Gobierno Bolivariano de Venezuela | Ministerio del Poder Popular para Ciencia y Tecnología | Diplomado para la Gestión de las Tecnologías de Información y la Comunicación

DISEÑO DE PROTOCOLOS DE SEGURIDAD A NIVEL DE CÓDIGO Y PROCEDIMIENTOS EN EL DESARROLLO DE APLICACIONES DEL OBSERVATORIO NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN.

Nombres y Apellidos del (de la) participante: Carlos Rafael Marrero Muñoz

Cédula de Identidad: V-7920566

Correo Electrónico: marrero.c@gmail.com

Teléfono: 04242093147

Docente Mediador: David Silva

Caracas, noviembre de 2024

Diplomado para la Gestión de las Tecnologías de Información y la Comunicación

VISTO BUENO DEL DOCENTE MEDIADOR

En mi carácter de Docente Mediador del Caso de Estudio presentado por el(la) ciudadano(a): Carlos Rafael Marrero Muñoz, portador de la Cédula de Identidad N.º: V-7920566 como requisito de egreso del Diplomado para la Gestión de las Tecnologías de Información y la Comunicación, Titulado: Diseño de protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones del Observatorio Nacional de Ciencia, Tecnología e Innovación.; considero que dicho Caso de Estudio reúne los requisitos y méritos suficientes para ser desarrollado tal como se describe en el presente documento.

En la Ciudad de Caracas, a los _____ del mes de _____ de 202_

(Firma del Docente Mediador)

_____

(Nombre(s) y Apellido(s))

(C.I. N.º: _____)

CONTENIDO

Descripción de la situación problemática

Desde el año 2022, se ha identificado una deficiencia en las medidas de seguridad y protección tanto a nivel de código como procedimental, en el desarrollo y despliegue de los aplicativos utilizados para la recolección y procesamiento de información. Este problema tiene su origen en la falta de políticas y lineamientos de seguridad de código y procedimientos homologados por parte de la Coordinación de Desarrollo de Aplicaciones, manifestándose en la Gerencia de Tecnologías de Información y Comunicación del Observatorio Nacional de Ciencia, Tecnología e Información (ONCTI).

La falta de protocolos de seguridad adecuados afecta principalmente a la Gerencia de Tecnologías de Información y Comunicación, pero potencialmente puede tener un impacto negativo en todas las áreas del ONCTI que estén involucradas en el manejo y análisis de la información recabada. Esta situación puede comprometer la integridad de la información, generando resultados inexactos en los análisis y procesamientos realizados sobre los datos, así como potencial vulnerabilidad de los sistemas informáticos como tal.

La solución a este problema requiere la formulación de medidas y controles de seguridad robustos y homologados, tanto a nivel de código como en los procedimientos. Esto garantizaría la confiabilidad, integridad y coherencia de la información recolectada, así como su confidencialidad, protegiendo a la institución de futuros riesgos y asegurando la calidad de los datos procesados.

Preguntas (general y específicas)

Pregunta general:

¿Cuáles son los riesgos de no contar con protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones del Observatorio Nacional de Ciencia, Tecnología e Innovación?

Preguntas específicas:

1. ¿Qué ocurre?

   Deficiencia en las medidas de seguridad y protección tanto a nivel de código como procedimental en el desarrollo y despliegue de los aplicativos de recolección y procesamiento de información

2. ¿Quién lo genera?

   La Coordinación de Desarrollo de Aplicaciones

3. ¿Desde cuándo ocurre?

   Desde el año 2022

4. ¿Dónde ocurre?

   En la Gerencia de Tecnologías de Información y Comunicación del Observatorio Nacional de Ciencia, Tecnología e Información (ONCTI)

5. ¿A quién afecta?

   En principio, a la Gerencia de Tecnologías de Información y Comunicación; potencialmente afecta a todas las áreas del ONCTI involucradas con el manejo y análisis de la información recolectada

6. ¿Cuál es el impacto?

   Posibilidad de que al verse comprometida la información recabada, los análisis y procesamientos de la misma arrojen resultados inexactos

7. ¿Cómo podría solucionarse el problema?

   Implementando protocolos y controles de seguridad, tanto a nivel de código como procedimental, en los aplicativos de recolección y procesamiento de la información que garanticen al máximo la confiabilidad, integridad y coherencia de la información obtenida, así como su confidencialidad y resguardo.

Objetivos (general y específicos)

Objetivo general:

Proponer protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI), que aseguren la confidencialidad, integridad, disponibilidad y autenticidad de los datos.

