados, este mecanismo se enfoca en evaluar la utilidad, alcance y adecuación de la política como documento rector.

Para ello, se establecen las siguientes disposiciones:

- **Periodicidad de revisión:** La política deberá ser evaluada al menos una vez por año, o antes si ocurren cambios significativos en la legislación nacional (como la Ley Nº8968), en los controles de la norma ISO/IEC 27001 o en los procesos internos que afecten su aplicación.
- **Responsables del proceso:** La revisión estará a cargo del Departamento de Tecnologías de Información, en coordinación con Mercadeo, quienes deberán valorar si los objetivos, lineamientos y alcances siguen respondiendo a las necesidades reales de los desarrollos web subcontratados.
- **Fuentes de retroalimentación:** La mejora continua podrá basarse en observaciones emitidas por auditores internos o externos, retroalimentación de los proveedores, dificultades operativas detectadas por las áreas responsables, o análisis de eventos relacionados con incumplimiento normativo o seguridad de datos.
- **Control de versiones:** Toda modificación deberá registrarse en el historial de versiones de esta política, documentando fecha, descripción del cambio y responsable. Esto garantizará trazabilidad documental y respaldo ante auditorías o fiscalizaciones institucionales.

Este proceso de evaluación permite asegurar que la política mantenga su valor estratégico como instrumento de cumplimiento, gestión de riesgo y protección de los derechos de las personas usuarias.

Historial de versiones de la política:

Tabla 6
Detalle de versiones de la política

Versión	Fecha	Descripción del cambio	Responsable
1.0	20/06/2025	Versión inicial de la política. Incluye lineamientos de actualización de estándares técnicos y normativa para el tratamiento de datos personales en desarrollos web subcontratados.	Johan Vega
1.2			
1.3			

Fuente: *Vega, 2025.*

APÉNDICE B

Proceso de validación de la calidad y seguridad de los desarrollos web

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

PROCESO DE VALIDACIÓN DE LA CALIDAD Y SEGURIDAD DE LOS DESARROLLOS WEB EN CUANTO A CÓDIGO FUENTE, ACCESOS Y CIFRADO.

JOHAN VEGA CÓRDOBA

MAYO, 2025

Cooperativa de Productores de Leche Dos Pinos R.L.		Código: PR-VCS-001
PROCESO DE VALIDACIÓN DE LA CALIDAD Y SEGURIDAD DE LOS DESARROLLOS WEB EN CUANTO A CÓDIGO FUENTE, ACCESOS Y CIFRADO		Versión 1
Realizado por: Johan Vega Córdoba	Departamento de Mercadeo	Página de 1 de 8

INTRODUCCIÓN

En el contexto actual de desarrollo digital, el uso de tecnologías web se ha convertido en un factor esencial para las estrategias de mercadeo de departamento de experiencia del consumidor. Sin embargo, el crecimiento en la demanda de desarrollos web ha traído consigo más riesgos asociados a la seguridad de la información, especialmente cuando los desarrollos no son creados directamente por el Departamento de Tecnologías de Información, sino por terceros contratados a través de áreas funcionales como mercadeo. Esta situación aumenta la exposición a incidentes como la fuga de datos, accesos no autorizados, inserción de código malicioso y pérdida de trazabilidad sobre los cambios realizados en el código fuente.

En la Cooperativa de Productores de Leche Dos Pinos R.L., el Departamento de Mercadeo ha incrementado en los últimos dos años significativamente la contratación de servicios de desarrollo web externo para la implementación de micrositios, páginas de campaña y soluciones interactivas. Ante esta realidad, se identifica una necesidad de establecer un procedimiento estandarizado que permita garantizar que todos desarrollos cumplan con prácticas mínimas de seguridad de la información.

Este procedimiento tiene como propósito central la construcción de un proceso formal que permita la revisión y control sistemático de tres componentes críticos: la validación del código fuente, el control de accesos y la encriptación de los datos. Estos elementos no solo representan prácticas esenciales recomendadas por la norma ISO/IEC 27001:2022, sino que también son coherentes con los principios establecidos en la Ley Nº8968 sobre protección de datos personales. Su cumplimiento permite mitigar los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información.

El procedimiento planteado busca establecer los requisitos específicos que se deben cumplirse antes, durante y después del desarrollo, así como la forma de documentar y verificar su implementación. Lo que se pretende es brindar al Departamento de Mercadeo de una herramienta útil y aplicable, que no dependa de plataformas o recursos tecnológicos sofisticados, sino de lineamientos claros, trazables y auditables para verificar el cumplimento correcto del procedimiento.

OBJETIVOS

El presente procedimiento tiene como objetivo principal establecer un estándar de seguridad aplicable a los desarrollos web contratados por el Departamento de Mercadeo de la Cooperativa de Productores de Leche Dos Pinos R.L., a fin de asegurar que cumplan con los requisitos mínimos de control y protección de la información. Este estándar se enfoca específicamente en tres componentes fundamentales para la seguridad de los activos digitales:

1. La validación del código fuente, asegurando su integridad, trazabilidad y control de versiones.
2. La gestión de accesos, garantizando que los privilegios sean otorgados únicamente proveedores o colaboradores externos se encuentren controlados, documentados y alineados a los principios de seguridad.
3. La encriptación de los datos, tanto en tránsito como en reposo, utilizando mecanismos criptográficos sólidos que protejan la confidencialidad e integridad de la información intercambiada o almacenada en el marco de dichos desarrollos.

Este procedimiento pretende facilitar la verificación del cumplimiento de estas medidas de seguridad mediante evidencia debidamente documentada, permitiendo auditorías internas, controles posteriores y la mejora continua de las prácticas en el ciclo de desarrollo web. La propuesta no requiere inversiones en herramientas específicas, sino que se apoya en lineamientos operativos claros, aplicables desde la contratación hasta la entrega final del producto digital.

ALCANCE

Este procedimiento será de aplicación obligatoria para todo desarrollo web solicitado o coordinado por el Departamento de Mercadeo, independientemente de la tecnología utilizada, siempre que:

1. El desarrollo involucre la recopilación, tratamiento o almacenamiento de información personal, credenciales de acceso, datos transaccionales o cualquier tipo de información considerada sensible según la clasificación interna de Dos Pinos o lo establecido en la Ley costarricense Nº8968.
2. El desarrollo sea ejecutado parcial o totalmente por proveedores externos, agencias, desarrolladores independientes o cualquier actor ajeno al área de Tecnologías de Información.
3. El producto digital sea accesible desde internet o expuesto públicamente (micrositios, landing pages, aplicaciones ligeras, concursos, formularios u otras soluciones equivalentes).

El procedimiento aplica desde la fase de planeación del proyecto (brief o requerimiento técnico), durante la ejecución, hasta la recepción y validación final del entregable. No será aplicable a desarrollos internos realizados por el Departamento de TI bajo el control de sus propias políticas, salvo que el área de Mercadeo lo solicite expresamente.

FUNDAMENTACIÓN NORMATIVA Y PRÁCTICAS APLICABLES

El procedimiento propuesto se fundamenta en las mejores prácticas internacionales de seguridad de la información y en la normativa legal costarricense en materia de protección de datos personales. Su propósito es asegurar que todo desarrollo web externo cuente con los controles mínimos que protejan la información, reduzcan los riesgos y garanticen su cumplimiento en la Cooperativa de Productores de Leche Dos Pinos R.L. Desde la perspectiva normativa, se consideran los siguientes marcos de referencia:

a) Norma ISO/IEC 27001:2022: Los controles aplicables al presente procedimiento se derivan del Anexo A de la ISO/IEC 27001:2022, distribuidos principalmente entre dos cláusulas:

- Cláusula 5 – Controles organizacionales: establece políticas institucionales y prácticas de gestión necesarias para garantizar que el acceso a los activos de información esté controlado, autorizado y documentado.
- Cláusula 8 – Controles tecnológicos: abarca las prácticas técnicas que aseguran la protección efectiva de la información mediante la implementación de herramientas, procedimientos seguros y validaciones técnicas.

Los controles específicos considerados son:

- A.5.15 – Control de acceso: Este control establece que deben definirse reglas para controlar el acceso físico y lógico a la información y otros activos asociados, basándose en requisitos de negocio y seguridad de la información. La implementación de este control implica la creación de políticas específicas de control de acceso, la identificación de activos, la clasificación de la información y la asignación de derechos de acceso adecuados.
- A.8.4 – Acceso al código Fuente: Este control requiere que el acceso de lectura y escritura al código fuente, herramientas de desarrollo y bibliotecas de software sea gestionado adecuadamente. Su propósito es prevenir la introducción de funcionalidades no autorizadas, evitar cambios no intencionados o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.
- A.8.13 – Protección de datos en tránsito: Este control establece que deben mantenerse copias de respaldo de la información, el software y los sistemas, y que estas copias deben

probarse regularmente de acuerdo con la política específica de respaldo acordada. Su objetivo es permitir la recuperación de datos o sistemas en caso de pérdida.

- A.8.30 – Desarrollo subcontratado: Este control establece que la organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados. Su propósito es garantizar que los desarrollos realizados por terceros cumplan con los requisitos de seguridad de la información establecidos por la organización.

Este último resulta especialmente relevante en el contexto de la presente propuesta, ya que exige la implementación de mecanismos que aseguren la confidencialidad, integridad y calidad de los desarrollos realizados por proveedores externos.

b) Ley Nº8968, Protección de la persona frente al tratamiento de sus datos personales: El procedimiento también se alinea con lo establecido en la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, particularmente:

- Artículo 6: Principio de calidad de la información: establece que los datos personales deben ser actuales, veraces, exactos y adecuados al fin para el que fueron recolectados.
- Artículo 11: Deber de confidencialidad: impone la obligación a quienes intervienen en el tratamiento de datos personales de guardar secreto profesional o funcional, incluso después de finalizada su relación con la base de datos.
- Artículo 12: Seguridad del tratamiento de los datos personales: obliga a los responsables de bases de datos a adoptar medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

En coherencia con este marco normativo, el procedimiento establece las siguientes buenas prácticas para cada componente crítico:

Validación del código fuente:

- Uso de repositorios privados con control de versiones (GitLab, GitHub Enterprise, Bitbucket).
- Trazabilidad de los cambios mediante registro de usuario y sello de tiempo.
- Revisión del código mediante herramientas de análisis estático (ej. SonarQube).
- Separación de entornos (desarrollo, pruebas, producción).

Control de accesos:

- Implementación del principio de mínimo privilegio.
- Cuentas individuales autenticadas y controladas por vigencia.
- Prohibición de cuentas genéricas o compartidas.
- Cierre obligatorio y documentado de accesos al finalizar el proyecto.

Encriptación de datos:

- Transmisión mediante HTTPS con TLS 1.2 o superior.
- Cifrado en reposo con algoritmos robustos como AES-256.
- Verificación de certificados digitales válidos en ambientes productivos y de prueba.
- Documentación de cifrado en APIs o servicios externos utilizados en el desarrollo.

Cuando el desarrollo sea subcontratado, el proveedor deberá entregar evidencia del cumplimiento de estos controles como parte del cierre del proyecto, en concordancia con el control A.8.30 de la ISO/IEC 27001.

Estas medidas no requieren la implementación de herramientas complejas ni licencias adicionales, sino una correcta planificación, verificación documental y compromiso con la seguridad desde el inicio del proyecto. Su aplicación permitirá fortalecer la cultura de seguridad en las prácticas operativas del Departamento de Mercadeo, reducir el riesgo legal y proteger la reputación institucional de la Cooperativa Dos Pinos.

RECOMENDACIÓN DE IMPLEMENTACIÓN

Para facilitar la implementación del procedimiento, se recomienda su aplicación en tres etapas consecutivas. Esta estrategia permitirá que los proyectos web contratados por el Departamento de Mercadeo puedan integrarse y cumplir progresivamente a un marco de seguridad estandarizado, sin afectar su ejecución operativa ni depender de recursos técnicos avanzados.
Etapa 1: Diagnóstico inicial del proveedor

Etapa #1: Diagnóstico inicial del proveedor

En esta fase se realiza una revisión previa de las condiciones técnicas del proveedor seleccionado. El objetivo es conocer su nivel de madurez en temas de seguridad y anticipar posibles brechas que deban corregirse desde el inicio del proyecto.

Acciones sugeridas:

- Validar si el proveedor utiliza herramientas de control de versiones como Git, GitHub, GitLab, etc.
- Consultar el método de acceso previsto a servidores, entornos de pruebas o bases de datos.
- Solicitar evidencia de prácticas de cifrado (uso de HTTPS, certificados, encriptación de archivos).
- Revisar si el proveedor tiene experiencia previa en proyectos donde se hayan exigido normas de seguridad o políticas corporativas.

Etapa #1: Estandarización de prácticas mínimas de seguridad

Esta fase corresponde al inicio del proyecto y debe integrarse dentro de los requisitos contractuales con cualquier proveedor de la Cooperativa en temas de desarrollo web. El objetivo es asegurar que las medidas de control de seguridad estén activas desde el diseño del desarrollo y que puedan verificarse durante su ejecución.

Acciones sugeridas:

- Incluir en el contrato de servicios los requisitos definidos en el presente procedimiento (validación de código, control de accesos, cifrado).

- Solicitar al proveedor que documente los accesos necesarios, las cuentas que utilizará y su vigencia.
- Verificar que el entorno de pruebas utilice protocolos seguros (TLS/SSL) y cuentas diferenciadas.
- Solicitar que el repositorio esté activo desde el inicio del desarrollo y que permita trazabilidad de cambios.

Etapa #3: Validación de cumplimiento y cierre del Proyecto

Al finalizar el desarrollo web, es necesario comprobar que los controles establecidos se cumplieron y que la información manejada durante el proyecto no haya quedado expuesta a riesgos.

Acciones sugeridas:

- Solicitar evidencia del uso de repositorio (bitácora de commits, control de versiones).
- Verificar que los accesos hayan sido eliminados o revocados correctamente.
- Comprobar que la comunicación entre usuario y servidor esté cifrada mediante certificado válido.
- Confirmar, si aplica, que los datos almacenados durante el desarrollo hayan sido cifrados o destruidos de forma segura.
- Registrar los hallazgos y resultados en un informe de cierre técnico que quede archivado como respaldo del cumplimiento del procedimiento.

PROCEDIMIENTO TÉCNICO PARA LA VALIDACIÓN DEL CÓDIGO, CONTROL DE ACCESOS Y CIFRADO DE DATOS

Este procedimiento se compone de tres bloques funcionales que abordan los elementos fundamentales de seguridad: la validación del código fuente, el control de accesos y la encriptación de datos tanto en tránsito como en reposo. Cada uno de estos componentes responde a los principios establecidos en la Ley Nº8968 y a los controles técnicos y organizacionales definidos en la norma ISO/IEC 27001:2022, particularmente en sus cláusulas 5 y 8.

La estructuración del procedimiento en fases diferenciadas permite su implementación progresiva en los proyectos contratados por el Departamento de Mercadeo, a partir de requerimientos específicos, acciones prácticas verificables y entregables documentados.

Cada componente incluye: un objetivo funcional, los requisitos técnicos, la referencia normativa correspondiente (control ISO y artículos de ley), la evidencia mínima que el proveedor debe presentar y los actores responsables de su verificación. Esto facilitará la trazabilidad, monitoreo y posible auditoría.

Gestión del código Fuente

Objetivo: Asegurar la trazabilidad, integridad y autenticidad del código fuente entregado por agencias o proveedores externos, mediante la implementación de mecanismos de control de versiones, revisión técnica y documentación de evidencias que permitan validar el cumplimiento de buenas prácticas de desarrollo seguro.

Controles aplicables:

- **ISO/IEC 27001:2022:** A.8.4 - Acceso al código fuente, A.8.30 – Desarrollo subcontratado
- **Ley Nº8968:** Artículo 6 - Principio de calidad de la información, Artículo 12 - Seguridad del tratamiento de los datos personales

Requisitos específicos:

- **Repositorio de control de versiones obligatorio:** El proveedor, o el tercero subcontratado bajo su responsabilidad, deberá disponer y administrar un repositorio privado que permita controlar las versiones del código fuente, como parte de los medios técnicos mínimos exigidos. Este repositorio debe estar alojado en plataformas especializadas como GitLab, Bitbucket, GitHub Enterprise u otra equivalente que permita acceso autenticado y trazabilidad completa del historial de cambios (commits).
  La Cooperativa de Productores de Leche Dos Pinos R.L. no proveerá infraestructura tecnológica para este propósito. La existencia y uso adecuado del repositorio deberá quedar establecido como cláusula en el contrato.
- **Autenticación individual y trazabilidad de cambios:** Toda modificación del código fuente deberá estar asociada a un usuario autenticado, con registro de autor, fecha y descripción del cambio. El repositorio debe permitir identificar quién hizo cada modificación, en qué momento y con qué finalidad. Queda prohibido el uso de cuentas genéricas o compartidas.
- **Estructura por entornos de desarrollo:** El repositorio deberá evidenciar la existencia de entornos separados para desarrollo, pruebas y producción. Esto puede reflejarse mediante el uso de ramas diferenciadas (por ejemplo: dev, staging, main) o estructuras equivalentes. La versión final publicada deberá coincidir con la versión revisada y aprobada.
- **Revisión técnica del código fuente:** El proveedor deberá realizar una revisión estructurada del código, preferiblemente mediante herramientas de análisis estático como SonarQube, Codacy u otra plataforma de inspección de código que permita identificar vulnerabilidades, código duplicado o malas prácticas. Los resultados deberán ser documentados, incluyendo el historial de hallazgos y las acciones correctivas aplicadas antes del despliegue.
- **Verificación por parte de Dos Pinos:** Durante el desarrollo, el Departamento de TI o el responsable del proyecto podrá solicitar **acceso temporal al repositorio en tiempo real** para inspección técnica. Este acceso deberá ser gestionado bajo mecanismos seguros, con vigencia definida. No obstante, la verificación final del cumplimiento se basará en la **entrega formal de evidencias técnicas documentadas** (capturas, bitácoras, informes), que serán archivadas por el equipo de Mercadeo como respaldo para eventuales auditorías.

- **Cierre técnico y trazabilidad posterior:** Una vez finalizado el proyecto, el proveedor deberá entregar un paquete documental de cierre**,** que incluya evidencias de control de versiones, historial de cambios, y declaración técnica firmada donde certifique que el código entregado corresponde con la versión auditada. Esta documentación deberá almacenarse internamente por Dos Pinos, como respaldo para auditorías futuras, sin requerir acceso continuo al repositorio.

Evidencias requeridas:

- Capturas de pantalla o exportación del historial de commits (fecha, autor, mensaje).
- Exportación de configuración de accesos (roles, permisos, autenticación).
- Evidencia de estructura por entornos (branches o carpetas de despliegue).
- Informe de análisis estático del código con resumen de hallazgos y correcciones.
- Declaración técnica del proveedor validando la versión final del código.
- Registro de acceso temporal otorgado a Dos Pinos (si se aplicó revisión en tiempo real).

Responsables:

- Proveedor o subcontratista (Cuando aplica): Responsable de implementar y administrar el repositorio, realizar las revisiones técnicas, entregar documentación y garantizar la trazabilidad del código fuente.
- Agencia contratada (Cuando aplica): Debe garantizar que cualquier tercero subcontratado cumpla con estos requisitos. La agencia es corresponsable ante Dos Pinos en caso de incumplimiento por parte del desarrollador.
- Responsable del proyecto (Mercadeo): Verifica que las evidencias sean entregadas y gestionadas, coordina con TI las revisiones necesarias y valida el cierre técnico.
- Departamento de TI (cuando aplica): Puede realizar inspecciones técnicas temporales y emitir criterio sobre el cumplimiento de buenas prácticas de desarrollo seguro.

Checklist de verificación para la gestión del código fuente:

Este checklist se utiliza como parte del cierre del proceso de gestión del código fuente. Permite validar el cumplimiento de los requisitos técnicos y dejar constancia documental para auditorías. Debe ser completado por el responsable del proyecto y archivado con la documentación final.

Tabla 7
Checklist de cierre proceso de gestión del código fuente

Item	Criterio de cumplimiento	Cumple	Observaciones
1	El proveedor utilizó un repositorio privado con control de versiones.	☐ Sí / ☐ No	
2	Todo acceso al repositorio fue autenticado y vinculado a usuarios individuales.	☐ Sí / ☐ No	
3	El historial de cambios (commits) incluye fecha, autor y descripción.	☐ Sí / ☐ No	
4	Se utilizaron ramas separadas para desarrollo, pruebas y producción.	☐ Sí / ☐ No	
5	Se presentó evidencia de análisis estático del código (ej. SonarQube).	☐ Sí / ☐ No	
6	La versión publicada en producción coincide con la versión revisada.	☐ Sí / ☐ No	
7	Se entregó documentación técnica de cierre del repositorio.	☐ Sí / ☐ No	
8	Se realizó verificación técnica por parte del Departamento de TI (cuando aplica).	☐ Sí / ☐ No	

Fuente: Vega*, 2025.*

Este checklist también se encuentra disponible en formato editable en línea para facilitar su uso y archivo digital. Puede acceder al documento mediante el siguiente enlace: Checklist de cumplimiento

Gestión de accesos en desarrollos web subcontratados

Objetivo: Establecer controles para que todo acceso habilitado durante el desarrollo web subcontratado sea autorizado, temporal y trazable, garantizando la confidencialidad de la información y el cierre efectivo de privilegios al finalizar el proyecto.

Controles aplicables:

- **ISO/IEC 27001:2022:** A.5.15 - Control de acceso, A.8.30 - Desarrollo subcontratado
- **Ley Nº8968:** Artículo 11- Deber de confidencialidad, Artículo 12 – Seguridad del tratamiento de los datos personales

Requisitos específicos:

- **Accesos documentados y autorizados:** Todo acceso otorgado a recursos relacionados con el desarrollo web (servidores, repositorios, entornos de prueba, sistemas de contenido, bases de datos o herramientas de despliegue) debe estar previamente autorizado, documentado y registrado en una matriz formal de accesos.
- **Individualización y autenticación:** Los accesos deben ser asignados de forma personal, con credenciales únicas asociadas a cada desarrollador, sin permitir el uso de cuentas genéricas o compartidas. Todos los accesos deben contar con autenticación controlada (por contraseña segura, doble factor o mecanismo equivalente).
- **Control de vigencia:** Toda credencial o usuario otorgado deberá tener un periodo de validez definido (dependiendo de la duración del proyecto, esto dependerá de la magnitud del desarrollo). El proveedor deberá especificar fecha de activación y fecha prevista de expiración.
- **Eliminación de accesos al cierre del proyecto:** Una vez finalizado el desarrollo, todos los accesos otorgados deberán ser revocados o eliminados. El proveedor deberá entregar constancia de que ningún tercero conserva accesos a sistemas, archivos o herramientas relacionados con el proyecto.
- **Registro de accesos físicos (si aplica):** Si el desarrollo involucra trabajo presencial con acceso físico a infraestructura de Dos Pinos, estos ingresos deberán documentarse por parte del proveedor y coordinarse con el área de TI con previo aviso.

Evidencias requeridas:

- Matriz de accesos inicial con detalle de cada usuario, tipo de acceso, sistema, vigencia y autorización.
- Bitácora de aprobaciones, modificaciones o cierres de accesos
- Captura o exportación de la configuración de usuarios activos al momento de cierre.
- Declaración técnica de cierre de accesos firmada por el proveedor o responsable del desarrollo.

Responsables:

- Proveedor o desarrollador: Responsable de gestionar todos los accesos requeridos y entregar documentación al respecto.
- Agencia contratada: Corresponsable en caso de subcontratación. Debe asegurar el cumplimiento de este control por parte del tercero ejecutor.
- Responsable del proyecto (Mercadeo): Custodia la matriz de accesos y valida su completitud. Solicita cierres al finalizar el proyecto.
- Departamento de TI (cuando aplica): Apoya en la validación técnica de accesos otorgados y su eliminación, en caso de que se vinculen a infraestructura interna.

Tabla 2
Ejemplo de Matriz de acceso

Nombre del usuario	Cargo	Sistema o plataforma	Nivel de acceso	Fecha de habilitación	Fecha de cierre	Autorizado por	Observaciones
Juan Pérez	Desarrollador externo	GitHub – Repositorio del proyecto	Lectura y escritura	15/05/2025	30/06/2025	TI	Acceso revocado
María Gómez	QA subcontratada	Entorno de pruebas (staging)	Solo lectura	20/05/2025	05/07/2025	TI	

Fuente: *Vega, 2025.*

Puede acceder al documento mediante el siguiente enlace: Matriz de accesos - Proyectos WEB Mercadeo

Gestión de cifrado de datos en tránsito y reposo

Objetivo: Establecer los mecanismos mínimos de cifrado requeridos para proteger la información sensible durante su transmisión y almacenamiento en el contexto de desarrollos web realizados por proveedores externos.

Controles aplicables:

- **ISO/IEC 27001:2022:** A.8.13 – Protección de datos en tránsito, A.8.30 - Desarrollo subcontratado
- **Ley Nº8968:** Artículo 12 – Seguridad del tratamiento de los datos personales

Requisitos específicos:

Cifrado de datos en tránsito:

- Uso obligatorio de protocolo HTTPS: Todos los desarrollos deben implementarse bajo conexiones seguras que utilicen HTTPS con certificados digitales válidos y actualizados, que operen bajo el protocolo TLS versión 1.2 o superior.
- Transmisión cifrada de formularios y credenciales: Toda recolección de datos personales (formularios de contacto, registro, autenticación, etc.) debe estar protegida mediante canal cifrado, sin permitir envíos en texto plano.
- Conexiones a sistemas externos: Toda integración con APIs, servicios de terceros o herramientas externas deberá realizarse sobre canales cifrados. Se debe validar que las credenciales de acceso o tokens viajen de forma segura.

Cifrado de datos en reposo:

- Cifrado de bases de datos sensibles o archivos temporales: Si el desarrollo contempla almacenamiento temporal o persistente de datos personales, estos deberán mantenerse cifrados mediante algoritmos reconocidos como AES-256 o equivalente.
- Evitar almacenamiento de información confidencial sin necesidad: El proveedor deberá justificar el almacenamiento de cualquier dato sensible y garantizar que no se almacene información de forma innecesaria ni en ubicaciones no controladas.

- Eliminación segura de datos al finalizar el proyecto: Una vez concluido el desarrollo, toda información sensible almacenada en servidores, respaldos temporales o bases de datos debe ser eliminada mediante métodos de borrado seguro o destrucción digital.

Evidencias requeridas:

- Captura de certificado SSL vigente y correctamente configurado (pantalla del navegador o consola del servidor).
- Evidencia de tráfico cifrado (por ejemplo, vista del candado de seguridad o uso de herramientas como DevTools, CURL, Wireshark).
- Captura o reporte de configuración de cifrado de bases de datos (pantalla de panel de control o script aplicado).
- Declaración técnica del proveedor sobre la eliminación segura de datos sensibles tras el cierre.

Responsables:

- Proveedor/desarrollador: Implementa los mecanismos de cifrado, presenta las evidencias requeridas y garantiza la eliminación segura de los datos al cierre del proyecto.
- Agencia contratada: Garantiza que los terceros subcontratados cumplan con estos requisitos técnicos y que se incluyan en la documentación final.
- Responsable del proyecto (Mercadeo): Solicita y archiva las evidencias de cifrado como parte del cierre técnico.
- Departamento de TI (cuando aplica): Puede validar la correcta implementación de los cifrados o recomendar estándares técnicos mínimos durante el desarrollo.

Historial de versiones del procedimiento:

Versión	Fecha	Descripción del cambio	Responsable
1.0	30/05/2025	Versión inicial del procedimiento. Incluye controles sobre código fuente, accesos y cifrado.	Johan Vega
1.2			
1.3			

APÉNDICE C

Normativa sobre tratamiento de datos personales y consentimiento de usuarios

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

NORMATIVA SOBRE TRATAMIENTO DE DATOS PERSONALES Y CONSENTIMIENTO DE USUARIOS

JOHAN VEGA CÓRDOBA

JULIO, 2025

INTRODUCCIÓN

A pesar de que la Cooperativa reconoce la importancia de proteger los datos personales en los entornos digitales, los resultados obtenidos evidencian la falta de una normativa estandarizada que regule de forma clara el tratamiento de esta información en los desarrollos web subcontratados. Las entrevistas realizadas con colaboradores del Departamento de Mercadeo y del área de Tecnologías de Información revelaron que, si bien existen prácticas básicas de seguridad, no se cuenta con un marco formal que garantice la aplicación consistente de principios como la confidencialidad, la calidad de los datos o el consentimiento informado.

Esta ausencia de directrices también se ve reflejada en el incumplimiento de controles establecidos por la norma ISO/IEC 27001:2022, particularmente aquellos relacionados con el control de acceso (A.5.15), la eliminación segura de información (A.8.10) y el cumplimiento de normas y políticas internas (A.5.36). La falta de documentación formal impide que las agencias proveedoras integren adecuadamente estos requerimientos en sus procesos, afectando la trazabilidad, la seguridad y el cumplimiento de los principios definidos en la Ley Nº8968.

En este contexto, la presente normativa busca unificar los criterios técnicos, legales y operativos para el tratamiento de datos personales en los desarrollos web impulsados por el Departamento de Mercadeo. Su función es asegurar la aplicación de estándares internacionales, garantizar la obtención y gestión adecuada del consentimiento del usuario, y establecer protocolos que resguarden la información personal durante todo su ciclo de vida, en conformidad con el marco normativo vigente.

OBJETIVO

Establecer una normativa que regule el tratamiento de datos personales en los desarrollos web subcontratados por el Departamento de Mercadeo, asegurando la aplicación de medidas técnicas y administrativas que garanticen la seguridad, confidencialidad y calidad de la información. Esta normativa contempla directrices para la obtención del consentimiento del usuario, la gestión de cookies, el control de accesos, la trazabilidad de los datos y la atención de solicitudes sobre información personal, en cumplimiento con la Ley Nº8968 y los controles definidos en la norma ISO/IEC 27001:2022.

ALCANCE

Esta normativa aplica a todos los desarrollos web subcontratados por el Departamento de Mercadeo que involucren la recolección, tratamiento o almacenamiento de datos personales mediante formularios, tecnologías de rastreo o integraciones analíticas. Es de aplicación obligatoria para agencias proveedoras, así como para el personal interno responsable de supervisar el cumplimiento técnico, funcional y legal de cada proyecto.