Objetivos específicos:

1. Realizar un diagnóstico detallado de las vulnerabilidades de seguridad en los sistemas actuales del ONCTI.

2. Realizar una revisión teórico conceptual de los aspectos involucrados en la propuesta de protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del Observatorio Nacional de Ciencia, Tecnología e Innovación, analizando las mejores prácticas de seguridad en el desarrollo de aplicaciones web, incluyendo estándares internacionales, así como resoluciones y recomendaciones de organismos de ciberseguridad nacionales.

3. Diagnosticar los aspectos generales y estructurales relacionados a la propuesta de protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del Observatorio Nacional de Ciencia, Tecnología e Innovación.

4. Diseñar los protocolos de seguridad a nivel de código y procedimientos que aborden vulnerabilidades identificadas, en el desarrollo de aplicaciones web del Observatorio Nacional de Ciencia, Tecnología e Innovación, categorizados por Generales, Estructurales, de Programación y Funcionales

5. Implementar pruebas de penetración y auditorías de seguridad para validar la efectividad de los protocolos de seguridad diseñados en un entorno controlado.

6. Capacitar al equipo de desarrollo del ONCTI sobre las mejores prácticas en seguridad informática, asegurando que los nuevos protocolos sean adoptados y aplicados

correctamente.

7. Monitorear y actualizar los protocolos de seguridad después de su implementación para mantener la protección ante nuevas amenazas y vulnerabilidades emergentes.

Justificación

En el mundo interconectado mediante sistemas y plataformas de información de hoy en día, el tema de la seguridad informática de dichos sistemas y plataformas, y el resguardo de la información manejada por los mismos, cobra por primera vez en la historia de la humanidad, una importancia crucial, siendo la guerra tecnológica y de información tan importante como la directamente bélica; Venezuela no escapa a esta situación; en efecto, Kaspersky Labs reportó durante el año 2023 más de 11.000 millones de ciberataques a Venezuela, principalmente a las plataformas del estado, siendo instituciones como el Consejo Nacional Electoral, Consejo Nacional Electoral (CNE), Conviasa, Ministerio Público (MP), Servicio Nacional Integrado de Administración Aduanera y Tributaria (Seniat), el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), Petróleos de Venezuela (PDVSA), el Banco Central de Venezuela (BCV) y el Tribunal Supremo de Justicia (TSJ) las más afectadas.

Más recientemente, en el año 2024 y en el marco de las Elecciones Presidenciales del 28 de julio de 2024, hubo una serie de ataques masivos, particularmente a la plataforma del CNE, estimándose en más de 30 millones de ataques por minuto; se reportaron ataques directos a al menos 26 instituciones del Estado Venezolano, estando otras 40 bajo investigación por haber sido objeto de ciberataques en sus respectivas plataformas tecnológicas, lo cual ha obligado al Estado a tomar una serie de medidas defensivas y de protección ante dichos ataques, tales como la creación del Consejo Nacional de Ciberseguridad, la activación del Plan Nacional de Ciberseguridad y la mejora en la infraestructura tecnológica de dichas instituciones.

De lo anterior se desprende la necesidad de implementar medidas de seguridad en las plataformas tecnológicas, ya que estos ataques están enmarcados en planes externos de desestabilización por parte de actores que poseen un fuerte poderíp tecnológico, lo que implica que, aun habiendo tenido su máxima expresión en las recientes elecciones presidenciales, no van a cesar, sino que, por el contrario, van a incrementar tanto su frecuencia como intensidad.

Debido a ello, es necesario reforzar la seguridad cibernética tanto a niveles de infraestructura como a nivel de software; los sistemas de información actuales deben ser revisados y auditados exhaustivamente con miras a una reingeniería orientada a prácticas y

procedimientos seguros y las nuevas aplicaciones deben tener la seguridad como parte crucial en el desarrollo de las mismas.

Por lo anteriormente expuesto y considerando la cambiante situación geopolítica debido a hechos que trascienden nuestras fronteras y la importancia estratégica de Venezuela a nivel de recursos naturales, se resalta la urgencia de fortalecer la seguridad informática en las instituciones públicas, como mecanismo de defensa primario de la soberanía nacional En el caso del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI), la implementación de protocolos de seguridad robustos es crucial para garantizar la confidencialidad, integridad y disponibilidad de los datos recolectados, procesados y analizados. Estos protocolos asegurarán que los sistemas sean resistentes a ataques, como inyecciones SQL, XSS, y otros tipos de vulnerabilidades comunes en aplicaciones web.

Además, la adopción de estándares internacionales como OWASP, ISO 27001, y NIST no solo contribuirá a mejorar la seguridad, sino que también permitirá al ONCTI mejorar la confianza de sus usuarios, instituciones asociadas y otras partes interesadas en la fiabilidad de sus sistemas tecnológicos. En un contexto donde la información y los datos son activos críticos, garantizar su seguridad también es una cuestión de responsabilidad institucional.