Debe implementarse desde la etapa de planificación del desarrollo web, incluyendo el diseño del flujo de datos, la definición de mecanismos de consentimiento y la gestión de cookies, hasta la atención de solicitudes posteriores por parte de los titulares de la información. Su cumplimiento será condición indispensable para la validación técnica y aprobación final del proyecto por parte del Departamento de Tecnologías de Información.

FUNDAMENTO NORMATIVO

La implementación de esta normativa se sustenta en disposiciones legales y estándares internacionales que exigen a las organizaciones garantizar la protección de los datos personales a lo largo de todo su ciclo de vida. En particular, responde a los principios establecidos en la Ley Nº8968, Protección de la persona frente al tratamiento de sus datos personales, y a los controles de la norma ISO/IEC 27001:2022, que orientan la gestión segura de la información y la responsabilidad organizacional.

Los controles aplicables son:

ISO/IEC 27001:2022

- **A.5.15 – Control de acceso:** Establece la necesidad de aplicar controles de acceso físicos y lógicos sobre los datos personales, garantizando que solo personal autorizado acceda a la información.
- **A.5.36 – Cumplimiento con normas, políticas y estándares:** Obliga a asegurar que se cumplan las políticas internas de tratamiento de datos, así como la legislación vigente, mediante medidas documentadas, auditables y ejecutables.
- **A.8.10 – Eliminación de información:** Requiere que la organización implemente mecanismos seguros para eliminar información personal una vez que haya cumplido su propósito, reduciendo riesgos de filtración o uso indebido.

Ley N°8968 – Protección de la persona frente al tratamiento de sus datos personales:

- **Artículo 6 – Principio de calidad de la información:** Exige que los datos personales sean veraces, actuales y adecuados al fin para el cual fueron recolectados, lo cual implica establecer políticas claras sobre su tratamiento.
- **Artículo 11 – Deber de confidencialidad:** Obliga a las personas que intervienen en el tratamiento de datos personales a mantener el secreto profesional o funcional incluso después de concluida su relación con la base de datos.
- **Artículo 12 – Protocolos de actuación:** Permite a las organizaciones definir internamente procedimientos específicos para la recolección, almacenamiento y manejo de datos personales, con el fin de garantizar su seguridad y trazabilidad.

PRINCIPIOS DE TRATAMIENTO DE DATOS PERSONALES

Todo tratamiento de datos personales en desarrollos web subcontratados debe realizarse conforme a principios que aseguren el respeto por los derechos del titular, la legalidad del procesamiento y la calidad de la información manejada. Estos principios guían la recolección, almacenamiento, transmisión y eliminación de datos, y son de cumplimiento obligatorio para proveedores, agencias y responsables del proyecto.

Los siguientes principios, derivados de la Ley Nº8968, deberán aplicarse de forma transversal en todo desarrollo digital que recolecte o procese datos personales:

- **Consentimiento informado:** Todo tratamiento debe contar con la autorización previa, expresa e inequívoca del titular de los datos. Esta autorización debe ser obtenida mediante mecanismos claros, visibles y verificables.
- **Finalidad:** La información recolectada solo podrá utilizarse para los fines específicos declarados al usuario en el momento de su recolección. Cualquier uso adicional requerirá un nuevo consentimiento.
- **Proporcionalidad:** Solo podrán solicitarse los datos estrictamente necesarios para cumplir con la finalidad establecida. Se prohíbe la recolección excesiva o irrelevante.
- **Veracidad y calidad:** Los datos personales deben mantenerse actualizados, exactos y pertinentes. Es responsabilidad del proveedor garantizar mecanismos para su actualización o corrección.
- **Confidencialidad:** La información recolectada debe ser tratada con reserva, evitando su divulgación, acceso no autorizado o uso indebido.
- **Seguridad:** Deben aplicarse medidas técnicas y organizativas que garanticen la integridad, disponibilidad y protección de los datos personales frente a accesos no autorizados, pérdidas o manipulaciones.

Además de los principios anteriores, todo desarrollo web deberá cumplir con el control de transmisión segura de datos mediante la implementación obligatoria del protocolo **HTTPS**, respaldado por un certificado SSL/TLS vigente. Para verificar su correcta implementación, el proveedor deberá realizar un escaneo técnico de seguridad previo al lanzamiento, y repetirlo

periódicamente, especialmente ante actualizaciones críticas o cambios en la infraestructura del sitio. Los resultados deberán ser archivados como evidencia técnica en el expediente del proyecto y estarán sujetos a revisión por parte del Departamento de TI.

Es importante recalcar que la presente normativa no establece una herramienta específica para la ejecución del escaneo técnico de seguridad, ya que esto dependerá de la metodología y recursos del proveedor a cargo del proyecto. Sin embargo, toda herramienta utilizada para este fin deberá contar con la validación previa del Departamento de TI, quien evaluará su idoneidad técnica y alineamiento con los objetivos de seguridad establecidos por la Cooperativa. El proveedor deberá incluir evidencia del escaneo en el expediente técnico del proyecto, conforme a lo indicado en el apartado ***PTC-AVF-001***.

Asimismo, para garantizar la confidencialidad de los datos personales durante las fases de desarrollo y prueba, se prohíbe el uso de datos reales en estos entornos sin autorización expresa del Departamento Legal y de TI. En caso de ser necesario, el proveedor deberá aplicar mecanismos de **enmascaramiento u ofuscación de los datos sensibles**, asegurando que no puedan ser asociados a personas identificables. Estas acciones deberán documentarse en un informe técnico que detalle el método aplicado, la fecha de ejecución, el responsable y evidencia visual del tratamiento, el cual se archivará como parte del expediente del proyecto.

OBTENCIÓN DEL CONSENTIMIENTO DEL USUARIO

Todo tratamiento de datos personales en un desarrollo web debe estar precedido por la obtención del consentimiento informado del usuario. Este consentimiento debe ser libre, previo, específico, informado y verificable, conforme a lo establecido en la Ley Nº8968. Su ausencia invalida cualquier proceso de recolección de datos personales y puede generar responsabilidades legales para la organización.

El consentimiento deberá integrarse en los formularios o puntos de captura de información mediante los siguientes mecanismos obligatorios:

- **Texto visible y comprensible** que indique de manera clara qué datos se están recolectando, para qué fin y quién será el responsable de su tratamiento.

- **Casilla de aceptación (checkbox) obligatoria**, no preseleccionada, con un mensaje como: “He leído y acepto la política de privacidad y tratamiento de datos personales”.
- **Enlace a la política de privacidad** que detalle las condiciones del tratamiento, incluyendo el uso de cookies, tiempos de retención y derechos del titular.
- **Registro de consentimiento** como parte de la evidencia técnica. El proveedor deberá incluir evidencia del consentimiento otorgado (por ejemplo, mediante logs o almacenamiento vinculado al registro).

El contenido exacto del mensaje de consentimiento, así como su redacción legal, deberá ser validado previamente por el Departamento Legal de la Cooperativa, como parte del proceso formal de aprobación del desarrollo web.

GESTIÓN DE COOKIES Y TECNOLOGÍAS DE SEGUIMIENTO

Todo desarrollo web subcontratado que utilice cookies o tecnologías de rastreo deberá implementar mecanismos que garanticen la transparencia, consentimiento informado y control por parte del usuario. Estas tecnologías, utilizadas comúnmente para fines analíticos, publicitarios o funcionales, deben gestionarse de manera que respeten la privacidad del usuario y cumplan con los principios establecidos en la Ley Nº8968.

Las agencias proveedoras deberán garantizar la implementación de una solución que permita al usuario:

- Ser informado de forma clara y accesible sobre el uso de cookies, su propósito y tipo.
- Otorgar o rechazar su consentimiento antes de que las cookies no esenciales sean activadas.
- Modificar o revocar su consentimiento en cualquier momento durante la navegación.
- Acceder a un aviso de cookies vinculado a la política de privacidad.

El banner o herramienta de gestión de cookies deberá presentarse desde el primer ingreso al sitio, sin que ninguna cookie no esencial (por ejemplo, rastreo de comportamiento o marketing) sea activada por defecto. La herramienta debe registrar la decisión del usuario como parte de la evidencia técnica del consentimiento.

En todos los casos, la configuración y los textos incluidos en el aviso de cookies deberán ser aprobados previamente por el Departamento Legal, con el respaldo del Departamento de TI y en coordinación con Mercadeo.

PROCEDIMIENTO PARA LA ATENCIÓN DE SOLICITUDES SOBRE DATOS PERSONALES

Todo usuario tiene derecho a solicitar el acceso, la rectificación o la eliminación de sus datos personales cuando hayan sido recolectados mediante los desarrollos web de la Cooperativa. Este derecho está respaldado por el Artículo 12 de la Ley Nº8968, que faculta a las organizaciones a definir protocolos internos para garantizar la trazabilidad y la protección de la información personal.

Con el fin de atender de forma oportuna y segura estas solicitudes, el proveedor deberá habilitar un mecanismo visible desde la misma página donde se recolectan los datos, ya sea mediante un formulario de contacto, un enlace a una política de privacidad con instrucciones claras, o una vía directa de comunicación habilitada para este fin.

El procedimiento debe cumplir con las siguientes condiciones:

- **Confirmación de identidad del solicitante:** Se realizará a través de mecanismos razonables que no expongan al usuario a procesos complejos ni inseguros.
- **Trazabilidad del caso:** Se procederá con el registro de la fecha, motivo de la solicitud, acciones realizadas y resolución aplicada.
- **Tiempo máximo de respuesta:** Se establecerá un período no mayor de 10 días hábiles desde la recepción formal de la solicitud.
- **Participación del Departamento de TI y Legal:** En casos donde se requiera validación adicional o eliminación técnica definitiva de la información.

Las evidencias del cumplimiento de este procedimiento deberán integrarse al expediente técnico del proyecto, conforme a lo indicado en el ***Protocolo de aprobación y validación final de los desarrollos web (PTC-AVF-001).*** La solicitud deberá gestionarse mediante un formulario digital redirigido al Centro de Contactos de la Cooperativa o por medio de contacto directo a través de los canales oficiales: centrodecontactos@dospinos.com o al número telefónico +506 2508-2525.

Historial de versiones de la normativa:

Tabla 8
Detalle de versiones de la normativa

Versión	Fecha	Descripción del cambio	Responsable
1.0	03/07/2025	Versión inicial de la normativa. Incluye objetivo, alcance, fundamento legal, principios, consentimiento informado, gestión de cookies, atención de solicitudes y trazabilidad técnica.	Johan Vega
1.2			
1.3			

Fuente: *Vega, 2025.*

APÉNDICE D

Directriz de evaluación y análisis dinámico de seguridad

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

DIRECTRIZ DE EVALUACIÓN Y ANÁLISIS DINÁMICO DE SEGURIDAD

JOHAN VEGA CÓRDOBA

JUNIO, 2025

INTRODUCCIÓN

La ejecución de pruebas de seguridad en los desarrollos web utilizados o creados para campañas publicitarias resulta esencial para mitigar riesgos antes de su publicación. En contextos donde las agencias externas o proveedores subcontratados realizan estas implementaciones, se vuelve necesario establecer directrices claras que permitan asegurar la integridad, confidencialidad y disponibilidad de los sistemas involucrados.

Este apartado define lineamientos específicos para la realización de evaluaciones dinámicas de seguridad, orientadas a detectar y mitigar vulnerabilidades técnicas en aplicaciones web, formularios de captura, sistemas de autenticación u otros componentes susceptibles a amenazas. Asimismo, se abordan los procedimientos fundamentales para documentar adecuadamente los hallazgos, implementar medidas de mitigación previas al lanzamiento del desarrollo y actualizar los criterios de análisis conforme a nuevas exigencias normativas o amenazas emergentes.

Estas directrices se fundamentan en los controles A.8.25 y A.8.29 de la norma ISO/IEC 27001:2022, así como en los artículos 6 y 12 de la Ley Nº8968, a fin de garantizar un nivel adecuado de seguridad técnica y cumplimiento legal en el tratamiento de datos personales.

OBJETIVOS

Establecer un conjunto de directrices para la evaluación dinámica de seguridad en los desarrollos web implementados por proveedores externos para campañas publicitarias de la Cooperativa de Productores de Leche Dos Pinos. Esta directriz busca garantizar la identificación temprana de vulnerabilidades técnicas antes de la publicación de los sitios, mediante la ejecución de pruebas, el uso de herramientas reconocidas y la aplicación de criterios mínimos de análisis.

Asimismo, se normará la documentación técnica de los hallazgos detectados, las acciones de mitigación aplicadas y la trazabilidad del cumplimiento de los controles de seguridad. Finalmente, se definirá un protocolo de actualización continua que permita incorporar nuevos criterios de evaluación conforme surjan amenazas emergentes, con base en lo establecido por la norma ISO/IEC 27001:2022 y la Ley Nº8968 sobre protección de datos personales.

ALCANCE

Esta directriz aplica a todos los desarrollos web subcontratados por el Departamento de Mercadeo de la Cooperativa de Productores de Leche Dos Pinos, incluidos landing pages, micrositios, formularios digitales y cualquier componente en línea diseñado como parte de alguna campaña publicitaria.

Su aplicación es obligatoria para todas las agencias externas o proveedores encargados del desarrollo, y podrá ser supervisada por el área de Tecnologías de Información cuando así se requiera. Estas disposiciones deberán cumplirse previo al despliegue de los desarrollos en entornos productivos o visibles al público general.

FUNDAMENTACIÓN NORMATIVA Y PRÁCTICAS APLICABLES

Las presentes directrices se sustentan en el cumplimiento de controles establecidos por la norma ISO/IEC 27001:2022 y disposiciones de la Ley Nº8968, con el objetivo de asegurar la integridad, disponibilidad y confidencialidad de la información procesada durante el desarrollo y despliegue de sitios web para campañas publicitarias.

Los controles aplicables son:

ISO/IEC 27001:2022

- **A.8.25 – Ciclo de vida de desarrollo seguro:** Establece la necesidad de integrar medidas de seguridad en todas las fases del desarrollo, incluyendo la planificación, codificación, prueba y mantenimiento de las aplicaciones web.
- **A.8.29 – Pruebas de seguridad:** Requiere la ejecución de pruebas de seguridad sistemáticas que permitan identificar vulnerabilidades técnicas antes de poner en funcionamiento los sistemas.

Ley N. ª 8968 – Protección de la persona frente al tratamiento de sus datos personales:

- **Artículo 6 – Principio de calidad de la información:** Dispone que los datos recolectados deben ser veraces, actualizados y adecuados al propósito de su tratamiento.
- **Artículo 12 – Seguridad del tratamiento de los datos personales:** Obliga a implementar medidas técnicas que prevengan el acceso no autorizado, alteración, pérdida o tratamiento indebido de los datos personales gestionados.

ESTÁNDARES DE PRUEBAS DE SEGURIDAD DINÁMICA

Con el fin de identificar vulnerabilidades técnicas antes del lanzamiento de los desarrollos web subcontratados, se establece un conjunto mínimo de pruebas de seguridad dinámica que deberán ejecutarse en distintas etapas del ciclo de desarrollo. Estas pruebas tienen como objetivo anticipar fallos que puedan comprometer la confidencialidad, integridad o disponibilidad de la información, así como evitar incidentes que afecten a los usuarios finales.

Las pruebas deberán ser realizadas por el proveedor o la agencia responsable, utilizando herramientas reconocidas en la industria. Los resultados deberán documentarse formalmente y servir como requisito previo para la aprobación de los desarrollos.

A continuación, se describen los tipos mínimos de prueba requeridos, organizados por etapas del ciclo de desarrollo:

1. **Pruebas durante el desarrollo (ambiente controlado):**

Tipo de prueba	Objetivo principal	Herramienta sugerida	Responsable
Simulación de ataques XSS	Detectar inserción de scripts maliciosos en campos de entrada (OWASP A03)	OWASP ZAP	Proveedor
Validación de autenticación	Evaluar robustez de mecanismos de login y gestión de sesiones (OWASP A07)	Herramientas propias / ZAP	Proveedor

Estas pruebas buscan prevenir ataques que se aprovechan de formularios mal configurados y sesiones de usuario vulnerables. Estas validaciones ayudan a detectar errores comunes que podrían comprometer la experiencia de navegación o permitir el acceso indebido a interfaces administrativas.

2. **Pruebas en fase final de desarrollo (Previo a QA):**

Tipo de prueba	Objetivo principal	Herramienta sugerida	Responsable
Escaneo de vulnerabilidades	Identificar puertos abiertos, configuraciones inseguras o servicios expuestos	OWASP ZAP, Nessus, Acunetix	Proveedor
Análisis de cabeceras HTTP	Validar políticas de seguridad en servidor web (CSP, HSTS, etc.)	SecurityHeaders, SSL Labs	Proveedor

En esta etapa se realizan validaciones más técnicas sobre la infraestructura web y la configuración del servidor. Estas pruebas permiten detectar brechas de seguridad que no son visibles desde el frontend, pero que pueden ser explotadas por atacantes con herramientas más automatizadas.

3. **Pruebas antes del paso a producción (QA Final):**

Tipo de prueba	Objetivo principal	Herramienta sugerida	Responsable
Pruebas de inyección SQL/HTML	Validar que entradas de datos no permitan comandos maliciosos (OWASP A01)	OWASP ZAP, Burp Suite	Proveedor

Por último, antes de liberar el desarrollo al entorno productivo, se debe comprobar que no existan entradas vulnerables que permitan alterar el funcionamiento del desarrollo o acceder a información sensible.

Todas las pruebas deben ejecutarse como requisito previo al despliegue final del desarrollo. La ausencia de estas validaciones o la falta de documentación técnica correspondiente será motivo suficiente para detener su publicación hasta que se acredite el cumplimiento del estándar.

DOCUMENTACIÓN DE HALLAZGOS Y MITIGACIÓN

Todos los hallazgos identificados durante las pruebas de seguridad dinámica deberán ser documentados formalmente por el proveedor responsable, previo al lanzamiento de los desarrollos web. Esta documentación permitirá establecer trazabilidad, verificar la aplicación de medidas correctivas y garantizar la protección de los datos personales tratados.

El informe entregado deberá contener, como mínimo, los siguientes elementos por cada vulnerabilidad detectada:

- Descripción técnica de la vulnerabilidad
- Evidencia de su existencia (captura, log o reporte)
- Clasificación del nivel de riesgo
- Medida de mitigación aplicada
- Estado final (resuelto / pendiente con justificación)
- Fecha de resolución
- Nombre del responsable técnico

La clasificación del nivel de riesgo deberá basarse en criterios reconocidos, como el marco OWASP Top Ten y los principios de impacto definidos por la norma ISO/IEC 27001, permitiendo priorizar la atención de vulnerabilidades críticas y garantizar su resolución previa al paso a producción.

La verificación de esta documentación será responsabilidad del área de Mercadeo. El departamento deberá asegurar la entrega y resguardo del informe técnico por parte del proveedor. Cuando se identifiquen hallazgos de alta criticidad, o se requiera validación técnica adicional, el Departamento de Tecnologías de Información podrá brindar apoyo en la revisión de evidencias, sin asumir responsabilidad directa sobre el cumplimiento.

Para complementar el control documental, se incluye una matriz de identificación y clasificación de riesgos técnicos, la cual permite visualizar las principales vulnerabilidades detectadas, su nivel de severidad, impacto y estado. Este documento debe ser entregado junto con el informe técnico como evidencia consolidada del proceso de revisión.

Objetivo del informe:

Registrar de manera estructurada las vulnerabilidades técnicas identificadas durante las pruebas de seguridad dinámica realizadas en los desarrollos web subcontratados, así como su nivel de riesgo, impacto, acciones correctivas y estado de mitigación.

Instrucciones importantes:

- Este documento debe ser completado por el proveedor una vez finalizadas las pruebas de seguridad dinámica.
- Por cada vulnerabilidad detectada, se deben registrar los datos solicitados en la matriz, clasificando el nivel de riesgo, el impacto y el estado de mitigación.
- La matriz debe ser entregada como complemento del informe técnico descrito en este procedimiento, el cual contiene las evidencias detalladas, medidas aplicadas y demás elementos requeridos por el apartado.
- La Cooperativa se reserva el derecho de solicitar validación adicional al Departamento de TI en caso de hallazgos críticos o inconsistencias.

Clasificación del riesgo:

La clasificación del nivel de riesgo deberá basarse en uno de los siguientes criterios:

- OWASP Top Ten, como referencia de vulnerabilidades críticas en aplicaciones web.
- CVSS, mediante herramientas que asignen puntuaciones automáticas al hallazgo.

En caso de no aplicar estos métodos, el proveedor podrá justificar el nivel de riesgo con base en el impacto funcional del hallazgo. Por ejemplo:

- Acceso a información sensible o datos personales → riesgo crítico.
- Afectación menor en componentes no expuestos → riesgo medio o bajo, con justificación técnica.

El proveedor es responsable de indicar y justificar el criterio utilizado. La Cooperativa podrá solicitar validación adicional al Departamento de TI en caso de inconsistencias o auditorías.

Matriz de identificación y clasificación de riesgos técnicos:

A continuación, se ejemplifica la forma correcta de documentar cada vulnerabilidad detectada en las pruebas.

Código	Vulnerabilidad detectada	Descripción técnica	Nivel de riesgo	Impacto potencial	Medida de mitigación	Estado
V-01	Inyección SQL	Manipulación de sentencias en campos de entrada	Crítico	Acceso a base de datos	Validación de entradas y consultas preparadas	Mitigado
V-02	XSS persistente	Código ejecutable almacenado sin control	Alto	Robo de sesión o redirecciones	Filtro de salida + políticas CSP	Mitigado
V-03	Sesión sin expiración	La sesión permanece activa indefinidamente	Medio	Suplantación de usuario	Definición de tiempo de expiración	Pendiente

Este matriz se encuentra disponible en formato editable en línea para facilitar su uso y archivo digital. Puede acceder al documento mediante el siguiente enlace: Matriz de riesgos

RESPONSABLES

Para asegurar la ejecución correcta de las pruebas de seguridad dinámica y el cumplimiento del procedimiento establecido, se definen los siguientes roles y responsabilidades:

Proveedor o agencia externa:

- Ejecutar las pruebas de seguridad dinámica conforme a los estándares descritos en la presente directriz.
- Documentar cada hallazgo técnico mediante un informe estructurado que contenga evidencias, clasificación de riesgo, medidas aplicadas y estado final.
- Completar y entregar la matriz de riesgos técnicos como parte del expediente del proyecto.
- Implementar las acciones correctivas necesarias antes del paso a producción.

Departamento de Mercadeo (responsable del proyecto):

- Solicitar formalmente al proveedor la realización de las pruebas de seguridad.
- Verificar que la documentación técnica y la matriz de riesgos hayan sido entregadas de forma completa y oportuna.
- Resguardar dicha documentación como parte del expediente digital del proyecto.
- Escalar los hallazgos críticos o casos especiales al Departamento de Tecnologías de Información, cuando corresponda.

Departamento de Tecnologías de Información (TI)

- Brindar apoyo técnico en la revisión de hallazgos cuando se requiera validación especializada.
- Colaborar en auditorías internas que soliciten la verificación de evidencias técnicas relacionadas con la seguridad.

PROTOCOLO DE ACTUALIZACIÓN

Con el objetivo de mantener vigente esta directriz ante la evolución de amenazas, tecnologías o cambios normativos, se establece el siguiente protocolo de revisión y actualización:

- La presente directriz deberá ser revisada al menos una vez al año por el Departamento de Tecnologías de Información, en coordinación con el Departamento de Mercadeo.
- También podrá actualizarse de forma extraordinaria cuando se presenten nuevas amenazas relevantes, modificaciones en los controles de la norma ISO/IEC 27001o reformas aplicables a la Ley Nº8968.
- Toda actualización deberá reflejarse en el historial de versiones del documento, incluyendo la descripción de los cambios y su validación por parte del responsable correspondiente.

Este protocolo busca asegurar que las directrices aquí establecidas se mantengan alineadas con los requerimientos técnicos y regulatorios, protegiendo de forma continua la información tratada en los desarrollos web de la Cooperativa.

Historial de versiones de la directriz:

Versión	Fecha	Descripción del cambio	Responsable
1.0	06/06/2025	Versión inicial de la directriz. Incluye objetivo, alcance, normativa, estándares a cumplir, documentación solicitada, responsables de ejecutar y protocolo de actualización.	Johan Vega
1.2			
1.3			

APÉNDICE E

Normativa de verificación mediante checklist de seguridad

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

NORMATIVA DE VERIFICACIÓN MEDIANTE CHECKLIST DE SEGURIDAD

JOHAN VEGA CÓRDOBA

JUNIO, 2025

INTRODUCCIÓN

Los desarrollos web contratados por el Departamento de Mercadeo, especialmente aquellos utilizados en campañas publicitarias, deben ser evaluados bajo criterios que garanticen el cumplimiento de los requisitos mínimos de seguridad antes de su publicación. Para estandarizar este proceso, se establece una normativa interna que obliga al uso de listas de verificación (checklists) como herramienta de control previo.

Esta normativa define la aplicación obligatoria de un checklist de seguridad que deberá ser completado por el proveedor y validado por el área solicitante, en este caso el departamento de Mercadeo. Su implementación busca garantizar que cada desarrollo sea evaluado conforme a los requisitos establecidos por la Cooperativa, en cumplimiento con los principios de la norma ISO/IEC 27001 y la Ley Nº8968.

OBJETIVO

Formular una normativa interna que estandarice y regule el proceso de verificación de seguridad en los desarrollos web subcontratados por el departamento de Mercadeo, mediante el uso obligatorio de un checklist técnico que permita validar el cumplimiento de los requisitos definidos por la Cooperativa antes de su publicación. Esta normativa tiene como finalidad garantizar que todos los entregables sean evaluados bajo los mismos criterios, contribuyendo así a la correcta protección de los datos tratados y la reducción de riesgos asociados a vulnerabilidades que puedan afectar el proyecto.

ALCANCE

La presente normativa aplica a todos los desarrollos web subcontratados por el Departamento de Mercadeo de la Cooperativa, orientados a campañas publicitarias, formularios de captación de datos, activaciones comerciales u otras iniciativas digitales que involucren landing pages, micrositios o plataformas web de carácter promocional.

Este lineamiento es de aplicación obligatoria para los proveedores encargados de la ejecución técnica, quienes deberán completar el checklist de seguridad previo a la entrega del desarrollo. Asimismo, es responsabilidad del personal del Departamento de Mercadeo exigir el cumplimiento del checklist, verificar su contenido y remitirlo al Departamento de Tecnologías de Información como parte del expediente técnico del proyecto.

La existencia y revisión de este checklist es un requisito solicitado por el Departamento de TI para aprobar la publicación de cualquier desarrollo web subcontratado, en función de los controles definidos en la política de seguridad de la Cooperativa. Aunque esta normativa es impulsada desde Mercadeo, responde a una necesidad institucional de asegurar que los desarrollos externos cumplan con las medidas mínimas de protección de la información basados en las buenas prácticas y normativas como la ISO270001 que regulan la protección y la integridad de la información.

Quedan excluidos de esta normativa los desarrollos internos gestionados directamente por TI, los cuales se rigen por sus propios procedimientos técnicos.

FUNDAMENTACIÓN NORMATIVA

La presente normativa se fundamenta en el cumplimiento de controles técnicos y organizacionales establecidos por la norma internacional ISO/IEC 27001:2022, así como en el marco legal definido por la Ley Nº8968, Protección de la persona frente al tratamiento de sus datos personales.

Desde la perspectiva de seguridad de la información, se consideran especialmente relevantes los siguientes controles del Anexo A:

- **A.5.36 – Cumplimiento de políticas y normas de seguridad de la información:** Exige que las organizaciones implementen mecanismos para asegurar que sus políticas y normas de seguridad sean aplicadas en la práctica. El checklist actúa como una herramienta verificable que permite evidenciar dicho cumplimiento antes de la publicación de desarrollos web.
- **A.6.8 – Reportes de eventos de seguridad de la información:** Establece la necesidad de contar con procesos para informar hallazgos o eventos que puedan comprometer la seguridad. El uso del checklist permite identificar posibles desviaciones o incumplimientos que deben ser notificados y tratados.

Desde el punto de vista legal, la propuesta se ampara en el artículo 12 de la Ley Nº8968, el cual habilita a las personas físicas y jurídicas a emitir protocolos de actuación para regular los procesos de recolección, almacenamiento y manejo de datos personales. Esta normativa, y en particular el checklist que se incorpora, constituye un componente de dicho protocolo, permitiendo dejar constancia de que el desarrollo fue verificado conforme a criterios técnicos antes de su puesta en línea.

ESTRUCTURA Y CONTENIDO DEL CHECKLIST DE SEGURIDAD

Este checklist constituye una herramienta obligatoria para todos los desarrollos web subcontratados por el Departamento de Mercadeo. Su función principal es estandarizar la evaluación de requisitos técnicos y normativos antes de que cualquier landing page, micrositio o formulario sea aprobado para su publicación.

Este instrumento debe ser completado por el proveedor responsable del desarrollo, revisado por el solicitante del proyecto en Mercadeo (ejecutivo líder), y posteriormente remitido al Departamento de Tecnologías de Información como parte del expediente técnico del proyecto.

A continuación, se describen los elementos mínimos que debe contener el checklist, agrupados en cuatro categorías clave:

Tabla 9
Validación general del entorno

Item	Descripción
Separación de ambientes	Verificar que el entorno de desarrollo y el entorno productivo estén completamente separados.
Versión final publicada	Confirmar que, el entorno de producción corresponde con la versión revisada y validada.
Eliminación de versiones de prueba	Asegurar que, versiones preliminares no estén expuestas públicamente.

Tabla 10
Control de acceso y credenciales

Item	Descripción
Protección mediante autenticación	Validar que los formularios con acceso a datos estén protegidos por mecanismos de autenticación, si corresponde.
Gestión de usuarios	Confirmar que, no existen usuarios genéricos o temporales activos en el entorno final.
Contraseñas guardadas	Verificar el uso de contraseñas con niveles mínimos de complejidad, si aplica.