Desde una perspectiva económica, la inversión en la implementación de estos protocolos es una medida preventiva que reducirá los costos asociados a posibles incidentes de seguridad, tales como la pérdida de datos, daño a la reputación de la institución y la necesidad de correcciones post-ataque, que generalmente son más costosas que la inversión en prevención. La prevención también contribuye a optimizar los recursos internos, dado que reduce el tiempo de respuesta ante incidentes y minimiza las intervenciones de emergencia.

La implementación de protocolos de seguridad bien definidos proporcionará una base sólida para el crecimiento del ONCTI a largo plazo. A medida que la organización se enfrente a la creciente demanda de datos y sistemas interconectados, estos protocolos garantizarán que el ONCTI pueda manejar esta carga de manera segura, permitiendo una mayor interoperabilidad con otros organismos y asegurando que los datos sean procesados y compartidos de manera eficiente sin comprometer su seguridad.

Por último, la sustentabilidad del proyecto radica en su capacidad de adaptarse a nuevas amenazas; los protocolos no sólo serán diseñados para cubrir las vulnerabilidades actuales, sino que estarán enmarcados en un proceso continuo de actualización y monitoreo, asegurando que los sistemas se mantengan protegidos a medida que evolucionan los riesgos y las tecnologías.

En resumen, esta iniciativa de seguridad no solo protege los activos digitales del ONCTI, sino que también contribuye a fortalecer la infraestructura tecnológica nacional, mejorando su resiliencia y posicionamiento estratégico frente a amenazas cibernéticas que podrían comprometer la estabilidad de los sistemas de información del Estado.

Delimitación

El presente Caso de Estudio se delimita dentro de los siguientes parámetros:

- Delimitación temporal: abril 2024- septiembre 2024

- Delimitación espacial: se concreta en los espacios del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI), específicamente en el área de programación, dejando de lado en el presente caso de estudio los aspectos de infraestructura.

- Delimitación Temática: Se aborda la temática referida a la utilización de protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del Observatorio Nacional de Ciencia, Tecnología e Innovación.

- Delimitación Metodológica: Se trata de un Caso de Estudio, que parte de un enfoque empírico que toma como apoyo una investigación documental, observacional y cuasi experimental.

Bases Teóricas y Conceptuales del Caso de Estudio

La seguridad en el desarrollo de aplicaciones web es un componente esencial para garantizar la protección de los datos y la robustez de los sistemas frente a ataques. En el caso del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI), el objetivo principal es tanto prevenir ataques al código como asegurar la integridad de los datos recolectados y procesados. Dado que las aplicaciones están orientadas principalmente a la obtención y gestión de datos, el diseño e implementación de protocolos de seguridad son críticos para evitar compromisos que podrían afectar la calidad y veracidad de la información utilizada.

1. Riesgos y amenazas potenciales

   Aunque hasta el momento no se han registrado incidentes de ciberseguridad a nivel de aplicaciones dentro del ONCTI, la creciente amenaza de ciberataques que ha experimentado el Estado venezolano representa un riesgo tangible. La ausencia de ataques previos no debe interpretarse como inmunidad, sino como una oportunidad para fortalecer las defensas antes de que ocurran incidentes que comprometan la confidencialidad, integridad o disponibilidad de los datos.

   El panorama actual presenta varios retos: no se siguen estándares de seguridad formales, y cada desarrollador trabaja de manera individual sin un enfoque normado o homologado. Esto incrementa la superficie de ataque, al carecer de un enfoque centralizado que asegure la implementación de buenas prácticas en el desarrollo.

2. Seguridad en el ciclo de vida del desarrollo de software (SDLC)

   El ciclo de vida de desarrollo de software (SDLC) debe integrar la seguridad en todas sus fases: desde la planificación hasta el mantenimiento. Sin embargo, en el ONCTI, no se realizan actualizaciones de seguridad ni revisiones post-despliegue, lo que deja las aplicaciones expuestas a posibles vulnerabilidades no detectadas en su fase inicial.

   Es deseable implementar procesos de mantenimiento continuo que incluyan revisiones periódicas y parches de seguridad a medida que nuevas vulnerabilidades sean descu-

biertas. Además, se debería realizar la adopción de metodologías que permitan la integración continua (CI) y la entrega continua (CD), favoreciendo un ciclo de desarrollo más controlado y eficiente.