Tabla 11
Protección de datos y tratamiento seguro

Item	Descripción
Recolección mínima de datos	Validar que los formularios recojan únicamente los datos estrictamente necesarios.
Uso de HTTPS	Confirmar que, todo el sitio opere bajo protocolo seguro (SSL/TLS).
Políticas visibles	Comprobar la presencia de enlaces visibles a políticas de privacidad y condiciones de uso.

Tabla 12
Validación técnica previa al despliegue

Item	Descripción
Revisión del Código Fuente	Confirmar que, el código fue validado conforme a lo establecido en el ***PROCESO DE VALIDACIÓN DE LA CALIDAD Y SEGURIDAD DE LOS DESARROLLOS WEB EN CUANTO A CÓDIGO FUENTE, ACCESOS Y CIFRADO*** (PR-VCS-001)**.**
Pruebas de seguridad aprobadas	Verificar que se ejecutaron las pruebas definidas en la ***DIRECTIZ DE EVALUACIÓN Y ANÁLISIS DINÁMICA DE SEGURIDAD*** **(**DR-EADS-001), incluyendo escaneos, análisis dinámicos o pruebas manuales.
Corrección de hallazgos	Confirmar que, no existan vulnerabilidades abiertas al momento del lanzamiento.

Al cierre del documento, el checklist debe incluir:

- Firma o confirmación del proveedor.
- Validación del área solicitante (Mercadeo).
- Fecha de revisión y observaciones, si las hubiera.

Este checklist actúa como una herramienta transversal que consolida el cumplimiento de distintas directrices definidas por la Cooperativa. Su aplicación permite verificar que el desarrollo web ha seguido los lineamientos técnicos establecidos en la ***Directriz para la validación del código fuente, la Directriz de evaluación y análisis dinámico de seguridad y otros procesos*** vinculados a la protección de datos y control de accesos.

El formato completo del checklist se deja disponible como anexo digital editable, a través del siguiente enlace: Checklist_Verificacion_Seguridad

PROCESO DE VALIDACIÓN MEDIANTE CHECKLIST

La aplicación de este instrumento es obligatoria como parte del proceso de revisión y aprobación de los desarrollos web subcontratados por el Departamento de Mercadeo. Su propósito es asegurar que los entregables hayan sido evaluados conforme a los requisitos técnicos establecidos por la Cooperativa antes de su publicación.

El proceso se compone de las siguientes cinco etapas:

1. **Finalización del desarrollo:** El proveedor culmina el desarrollo de la landing page, micrositio o formulario, siguiendo las especificaciones técnicas y normativas aplicables. Esta etapa ocurre antes del despliegue en el entorno productivo, y da inicio al proceso formal de validación mediante checklist.
2. **Aplicación del checklist:** El proveedor completa el checklist de verificación de seguridad, marcando cada ítem correspondiente y agregando observaciones en caso necesario. El checklist debe reflejar el cumplimiento de las directrices técnicas establecidas.
3. **Revisión por parte del Departamento de Mercadeo:** El responsable del proyecto en Mercadeo valida el contenido del checklist, asegura su completitud y verifica que no existan pendientes o vulnerabilidades sin resolver.
4. **Remisión al Departamento de TI:** El checklist validado debe ser enviado al Departamento de Tecnologías de Información junto con el expediente técnico del proyecto, como condición previa para su aprobación final.
5. **Validación técnica final (cuando aplica):** El Departamento de TI podrá realizar una revisión técnica complementaria en caso de hallazgos críticos, solicitudes especiales o auditorías. Su participación garantiza la trazabilidad y respaldo del proceso.

RESPONSABLES

La correcta aplicación de esta herramienta depende de la coordinación entre los distintos actores involucrados en el desarrollo y publicación de sitios web. A continuación, se detallan las responsabilidades asignadas a cada parte:

Proveedor externo del desarrollo:

- Completar el checklist correctamente una vez finalizado el desarrollo.
- Adjuntar evidencia técnica correspondiente (capturas, enlaces funcionales, reportes, etc.).
- Asegurar que, todos los ítems hayan sido debidamente abordados antes de la entrega final.

Departamento de Mercadeo:

- Solicitar al proveedor el cumplimiento del checklist como parte del proceso de cierre del proyecto.
- Revisar y validar que el checklist esté completo, consistente y alineado con los requisitos definidos.
- Remitir el checklist validado al Departamento de Tecnologías de Información junto con el expediente del proyecto.

Departamento de Tecnologías de Información:

- Verificar el cumplimiento técnico del checklist, cuando aplique, como parte del proceso de aprobación previo a la publicación.
- Solicitar aclaraciones o validaciones adicionales si se detectan inconsistencias o vacíos técnicos.
- Archivar el checklist como evidencia de cumplimiento para fines de auditoría interna o requerimientos regulatorios.

Historial de versiones de la normativa:

Versión	Fecha	Descripción del cambio	Responsable
1.0	12/06/2025	Versión inicial de la normativa. Contempla el objetivo general, alcance definido, fundamento normativo aplicable, criterios obligatorios del checklist, proceso de validación, roles asignados	Johan Vega
1.2			
1.3			

APÉNDICE F

Protocolo de aprobación y validación final de los desarrollos web

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

PROTOCOLO DE APROBACIÓN Y VALIDACIÓN FINAL DE LOS DESARROLLOS WEB

JOHAN VEGA CÓRDOBA

JUNIO, 2025

Cooperativa de Productores de Leche Dos Pinos R.L.		Código: PTC-AVF-001
PROTOCOLO DE APROBACIÓN Y VALIDACIÓN FINAL DE LOS DESARROLLOS WEB		Versión 1
Realizado por: Johan Vega Córdoba	Departamento de Mercadeo	Página de 1 de 12

INTRODUCCIÓN

Una vez finalizado el desarrollo de un sitio web subcontratado, es imprescindible contar con un protocolo que permita validar, de forma técnica y documental, que dicho proyecto cumple con todos los estándares de seguridad, normativas legales y lineamientos institucionales definidos previamente. La ausencia de un proceso estructurado para esta validación final puede derivar en la publicación de soluciones con grandes vulnerabilidades activas, un manejo inadecuado de datos personales o falta de trazabilidad operativa.

Este protocolo establece los pasos obligatorios que deben seguirse antes de aprobar cualquier desarrollo web realizado por proveedores externos, garantizando que la revisión técnica por parte del Departamento de Tecnologías de Información y la verificación complementaria del Departamento de Mercadeo se ejecuten de forma coordinada y documentada. De esta forma, se asegura que toda solución digital publicada en nombre de la Cooperativa cumpla con los principios de seguridad, calidad y responsabilidad institucional.

OBJETIVO

Establecer un protocolo formal que regule el proceso de aprobación y validación final de los desarrollos web subcontratados por el Departamento de Mercadeo, con el fin de garantizar que ningún proyecto sea publicado sin haber cumplido previamente con todos los controles de seguridad, requisitos normativos y entregables documentales definidos por la Cooperativa. Este protocolo busca asegurar la trazabilidad, calidad y conformidad técnica de las soluciones digitales, fortaleciendo el cumplimiento institucional y la protección de la información gestionada.

ALCANCE

El presente protocolo es de aplicación obligatoria para todos los desarrollos web gestionados por el Departamento de Mercadeo que sean realizados por proveedores externos, tales como sitios, micrositios, formularios digitales, encuestas interactivas y plataformas temporales vinculadas a campañas publicitarias, promociones o estrategias institucionales.

Su aplicación inicia una vez que el proveedor ha completado el desarrollo técnico y debe realizar la entrega formal del proyecto. El protocolo debe ser ejecutado antes de cualquier despliegue en producción o puesta en línea del sitio, como parte del flujo de cierre técnico y aprobación funcional del proyecto.

Están sujetos a este protocolo:

- Los proveedores externos, quienes deberán entregar el checklist oficial, documentación técnica y evidencias requeridas.
- El Departamento de Mercadeo, como unidad solicitante, encargado de revisar la entrega, completar el expediente y coordinar con TI.
- El Departamento de Tecnologías de Información, responsable de validar los aspectos técnicos, verificar cumplimiento normativo y autorizar el paso a producción.

La validación final contemplada en este protocolo representa el último filtro de calidad, seguridad y cumplimiento antes de que el desarrollo sea accesible para usuarios internos o externos, por lo que su cumplimiento será condición indispensable para toda publicación.

FUNDAMENTO NORMATIVO

La implementación del presente protocolo se sustenta en disposiciones legales y estándares internacionales que exigen a las organizaciones contar con mecanismos formales para validar la conformidad técnica y documental de sus procesos antes de su ejecución o puesta en marcha. En el contexto de los desarrollos web subcontratados, esta validación previa garantiza el cumplimiento de los principios de seguridad, legalidad y trazabilidad definidos por la Cooperativa.

A continuación, se detallan los artículos y controles específicos que respaldan normativamente este procedimiento:

Ley Nº8968 – Protección de la Persona frente al Tratamiento de sus Datos Personales

- Artículo 12: Este artículo faculta a las organizaciones a emitir protocolos internos que regulen los pasos a seguir en la recolección, almacenamiento y manejo de datos personales, en conformidad con la normativa vigente. En este contexto, el presente protocolo actúa como medida formal de control y validación, garantizando que ningún desarrollo web sea publicado sin revisión técnica previa.

Normativa internacional aplicable: Norma ISO/IEC 27001:2022

- Control A.5.1 – Políticas de seguridad de la información: Exige que la organización defina, apruebe y mantenga políticas que establezcan los objetivos de seguridad, alineadas con el marco legal y los riesgos identificados. Este control respalda la creación de esta política como instrumento formal de dirección.
- Control A.5.36 – Cumplimiento con normas y políticas: Señala la necesidad de asegurar que las actividades organizacionales estén alineadas con políticas, reglas y estándares vigentes. En el caso de Dos Pinos, esto implica garantizar que proveedores y personal interno trabajen conforme a los estándares definidos y actualizados periódicamente.
- Control A.6.18– Políticas de seguridad de la información: Este control exige la existencia de mecanismos formales para la documentación, reporte y seguimiento de eventos de seguridad. En este protocolo, cualquier hallazgo técnico detectado durante la revisión por parte de TI deberá quedar registrado como parte del expediente del desarrollo, asegurando trazabilidad, respuesta y eventual mitigación.

PROCESO DE APROBACIÓN Y VALIDACIÓN FINAL

La aprobación y publicación de cualquier desarrollo web subcontratado requiere completar una serie de pasos obligatorios que permitan validar su calidad técnica, cumplimiento normativo y trazabilidad documental. Este proceso debe ejecutarse una vez finalizado el desarrollo, como condición previa a su despliegue en producción.

A continuación, se describen las etapas del proceso:

1. **Finalización técnica y entrega formal**

El proveedor deberá entregar al Departamento de Mercadeo los siguientes elementos:

- Desarrollo funcional completo alojado en un entorno pre productivo accesible para revisión por parte de TI y Mercadeo.
- Checklist de verificación de seguridad ***(NTV-CDS-001)*** debidamente completado, en su versión institucional oficial.
- Evidencia técnica de cumplimiento, que deberá incluir como mínimo:
    - Capturas de pantalla de configuraciones clave (control de acceso, HTTPS, headers de seguridad, roles asignados, etc.).
    - URL funcional del entorno de pruebas con acceso temporal para revisión.
    - Consola de validación del navegador (para comprobar certificados, cookies seguras, CSP u otras cabeceras).
    - Resultados de escaneos o pruebas de seguridad realizadas, cuando aplique.
    - Justificación técnica del nivel de riesgo asignado a cada hallazgo detectado, en caso de vulnerabilidades.
    - Evidencia de la política de privacidad visible o documentación del consentimiento, si se recolectan datos personales.

- Documentación complementaria relacionada con el tratamiento de datos personales, según los criterios definidos en la ***Política de cumplimiento normativo y actualización de estándares (PCN-AE-001)***

2. **Validación funcional por parte de Mercadeo**

Mercadeo verificará que el entregable cumpla con los objetivos funcionales del proyecto, que la documentación esté completa y organizada, y que se incluya todo lo necesario para su revisión técnica. Una vez validado internamente, Mercadeo remitirá el expediente al Departamento de Tecnologías de Información para su revisión técnica final.

3. **Revisión técnica por parte del Departamento de TI**

El departamento como área experta y líder evaluará los siguientes puntos:

- La integridad y veracidad del Checklist de verificación de seguridad ***(NTV-CDS-001).***
- El cumplimiento de los controles técnicos definidos en el Procedimiento técnico para la validación del código, control de accesos y cifrado de datos ***(PR-VCS-001).***
- La incorporación de criterios y resultados establecidos en la Directriz de evaluación y análisis dinámico de seguridad ***(DR-EADS-001)***, incluyendo pruebas dinámicas y mitigación de vulnerabilidades.
- La aplicación de la Política de cumplimiento normativo y actualización de estándares ***(PCN-AE-001)*** en lo referente al tratamiento de datos personales.

Cualquier hallazgo o incumplimiento será devuelto a Mercadeo para que gestione la corrección con el proveedor antes de continuar con el proceso.

4. **Comunicación de aprobación**

Una vez verificado el cumplimiento técnico y documental, el Departamento de TI emitirá una aprobación formal a Mercadeo. Esta aprobación será condición necesaria para proceder con la publicación del desarrollo en el entorno productivo institucional.

5. **Archivo del expediente**

Mercadeo será responsable de archivar todos los documentos relacionados en el expediente del proyecto. Este expediente deberá incluir:

- El checklist aprobado.
- Las evidencias técnicas.

- La aprobación formal de TI.
- Cualquier observación, validación o solicitud de ajuste emitida durante el proceso.

Este archivo constituirá la base documental para fines de auditoría, trazabilidad institucional y mejora continua de procesos futuros. Como parte de este expediente, se deberá completar y archivar el ***Formulario de validación final – Proyectos web subcontratados*** (ver Anexo 1), el cual permite verificar formalmente el cumplimiento de los entregables definidos en este protocolo.

EVIDENCIA Y TRAZABILIDAD DOCUMENTAL

Como parte del cierre del proceso de validación final, es obligatorio conservar un respaldo documental que permita demostrar el cumplimiento de los criterios técnicos y normativos definidos para la publicación de desarrollos web subcontratados. Este respaldo constituye la principal evidencia institucional ante auditorías internas o externas, y fortalece la trazabilidad de cada proyecto.

Las evidencias que deben ser archivadas incluyen, como mínimo:

- El Checklist de verificación de seguridad ***(NTV-CDS-001)***, firmado por el proveedor y validado por TI.
- Las evidencias técnicas del cumplimiento de controles, incluyendo capturas, configuraciones, enlaces, y justificaciones de riesgo.
- La aprobación formal emitida por el Departamento de TI. Que en este caso puede ser la copia del correo electrónico donde se da el aval final.
- La documentación correspondiente al cumplimiento de la Política de cumplimiento normativo y actualización de estándares ***(PCN-AE-001).***
- Cualquier observación, comentario técnico o solicitud de ajuste registrada durante el proceso.

El expediente completo deberá ser archivado por el Departamento de Mercadeo como área solicitante, resguardado en formato digital en la carpeta del proyecto y disponible ante requerimientos de auditoría o revisión institucional.

ANEXOS

Anexo 1- Formulario de validación final – Proyectos web subcontratados

Este anexo complementa el protocolo institucional (PTC-AVF-001) y debe ser utilizado en cada cierre de proyecto para registrar el cumplimiento de los criterios definidos. Su uso es obligatorio para el proveedor y el Departamento de Mercadeo antes de solicitar la aprobación de TI.

Objetivo: Verificar que el desarrollo web ha cumplido con los criterios técnicos, normativos y documentales establecidos en el protocolo de aprobación y validación final.

Instrucciones: Complete este formulario al finalizar el desarrollo. Indique en cada criterio como cumplido o no cumplido, agregue observaciones si aplica, y archive este documento junto con el expediente técnico del proyecto. La validación debe completarse antes de autorizar su publicación en producción.

Tabla 13

Formulario de validación final – Proyectos web subcontratados

Item	Criterio de validación	Cumple	Observaciones
1	Se entregó el desarrollo funcional en entorno de pruebas	Sí / No	
2	Se completó y adjuntó el checklist NTV-CDS-001	Sí / No	
3	Se incluyó evidencia técnica (capturas, enlaces, configuración de seguridad)	Sí / No	
4	Se entregó justificación del riesgo de vulnerabilidades detectadas	Sí / No	
5	Se presentó documentación técnica conforme a la directriz DR-EADS-001	Sí / No	
6	Se cumplieron los lineamientos de la política PCN-AE-001 sobre tratamiento de datos	Sí / No	
7	Se recibió aprobación formal de TI	Sí / No	
8	El expediente fue archivado en la carpeta oficial del proyecto	Sí / No	

Fuente: *Vega, 2025.*

Este formulario estará disponible en formato digital para su llenado en línea por parte del proveedor y el Departamento de Mercadeo. En el siguiente enlace: Formulario de validación final – Proyectos web subcontratados

Importante, deberá archivarse como parte del expediente documental del desarrollo web.

Historial de versiones del protocolo:

Tabla 14
Detalle de versiones del protocolo

Versión	Fecha	Descripción del cambio	Responsable
1.0	27/06/2025	Versión inicial del protocolo. Incluye proceso de validación final, entrega de evidencias y coordinación entre Mercadeo, TI y proveedores.	Johan Vega
1.2			
1.3			

Fuente: *Vega, 2025.*

APÉNDICE G

Normativa de gestión de incidentes de seguridad y monitoreo de actividades

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA EN INFORMÁTICA

NORMATIVA DE GESTION DE INCIDENTES DE SEGURIDAD Y MONITOREO DE ACTIVIDADES

JOHAN VEGA CÓRDOBA

JULIO, 2025

INTRODUCCIÓN

La gestión oportuna de incidentes de seguridad y el monitoreo continuo de los desarrollos web son elementos críticos para garantizar la integridad, confidencialidad y disponibilidad de la información en las campañas digitales de la Cooperativa. En un entorno donde los sitios web recopilan, procesan o almacenan datos personales, cualquier vulnerabilidad no gestionada puede representar un gran riesgo operativo, reputacional y legal para la organización.

Durante el análisis de resultados, varios colaboradores del Departamento de TI indicaron que “no se tienen controles establecidos para el manejo de incidentes en desarrollos externos” y que “cada proyecto se trata de forma aislada sin un procedimiento definido para el monitoreo después de su lanzamiento”. Además, entre las respuestas de los proveedores se reflejó que “no se solicita un protocolo para reportar incidentes”, lo cual evidencia una necesidad institucional de estandarizar este proceso.

Con base en lo anterior, esta normativa tiene el propósito de establecer los lineamientos mínimos que deberán cumplirse para identificar, registrar, comunicar y resolver incidentes de seguridad que puedan presentarse en los desarrollos subcontratados por el Departamento de Mercadeo.

OBJETIVO

Establecer una normativa institucional que permita gestionar de forma estandarizada los incidentes de seguridad en los desarrollos web subcontratados, mediante procedimientos claros de detección, respuesta y documentación. Asimismo, asegurar que, los hallazgos derivados de dichos incidentes sean utilizados como insumos para mejorar los criterios de seguridad en futuros desarrollos.

ALCANCE

Esta normativa aplica a todos los desarrollos web subcontratados por el Departamento de Mercadeo de la Cooperativa que estén destinados a campañas publicitarias, incluyendo landing pages, micrositios y formularios. Es de cumplimiento obligatorio para proveedores, agencias externas y personal de Mercadeo involucrado en la gestión o supervisión de dichos proyectos.

Incluye tanto la detección y gestión de incidentes de seguridad que puedan surgir antes, durante o después del lanzamiento del sitio, como la documentación de acciones correctivas y aprendizajes aplicables a futuros proyectos, sin requerir mantenimiento posterior en sitios desactivados.

FUNDAMENTO NORMATIVO

El fundamento normativo para la gestión de incidentes de seguridad y el monitoreo de actividades en los desarrollos web del Departamento de Mercadeo de Dos Pinos se encuentra en el Artículo 10 de la Ley Nº8968, el cual establece la obligación de adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos personales. Este artículo indica expresamente que deben prevenirse eventos como la alteración, pérdida, acceso no autorizado o tratamiento ilícito de la información, lo cual se relaciona directamente con la detección, gestión y corrección de incidentes de seguridad. Asimismo, se exige que tales medidas incluyan mecanismos de seguridad física y lógica adecuados, alineados con el desarrollo tecnológico actual.

En complemento, los controles establecidos en la norma ISO/IEC 27001:2022 refuerzan estas disposiciones. Para ser más específicos, se aplican los siguientes:

- **Control A.5.24 (Gestión de incidentes de seguridad de la información):** Exige establecer responsabilidades claras y procesos estructurados para responder ante incidentes de seguridad.
- **Control A.5.25 (Evaluación y Decisión sobre Eventos de Seguridad de la Información):** Obliga a analizar las causas raíz y aplicar mejoras continuas luego de cada incidente.
- **Control A.6.8 (Informes de eventos de seguridad de la información):** Establece que cualquier evento relevante debe ser reportado a las personas o unidades responsables.
- **Control A.8.16 (Actividades de seguimiento):** Establece que deben implementarse mecanismos de monitoreo para detectar actividades anómalas, accesos no autorizados o posibles vulnerabilidades.

La integración de estos controles y del marco legal de la Ley Nº8968, permite establecer de forma correcta un enfoque preventivo y correctivo que garantice la integridad de los sistemas digitales utilizados en las campañas de mercadeo, así como la protección efectiva de los datos personales de los usuarios.

PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES Y MONITOREO DE ACTIVIDADES

Con el objetivo de garantizar la protección de los datos personales y la continuidad de los servicios digitales, se establece el siguiente procedimiento para la detección, gestión, notificación y monitoreo de incidentes de seguridad en los desarrollos web subcontratados por la Cooperativa:

Detección y registro del incidente

La detección oportuna de incidentes representa el primer paso crítico en la contención de riesgos asociados a la seguridad de los desarrollos. A continuación, se detallan las acciones puntuales para identificar, reportar y documentar técnicamente cualquier evento:

- **Reporte inicial:** Toda anomalía, comportamiento inusual o incidente confirmado debe ser reportado de inmediato por la agencia externa o por el personal interno que lo detecte. El canal de reporte será definido previamente por el Departamento de Mercadeo, y podrá incluir medios como correo o formularios digitales.
- **Registro del incidente:** El evento será documentado en un formulario técnico que deberá incluir como mínimo:
    - Fecha y hora de detección.
    - Sitio web o sistema afectado.
    - Descripción del incidente observado.
    - Persona o equipo que lo reporta.
    - Evidencia preliminar (capturas de pantalla, logs del servidor, alertas del sistema).
- **Asignación de prioridad:** El incidente se clasificará de acuerdo con su impacto potencial, tomando en cuenta variables como:
    - Tipo de información comprometida.
    - Grado de exposición pública.
    - Afectación a servicios críticos de campaña o experiencia del usuario.
- **Preservación de evidencia:** Se deberá conservar toda la evidencia técnica vinculada al incidente, incluyendo logs, archivos fuente, registros de auditoría, capturas del navegador o respuestas del sistema, según el caso.

Para asegurar una documentación estandarizada, el Departamento de Mercadeo dispondrá de la siguiente plantilla, que deberá ser utilizada en todo reporte técnico de incidentes:

Tabla 15
Formulario de reporte técnico de incidentes

Campo	Descripción
Fecha y hora del incidente	Momento exacto en que se detecta el evento.
Sistema afectado	URL o nombre del sitio web/plataforma afectada.
Tipo de incidente	Brecha de acceso, pérdida de datos, comportamiento inusual, otro.
Descripción del incidente	Detalle técnico del evento observado.
Medio de detección	Indicar si fue mediante monitoreo, alerta automática, reporte humano, etc.
Impacto preliminar	Breve descripción del posible alcance o afectación inicial.
Acciones inmediatas tomadas	Ejemplo: aislamiento del sistema, cambio de contraseñas, escaneo inicial.
Evidencia adjunta	Indicar si se incluyen logs, capturas de pantalla, reportes, etc.
Persona que reporta	Nombre, cargo, correo institucional.
Responsable de recepción	Nombre del receptor del incidente en TI o Mercadeo.

Fuente: *Vega, 2025.*

El archivo editable del formulario de reporte técnico de incidentes puede ser consultado y descargado en el siguiente enlace: Formulario de reporte técnico de incidentes

Notificación y comunicación interna

Una vez documentado el incidente, se debe activar el proceso de notificación interna, el cual permite alertar a los equipos responsables y coordinar una respuesta oportuna:

- **Remisión formal del incidente:** El reporte técnico debe ser enviado por parte del responsable inicial (ya sea del equipo de Mercadeo o la agencia externa) al contacto designado en el Departamento de Tecnologías de la Información (TI), utilizando los medios oficiales previamente establecidos (correo institucional, plataforma compartida u otro canal habilitado).
- **Plazo de notificación:** La notificación debe realizarse en un plazo máximo de 24 horas naturales desde el momento en que el incidente fue detectado. El incumplimiento de este plazo deberá justificarse por escrito.

- **Verificación y acuse de recibo:** El equipo de TI confirmará la recepción del reporte, verificará su completitud y procederá con la revisión inicial del incidente. En caso de que el informe esté incompleto o carezca de evidencia suficiente, se devolverá al remitente para su corrección.
- **Notificación a jefaturas:** Una vez validado el incidente, el Departamento de TI informará a las jefaturas de Mercadeo y, si se estima necesario, a instancias legales o de auditoría interna. Esta decisión dependerá de la criticidad y del impacto del incidente.

Evaluación y contención

Una vez notificado el incidente y validada su existencia por parte del Departamento de Tecnologías de la Información, se procederá con su evaluación técnica y la aplicación de medidas de contención inmediatas para mitigar el impacto:

- **Análisis técnico inicial:** El equipo de TI, en conjunto con la agencia externa responsable (si corresponde), analizará la naturaleza del incidente, su origen probable, los sistemas afectados y el alcance del impacto.
- **Medidas de contención:** Si el incidente representa una amenaza activa o potencial para otros sistemas, se deben aplicar acciones inmediatas como:
    - Aislamiento del servidor afectado o aplicación temporal de reglas de firewall.
    - Suspensión del acceso al sistema o funcionalidad comprometida.
    - Desactivación temporal del sitio web si así se determina técnicamente.
- **Documentación de la causa raíz:** Durante esta fase se identificará la causa raíz del incidente. Esta información debe ser incorporada al informe final del incidente.
- **Coordinación con la agencia externa:** Si la causa del incidente se relaciona con una configuración o error de desarrollo, se solicitará formalmente a la agencia externa la implementación de las medidas técnicas correctivas necesarias. Esta respuesta debe ser documentada por el proveedor y aprobada por TI antes de continuar con el restablecimiento de los servicios.

Recuperación y cierre del incidente

Tras la contención del incidente, se deben ejecutar las acciones necesarias para restablecer los sistemas afectados y formalizar el cierre técnico y documental del evento:

- **Restablecimiento seguro:** Una vez mitigada la amenaza, se procederá a la recuperación de los servicios afectados. Este restablecimiento deberá garantizar que:
    - Se haya corregido la causa raíz.
    - Se hayan aplicado los parches, configuraciones o controles requeridos.
    - El sistema se encuentre libre de vulnerabilidades residuales.
- **Validación por parte de TI:** Antes de restablecer el funcionamiento completo del desarrollo web, el equipo de TI deberá ejecutar pruebas de verificación técnica que confirmen que el incidente ha sido solucionado de forma efectiva. No se reactivará el entorno hasta completar esta validación.
- **Cierre documental del incidente:** La plantilla de reporte técnico utilizada en la fase de detección deberá ser completada con la información de cierre, incluyendo las acciones aplicadas, la fecha de resolución y la validación final.

Actualización y mejora de criterios de seguridad

Una vez cerrado el incidente, los hallazgos identificados durante el análisis y la resolución deberán ser considerados como insumos para mejorar los criterios de seguridad aplicables en futuros desarrollos web del Departamento.

- **Incorporación de aprendizajes:** Toda vulnerabilidad, fallo de configuración o error detectado deberá ser documentado y evaluado para determinar si requiere un ajuste en las prácticas estándar de seguridad, como el checklist de validación, las pruebas previas al lanzamiento o las configuraciones mínimas requeridas para agencias externas.
- **Retroalimentación a agencias externas:** Cuando corresponda, se deberán comunicar las lecciones aprendidas a los proveedores involucrados, con el fin de prevenir la reincidencia del mismo tipo de fallo en campañas posteriores.
- **Ajuste a procedimientos internos:** Si el incidente revela una debilidad en el flujo de revisión, comunicación o control interno, el Departamento de Mercadeo, en conjunto con TI, deberá considerar ajustes a los protocolos vigentes.
- **Ciclo de mejora continua:** Aunque los desarrollos web de campaña pueden llegar ser temporales, los procedimientos de seguridad deben mantenerse en revisión constante. Cada incidente representa una oportunidad para fortalecer la calidad técnica y normativa de futuros proyectos.

RESPONSABLES

Para asegurar la correcta ejecución del procedimiento de gestión de incidentes de seguridad y actualización de criterios en los desarrollos web subcontratados por el Departamento de Mercadeo, se definen las siguientes responsabilidades:

Tabla 16
Responsables del procedimiento

Rol	Responsabilidades
Agencias externas o proveedores	• Detectar y reportar incidentes de seguridad. • Completar el formulario técnico de reporte. • Ejecutar acciones correctivas sobre el desarrollo afectado.
Departamento de Mercadeo	• Recibir y canalizar reportes de incidentes. • Coordinar con TI las alertas • Archivar la documentación del incidente. • Incorporar aprendizajes en futuras campañas.
Departamento de TI	• Validar técnicamente el incidente. • Coordinar la contención y recuperación. • Aprobar el restablecimiento del sistema. • Apoyar en ajustes técnicos y recomendaciones de seguridad.

Fuente: *Vega, 2025.*

Historial de versiones de la normativa:

Tabla 17
Detalle de versiones de la normativa

Versión	Fecha	Descripción del cambio	Responsable
1.0	03/07/2025	Versión inicial de la normativa. Incluye objetivo, alcance, fundamento legal, principios, consentimiento informado, gestión de cookies, atención de solicitudes y trazabilidad técnica.	Johan Vega
1.2			
1.3			

Fuente: *Vega, 2025.*

REFERENCIAS

Amazon Web Services. (2023). *Best Practices for Backend Development*. https://aws.amazon.com/backend-best-practices/

Arroyo Valenciano, J. A. (2022). Las variables como elemento sustancial en el método científico. Revista Educación, 46(1). https://doi.org/10.15517/revedu.v46i1.45609

Arsys. (2024, 12 de enero). Backend: qué es y por qué tiene tanta importancia en desarrollo web. Blog de Arsys. https://www.arsys.es/blog/backend-que-es-y-por-que-tiene-tanta-importancia-en-desarrollo-web

Bishop, M., & Snyder, T. (2022). *Computer Security: Principles and Practice* (5th ed.). Pearson.

Castillo Medina, F. (2021). La ciberseguridad y sus escenarios de aplicación en las organizaciones. *Revista Iberoamericana de Seguridad Informática, 10*(2), 164-172.

ComplianceQuest. (2022). FDA Software Validation: A Helpful Guide to 2025. Recuperado de https://www.compliancequest.com/blog/understanding-fda-software-validation/

Concepto.de. (2024). Fuentes de información. https://concepto.de/fuentes-de-informacion/

Fernández Casado, P. E. (2024). Iniciación a la creación de páginas web (1.ª ed.). RA-MA Editorial. https://elibro.net/es/ereader/bibliouia/267661?page=8

Fernández Casado, P. E. (2024). Posicionamiento SEO: curso práctico (1.ª ed.). RA-MA Editorial. https://elibro.net/es/ereader/bibliouia/273945?page=157

Fischer de la Vega, L. E., & Espejo Callado, J. (2024). Mercadotecnia en la era digital (1.ª ed.). McGraw-Hill Interamericana Editores.

González, J. M. (2022). *Ley 8968: Protección de Datos Personales en Costa Rica*. Editorial Jurídica Continental.

Hernández-Sampieri, R., Fernández, C., & Baptista, P. (2023). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (7.ª ed.). McGraw Hill.

Juanjo Artero. (2023). *First-Party Data: Qué es y cómo funciona*. https://juanjoartero.com/first-party-data-que-es-y-como-funciona/

Kerin, R. A., & Hartley, S. W. (2023). *Marketing*. McGraw-Hill Interamericana. https://www.ebooks7-24.com/?il=31453

Lotame. (2022). *First-Party Data: What It Is and Why It Matters*. https://www.lotame.com/first-party-data/

Loyanes Aguilar, L. (2020). Fundamentos de programación: algoritmos, estructura de datos y objetos. McGraw-Hill. https://www.ebooks7-24.com/?il=10409

Núñez Cudriz, A. F., & Miranda Corrales, C. (2020). El marketing digital como un elemento de apoyo estratégico a las organizaciones. *Revista Científica Profundidad Construyendo Futuro, 11*(11), 54-66. https://www.redalyc.org/journal/4096/409663283006/409663283006.pdf

Patel, Z. (2024). Software architecture: Frontend and backend. Medium. https://medium.com/@zeel.patel1441/software-architecture-frontend-and-backend-7c30af1cf9e2

Sachdev, R. (2024). *Marketing digital* (1.ª ed. en español). McGraw-Hill Interamericana Editores.

SafetyCulture. (2023). Cómo realizar una auditoría de cumplimiento. Recuperado de https://safetyculture.com/es/temas/auditoria-de-cumplimiento/

Universidad de Puerto Rico, Recinto de Río Piedras. (2022). *Fuentes terciarias*. https://uprrp.libguides.com/fuentes_secundarias/que_son_terciarias

APÉNDICES

Cuestionario

En el marco de una investigación sobre la seguridad y proceso de control de los desarrollos web del departamento de mercadeo de la Cooperativa de productores de leche Dos Pinos, le invitamos a completar este cuestionario. Su participación es de gran importancia para comprender cómo el tema en estudio influye en la actividad de la organización.

Este cuestionario es confidencial. Sus respuestas solo se utilizarán con fines de investigación y no serán compartidas con ninguna otra persona o institución. Completar el cuestionario tomará aproximadamente de 10 a 15 minutos.

Sección #1: **Validación de funcionamiento, accesos y protección de datos**

Estas preguntas buscan conocer si, antes de lanzar un sitio web, se revisa su correcto funcionamiento, se controla quién accede y se protegen los datos personales que ahí se recopilan.

1. ¿Antes de lanzar una página web, se revisa si funciona correctamente y no tiene errores graves?

   ☐ Sí ☐ No ☐ No sabe / No aplica

2. ¿Las personas que ingresan a los sistemas web tienen accesos limitados según lo que les corresponde hacer?

   ☐ Sí ☐ No ☐ No sabe / No aplica

3. ¿Se protege la información que se guarda en los formularios o páginas web, como correos, teléfonos o algún otro dato personal y confidencial?

   ☐ Sí ☐ No ☐ No sabe / No aplica

4. ¿Se revisa el trabajo entregado por las agencias antes de usarlo públicamente (las páginas web)?

   ☐ Sí ☐ No ☐ No sabe / No aplica

Sección #2: **Revisión de seguridad y requisitos para agencias externas**

Este bloque evalúa si a las agencias externas a Dos Pinos se les solicita cumplir con medidas básicas de seguridad antes de entregar sus desarrollos.

5. ¿A las agencias se les piden requisitos de seguridad cuando entregan un desarrollo web?
   ☐ Sí ☐ No ☐ No sabe / No aplica
6. ¿Se les brinda a las agencias alguna lista o documento con lo que deben revisar antes de entregar un sitio web?
   ☐ Sí ☐ No ☐ No sabe / No aplica
7. ¿Cuándo algo no cumple con los requisitos, se devuelve a la agencia los errores para que hagan cambios?
   ☐ Sí ☐ No ☐ No sabe / No aplica

Sección #3: **Uso de listas de verificación o control previo al lanzamiento**

Estas preguntas buscan saber si existe una guía o lista que ayude al departamento en revisar los sitios web antes de publicarlos.

8. ¿Se usa alguna lista o guía para revisar que un sitio web esté completo y seguro antes de lanzarlo?
   ☐ Sí ☐ No ☐ No sabe / No aplica
9. ¿Esa lista incluye aspectos como accesos, datos personales o pruebas básicas?
   ☐ Sí ☐ No ☐ No sabe / No aplica
10. ¿Alguien firma o aprueba que se revisó todo antes de lanzar un sitio?
    ☐ Sí ☐ No ☐ No sabe / No aplica

Sección #4: **Actualización de prácticas o medidas de seguridad**

Este bloque analiza si se actualizan las prácticas internas y si se capacita al equipo cuando cambian las normativas o se detectan mejoras necesarias.

11. ¿Se revisan y actualizan con el tiempo las medidas o recomendaciones para sitios web?
    ☐ Sí ☐ No ☐ No sabe / No aplica
12. ¿El personal de mercadeo, TI o agencias reciben capacitación sobre cómo cuidar mejor los datos o proteger los sitios?
    ☐ Sí ☐ No ☐ No sabe / No aplica

13. ¿Se aplican cambios dentro del proceso de creación de sitios web cuando hay nuevas leyes o recomendaciones técnicas sobre privacidad de los datos?
    ☐ Sí ☐ No ☐ No sabe / No aplica

Sección #5: **Revisión final y seguimiento después del lanzamiento**

Estas preguntas permiten saber si existe una última revisión antes de lanzar un desarrollo web, y si se le da seguimiento después de estar en línea.

14. ¿Existe una revisión final obligatoria antes de lanzar un sitio web?
    ☐ Sí ☐ No ☐ No sabe / No aplica
15. ¿Después de lanzar un sitio, se sigue monitoreando si funciona bien y si hay fallos?
    ☐ Sí ☐ No ☐ No sabe / No aplica

Pregunta abierta final

Por último, si desea compartir una sugerencia o idea adicional, puede hacerlo aquí.

¿Desea realizar algún comentario o sugerencia sobre cómo mejorar la seguridad de los sitios web que se usan en el Departamento de Mercadeo?

Resultados del cuestionario aplicado

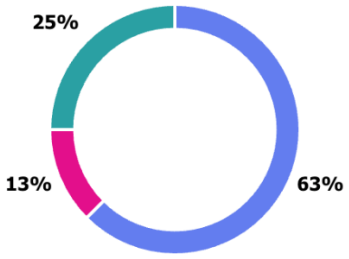
El cuestionario fue aplicado al personal del Departamento de Mercadeo y a proveedores actuales de la Cooperativa Dos Pinos involucrados en el desarrollo de sitios web, con el fin de evaluar prácticas actuales relacionadas con la seguridad, validación y tratamiento de datos personales.

1. ¿Antes de lanzar una página web, se revisa si funciona correctamente y no tiene errores graves?

2. ¿Las personas que ingresan a los sistemas web tienen accesos limitados según lo que les corresponde hacer?

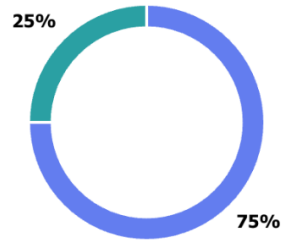
3. ¿Se protege la información que se guarda en los formularios o páginas web, como correos, teléfonos o algún otro dat o personal y confidencial?

SÍ	5
No	1
No sabe / No aplica	2



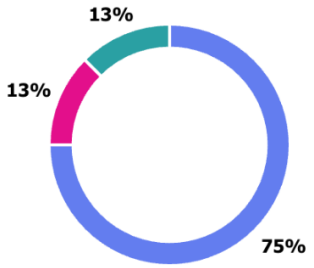
4. ¿Se revisa el trabajo entregado por las agencias antes de usarlo públicamente (las páginas web)?

Sí	6
No	0
No sabe / No aplica	2



5. ¿A las agencias se les piden requisitos de seguridad cuando entregan un desarrollo web?

Sí	6
No	1
No sabe / No aplica	1

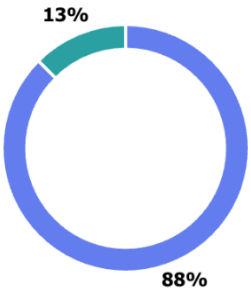


6. ¿Se les brinda a las agencias alguna lista o documento con lo que deben revisar antes de entregar un sitio web?

Sí	4
No	0
No sabe / No aplica	4

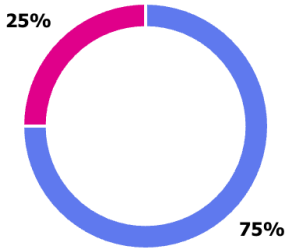
7. ¿Cuándo algo no cumple con los requisitos, se devuelve a la agencia los errores para que hagan cambios?

Sí	7
No	0
No sabe / No aplica	1



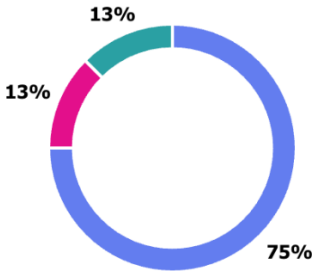
8. ¿Se usa alguna lista o guía para revisar que un sitio web esté completo y seguro antes de lanzarlo?

Sí	6
No	2
No sabe / No aplica	0



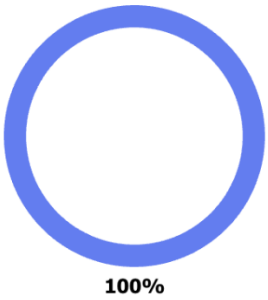
9. ¿Esa lista incluye aspectos como accesos, datos personales o pruebas básicas?

Sí	6
No	1
No sabe / No aplica	1



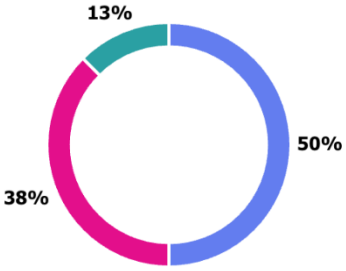
10. ¿Alguien firma o aprueba que se revisó todo antes de lanzar un sitio?

Sí	8
No	0
No sabe / No aplica	0



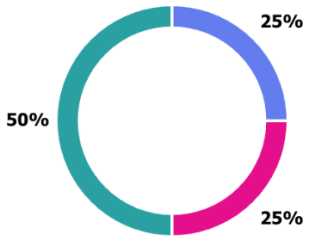
11. ¿Se revisan y actualizan con el tiempo las medidas o recomendaciones para sitios web?

Sí	4
No	3
No sabe / No aplica	1



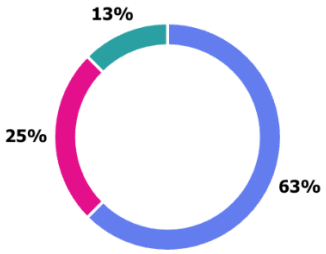
12. ¿El personal de mercadeo, TI o agencias reciben capacitación sobre cómo cuidar mejor los datos o proteger los sitio s?

Sí	2
No	2
No sabe / No aplica	4



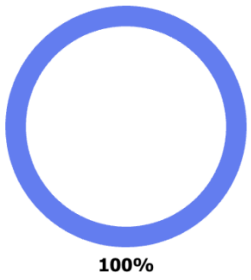
13. ¿Se aplican cambios dentro del proceso de creación de sitios web cuando hay nuevas leyes o recomendaciones técni cas sobre privacidad de los datos?

Sí	5
No	2
No sabe / No aplica	1



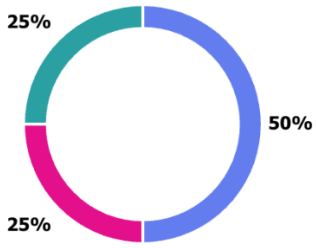
14. ¿Existe una revisión final obligatoria antes de lanzar un sitio web?

Sí	8
No	0
No sabe / No aplica	0



15. ¿Después de lanzar un sitio, se sigue monitoreando si funciona bien y si hay fallos?

Sí	4
No	2
No sabe / No aplica	2



16. **Pregunta abierta final**

Por último, si desea compartir una sugerencia o idea adicional, puede hacerlo aquí. ¿Desea realizar algún comentario o sugerencia sobre cómo mejorar la seguridad de los sitios web que se usan en el Departamento de Mercadeo?

3
Respuestas

Respuestas más recientes
...

16. Pregunta abierta final Por último, si desea compartir una sugerencia o idea adicional, puede hacerlo aquí. ¿Desea realizar algún comentario o sugerencia sobre cómo mejorar la seguridad de los sitios web que se usan en el Departamento de Mercadeo?

3 Respuestas

ID ↑	Nombre	Respuestas
1	anonymous	No
2	anonymous	Deben de contratar algun servicio anualmente, que analice todas las plataformas existentes esto con el objetivo de realizar las recomendaciones tecnicas para aplicarlas.
3	anonymous	no

Guía de entrevista

Organización:	**Cooperativa de Productores de Leche Dos Pinos**
Nombre del entrevistado:	
Cargo dentro de la organización:	
Fecha de la entrevista:	

Sección 1: Seguridad en los Desarrollos Web

1. ¿Cómo se gestiona actualmente la seguridad en los desarrollos web utilizados por el Departamento de Mercadeo?
2. ¿Existen protocolos establecidos para verificar la seguridad de los desarrollos web creados por agencias externas a Dos Pinos antes de su implementación?
3. ¿Existe una persona o grupo de personas encargados de supervisar los aspectos de seguridad en los proyectos web del departamento de Mercadeo?

Sección 2: Controles de Seguridad y Normativas

4. ¿Están familiarizados los procesos internos de TI actualmente con la normativa ISO 27001 y la Ley Nº8968 en relación con la seguridad de la información?
5. ¿Existen medidas de seguridad para proteger los datos personales de los usuarios en los desarrollos web del Departamento de Mercadeo?
6. ¿Cómo se manejan los permisos de acceso y control de usuarios dentro de los desarrollos web? ¿En el caso de agencias externas, se realizan estos controles?
7. ¿Las agencias externas deben cumplir con estándares de seguridad específicos antes de entrega algún proyecto?

Sección 3: Evaluación de Seguridad y Procesos de Mejora

8. ¿Se realizan auditorías o revisiones de seguridad antes de lanzar un desarrollo web al público?
9. ¿Han identificado vulnerabilidades en desarrollos web previos? ¿Cómo han sido manejadas y corregidas?
10. ¿Se ejecutan pruebas de seguridad como evaluación de código o pruebas de carga en los desarrollos web?

11. ¿Existe un procedimiento de aprobación final antes del lanzamiento de un sitio web creado por alguna agencia externa a Dos Pinos?

Sección 4: Monitoreo y Mejoras en Seguridad

12. ¿Cómo se monitorean los desarrollos web luego de su lanzamiento para identificar posibles fallos de seguridad?
13. ¿Se realizan capacitaciones al personal de Mercadeo, TI sobre seguridad en desarrollos web y normativas aplicables?
14. ¿Qué mejoras considera necesarias para fortalecer la seguridad en los desarrollos web del Departamento de Mercadeo?
15. ¿Cómo evalúa el cumplimiento actual de las agencias externas en términos de seguridad y normativas aplicadas?

Resultados de guía aplicada

Las entrevistas fueron realizadas a dos colaboradores del área de Tecnologías de Información de la Cooperativa Dos Pinos, con el fin de conocer las prácticas actuales relacionadas con la seguridad, validación y control en los desarrollos web del Departamento de Mercadeo.

Organización:	**Cooperativa de Productores de Leche Dos Pinos**
Nombre del entrevistado:	Marianela Rodríguez Rojas
Cargo dentro de la organización:	Departamento de TI
Fecha de la entrevista:	Miércoles 28 de Mayo

Sección 1: Seguridad en los Desarrollos Web

1. **¿Cómo se gestiona actualmente la seguridad en los desarrollos web utilizados por el Departamento de Mercadeo?** *"Bueno, realmente desde Mercadeo no hay algo tan establecido, casi siempre dependemos del proveedor. A veces sí lo conversamos con TI, pero no es que haya un proceso como tal. Se confía mucho en que la agencia lo haga bien y que cumpla con lo básico de seguridad. Ya si TI detecta algo, ahí es donde entran. Pero desde Mercadeo no hay una revisión específica de eso".*
2. **¿Existen protocolos establecidos para verificar la seguridad de los desarrollos web creados por agencias externas a Dos Pinos antes de su implementación?**
   "No, no hay un protocolo como tal. Uno esperaría que eso venga ya trabajado por la agencia, pero no hay una revisión específica por parte de nosotros".
3. **¿Existe una persona o grupo de personas encargados de supervisar los aspectos de seguridad en los proyectos web del departamento de Mercadeo?**
   "Desde Mercadeo como tal, no. O sea, nosotros vemos más el contenido, el diseño, la experiencia… pero temas de seguridad, eso ya le corresponde a TI. Si hay algo muy puntual, lo escalamos, pero no hay alguien dentro del equipo que vea eso directamente".

Sección 2: Controles de Seguridad y Normativas

4. **¿Están familiarizados los procesos internos de TI actualmente con la normativa ISO 27001 y la Ley Nº8968 en relación con la seguridad de la información?**
   "No sabría decirte mucho, sé que algunos compañeros hablan de la ISO, que es un marco y que algunas cosas se trabajan en pro de esto, pero que cumplamos esta normal al 100% no".
5. **¿Existen medidas de seguridad para proteger los datos personales de los usuarios en los desarrollos web del Departamento de Mercadeo?**
   "Depende del desarrollo. En algunos casos, cuando hay formularios o algo que recoge datos, sí se pide que estén protegidos, pero no hay una revisión a fondo desde nuestro lado. Confiamos en que la agencia cumpla con eso y, si es necesario, se consulta con TI".
6. **¿Cómo se manejan los permisos de acceso y control de usuarios dentro de los desarrollos web? ¿En el caso de agencias externas, se realizan estos controles?**
   "No sé si ahorita tenemos un control. Tal vez otro compañero lo sepa. El dominio es nuestro y a algunos proveedores les damos algunos permisos, pero no sé si tenemos un control formalizado de momento. Desconozco".
7. **¿Las agencias externas deben cumplir con estándares de seguridad específicos antes de entrega algún proyecto?**
   "No tenemos un documento o lineamiento que diga qué deben cumplir exactamente. Uno espera que la agencia cumpla con lo básico, pero no se les da un estándar claro. A veces TI sí revisa algo antes de publicar, pero no es un requisito formal ni algo que esté definido desde el inicio del proyecto".

Sección 3: Evaluación de Seguridad y Procesos de Mejora

8. **¿Se realizan auditorías o revisiones de seguridad antes de lanzar un desarrollo web al público?** *"No, no se realiza, pensaría que se hace la auditoria después de que se publique, sí".*

9. **¿Han identificado vulnerabilidades en desarrollos web previos? ¿Cómo han sido manejadas y corregidas?**

   "No sé si han detectado vulnerabilidades, lo que ha pasado un reporte donde me brindan páginas web a nombre de Dos Pinos, para revisar si las debemos mantener o dar de baja. Pero no es que hacemos un proceso de estar pendiente al detalle de cada web".

10. **¿Se ejecutan pruebas de seguridad como evaluación de código o pruebas de carga en los desarrollos web?**

    "Sé que se han pruebas de código, pero en aplicativos, pero no en desarrollos web- Creo que no".

11. **¿Existe un procedimiento de aprobación final antes del lanzamiento de un sitio web creado por alguna agencia externa a Dos Pinos?**

    "No, actualmente no se realiza".

Sección 4: Monitoreo y Mejoras en Seguridad

12. **¿Cómo se monitorean los desarrollos web luego de su lanzamiento para identificar posibles fallos de seguridad? "***Se hace a través de un scaneo que se hacen los compañeros, para verificar qué webs están a nombre de Dos Pinos, de momento, solo eso".*

13. **¿Se realizan capacitaciones al personal de Mercadeo, TI sobre seguridad en desarrollos web y normativas aplicables?** *"No, a Mercadeo no lo involucramos, esto lo dejamos solo al departamento de seguridad de TI".*

14. **¿Qué mejoras considera necesarias para fortalecer la seguridad en los desarrollos web del Departamento de Mercadeo?**

    "Que se aseguren que todo lo que hagan lo pasen por TI, porque muchas veces gestionan Desarrollos y no nos involucran, y esto hace que no tengamos visibilidad de nada".

15. **¿Cómo evalúa el cumplimiento actual de las agencias externas en términos de seguridad y normativas aplicadas?** *"De momento bien, porque solo he tenido contacto con un solo proveedor".*

Organización:	**Cooperativa de Productores de Leche Dos Pinos**
Nombre del entrevistado:	Jorge Eduardo Soto Mora
Cargo dentro de la organización:	Departamento de TI
Fecha de la entrevista:	Miércoles 28 de Mayo

Sección 1: Seguridad en los Desarrollos Web

1. **¿Cómo se gestiona actualmente la seguridad en los desarrollos web utilizados por el Departamento de Mercadeo?** *"Para el departamento de Mercadeo no hay un proceso fijo para eso. Normalmente lo vemos con los encargados cuando logramos identificar una nueva solicitud de un desarrollo web y si algo nos genera duda, lo consultamos, para seguir brindando apoyo".*
2. **¿Existen protocolos establecidos para verificar la seguridad de los desarrollos web creados por agencias externas a Dos Pinos antes de su implementación?**
   "Sí, hoy por hoy hay un procedimiento de análisis de vulnerabilidad este sobre desarrollos y bueno sobre aplicaciones, infraestructura, ya se ejecuta, se valida y forma parte de lo que es una salida a producción de un nuevo sitio. Esto Dentro de TI, pero si esto no pasa por el área de TI, que ya nos ha pasado, muy difícilmente tengamos visibilidad para poder hacer esas verificaciones. Tenemos un servicio de protección de marca, y muchas veces hemos visto sitios que nunca hemos aprobado o que no pasaron por nuestra dirección, y esto pasa generalmente ya después de su producción".
3. **¿Existe una persona o grupo de personas encargados de supervisar los aspectos de seguridad en los proyectos web del departamento de Mercadeo?**
   "Hoy tenemos 2 especialista en ciberseguridad, hay un arquitecto. Pero nos basamos en las solicitudes de lo que nos vaya ingresando o de lo que logramos identificar. Algunas veces nos hemos encontrado sitios en ambientes de pruebas, y muchas veces esos mismos sitios ya están publicados. Y como te digo, solo nosotros dos estamos dedicados para toda la Cooperativa, pero muchas veces nos quedamos un poco cortos para atender todo. La idea es que todos los desarrollos pasen por nuestro departamento".

Sección 2: Controles de Seguridad y Normativas

4. **¿Están familiarizados los procesos internos de TI actualmente con la normativa ISO 27001 y la Ley Nº8968 en relación con la seguridad de la información?**

   "Sí, estamos alineados, nuestros procesos están basados en la ISO y las mejores normas. Hemos tenidos consultorías para entender la madurez que tenemos en cuanto a nuestros procesos. Y con respecto a la Ley de protección de datos, tratamos de implementar un disclaimer para que el usuario entienda sobre el uso de sus datos".

5. **¿Existen medidas de seguridad para proteger los datos personales de los usuarios en los desarrollos web del Departamento de Mercadeo?**

   "Normalmente son desarrollos a un tercero y eso tiene que estar amparado bajo el contrato que tenga mercadeo con el tercero y ahí sale completamente de nuestro control porque puede ser que sea infraestructura no administrada por la dirección de tecnología. Sin embargo, en los análisis de vulnerabilidades que se realizan en los análisis dinámicos o los análisis estáticos, dependiendo del desarrollo, logramos identificar algunas brechas y solicitamos que se hagan las medidas correcciones en pro de brindar esta protección".

6. **¿Cómo se manejan los permisos de acceso y control de usuarios dentro de los desarrollos web? ¿En el caso de agencias externas, se realizan estos controles?**

   "A ver a ver ya hay directrices, si pasa por la dirección de tecnología, se solicita que sea través de la integración de nuestro Active Directory o sea que sea una integración de usuarios por federación, si son con usuarios internos, si son con usuarios externos, pues bueno, hay que administrar una base de datos con todas las características y demás, siempre que pase por tecnología. Si son desarrollos de terceros, la recomendación es la misma. Sin embargo, como le mencionaba anteriormente, esto va a depender de qué tanto tecnología esté siendo involucrado con las iniciativas porque ahí es donde en el contrato podemos definir y apoyar a mercadeo en que se consideren las mejores prácticas, para brindar esa protección. Si no pasa por nosotros, es muy probable que no se consideren algunos aspectos".

7. **¿Las agencias externas deben cumplir con estándares de seguridad específicos antes de entrega algún proyecto?**

   "Hay aspectos que deben de cumplirse cuando son cuando pasan por la dirección de tecnología. Por ejemplo, a nivel de arquitectura hay temas que deben de considerarse a nivel de cumplimiento con estándares específicos. Eso a nivel de la dirección de tecnología está claro, como te digo, va a depender mucho de qué tan involucrado esté la dirección. El punto crucial y la mayor debilidad que existe en esto es cuando una empresa de publicidad que su naturaleza no necesariamente es el desarrollo de un sitio web porque ellos lo que utilizan normalmente son administradores de contenido, no son sitios webs, van y modifican un administrador de contenido dándole las características que requieren la cooperativa y se deja de lado todos los aspectos técnicos y de seguridad que deben de considerarse para brindar la protección necesaria. Casi siempre las agencias subcontratan un tercero para el desarrollo el web, y la Cooperativa no tiene un contrato con ese tercero, lo que complica la revisión más detallada".

Sección 3: Evaluación de Seguridad y Procesos de Mejora

8. **¿Se realizan auditorías o revisiones de seguridad antes de lanzar un desarrollo web al público?** *"Sí, se solicita una revisión, para verificar si tienen posibles vulnerabilidades y se le informa a Mercadeo para que ellos puedan estar al tanto de la situación".*
9. **¿Han identificado vulnerabilidades en desarrollos web previos? ¿Cómo han sido manejadas y corregidas?**

   "Sí, se han identificado. Parte del proceso, es que no se aceptan vulnerabilidad altas o medias, con el objetivo de que el sitio pueda estar en producción, sin ninguna brecha para evitar cualquier ataque. A no ser que sea un caso muy específico, y que esté con la debida justificación y que también el negocio pueda asumir ese riesgo. En este caso los directores toman el riesgo correspondiente de la brecha que se está identificando dentro del sitio".

10. **¿Se ejecutan pruebas de seguridad como evaluación de código o pruebas de carga en los desarrollos web?**

    "Sí, de hecho, se hacen pruebas de análisis estático, dinámico y dependencias de librerías con terceros. Todo esto se realiza actualmente".

11. **¿Existe un procedimiento de aprobación final antes del lanzamiento de un sitio web creado por alguna agencia externa a Dos Pinos?**

    "Hay procedimientos para todos sitios, pero cuando este dentro de la Dirección de TI, en el caso específicos de agencias y proveedores, que hacen desarrollos más temporales, que son de terceros. En estos temas, nosotros no tenemos no tenemos controles".

Sección 4: Monitoreo y Mejoras en Seguridad

12. **¿Cómo se monitorean los desarrollos web luego de su lanzamiento para identificar posibles fallos de seguridad? "***Hay monitoreos y procesos de análisis de vulnerabilidades, con aplicaciones propias, hacemos pruebas apoyados de consultorías. Estas son las acciones que realizamos. Y tenemos algunos servicios de inteligencia que constantemente nos informan de sitios que pueden estar con una posible vulnerabilidad, y verificar si esta alerta es real. Ya después de ahí, tomamos acciones".*

13. **¿Se realizan capacitaciones al personal de Mercadeo, TI sobre seguridad en desarrollos web y normativas aplicables?** *"Solo se ha dado capacitaciones al equipo de TI. De momento al departamento de Mercadeo no se la ha brindado ninguna capacitación sobre ese tema".*

14. **¿Qué mejoras considera necesarias para fortalecer la seguridad en los desarrollos web del Departamento de Mercadeo?**

    "Que nos involucren en el proceso. Es primordial que mercadeo tenga conocimiento de las posibles brechas que puedan generarse a través de desarrollos de terceros de los cuales la Cooperativa no tiene administración".

15. **¿Cómo evalúa el cumplimiento actual de las agencias externas en términos de seguridad y normativas aplicadas?** *"Súper bien, y hemos trabajado muy de la mano cuando nos permiten involucrarnos en el proceso".*