3. Confidencialidad, Integridad, Disponibilidad, Autenticidad y No Repudio
    - La confidencialidad es el principio que garantiza que la información solo esté accesible para aquellos usuarios o sistemas que tienen autorización para acceder a ella. Es un pilar esencial en la protección de datos sensibles y privados.
        - Cifrado de datos: Utilizar técnicas de cifrado como AES (Advanced Encryption Standard) o TLS (Transport Layer Security) para proteger los datos en tránsito y en reposo. El cifrado asegura que, incluso si un atacante intercepta los datos, no pueda leer ni modificar la información.
        - Autenticación y control de acceso: Implementar mecanismos robustos de autenticación (como autenticación multifactor) y control de acceso basado en roles (RBAC - Role-Based Access Control) para garantizar que solo los usuarios autorizados puedan acceder a información específica.
        - Encriptación de credenciales. Las credenciales deben ser cifradas utilizando técnicas como bcrypt para proteger contraseñas; adicionalmente, las sesiones deben ser protegidas con tokens de acceso seguros como JWT (JSON Web Tokens), que garantizan que la información sensible no quede expuesta.
    - La integridad asegura que los datos no sean alterados o corrompidos de manera no autorizada, tanto en tránsito como en reposo. Cualquier cambio en los datos debe ser realizado de manera controlada y autorizada.
        - Sumas de verificación y hashes: Usar algoritmos como SHA-256 o MD5 para generar sumas de verificación (hashes) de los datos. Esto permite verificar si los datos han sido modificados durante su almacenamiento o transmisión.
        - Firmas digitales: Utilizar firmas digitales para garantizar la autenticidad de los datos y verificar que estos no hayan sido alterados por partes no autorizadas. En Venezuela, la Superintendencia de Certificación Electrónica (SUSCERTE) se encarga de acreditar, certificar y autorizar a los

proveedores de servicios de certificación electrónica, en la actualidad existen dos proveedores acreditados por SUSCERTE: La Fundación Instituto de Ingeniería, perteneciente al sector público, y la empresa privada PROCERT C.A.; recordemos que la validez legal de las firmas electrónicas se encuentra avalada por el artículo 16 de la Ley de Mensajes de Datos y Firmas Electrónicas y el Decreto Ley 1.204, el cual tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico

- La autenticidad garantiza que tanto los usuarios como los sistemas puedan verificar que los datos o las transacciones provienen de una fuente legítima y no han sido manipulados.
    - Certificados digitales: Usar certificados SSL/TLS para autenticar la identidad de los servidores y cifrar las comunicaciones entre los clientes y el servidor.
    - Autenticación de dos factores (2FA): Reforzar la autenticidad de los usuarios mediante la autenticación de dos factores, que exige una segunda forma de verificación.
- . El principio de no repudio asegura que, una vez que se ha realizado una acción (por ejemplo, una transacción o modificación de datos), ninguna de las partes involucradas pueda negar haber realizado dicha acción.
    - Registros de auditoría: Mantener un registro detallado de las acciones de los usuarios y de las transacciones realizadas en el sistema. Los registros deben ser inmutables y almacenados en sistemas seguros.
    - Firmas electrónicas: Implementar firmas electrónicas para garantizar que las transacciones sean legalmente vinculantes y no puedan ser negadas posteriormente.

4. Estándares y normativas de seguridad

Actualmente, el ONCTI no sigue ningún estándar de seguridad específico, lo que deja un vacío en la implementación de prácticas comunes que aseguren la robustez de las aplicaciones. Se recomienda alinear los procesos de desarrollo con estándares reconocidos, como:

- OWASP (Open Web Application Security Project): es una comunidad sin fines de lucro que se dedica a mejorar la seguridad de las aplicaciones web mediante la creación de recursos gratuitos, como guías, herramientas y listas de vulnerabilidades comunes. El proyecto más importante de OWASP es la OWASP Top 10, que enumera las principales amenazas para la seguridad de las aplicaciones web y proporciona prácticas recomendadas para mitigar estas amenazas
    - . Los protocolos de seguridad deben alinearse con las mejores prácticas que promueve OWASP, especialmente con respecto a la prevención de inyecciones SQL, gestión segura de sesiones, validación y sanitización de entradas y la protección contra XSS y CSRF.
    - El OWASP ASVS (Application Security Verification Standard) puede ser utilizado para realizar auditorías de seguridad a las aplicaciones y asegurarse de que estén protegidas contra las vulnerabilidades más comunes.
- ISO/IEC 27001: Es un estándar internacional para la gestión de la seguridad de la información. Esta norma define los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) dentro del contexto de la organización. La norma está diseñada para proteger la confidencialidad, integridad y disponibilidad de la información dentro de una organización
    - . Implementar un SGSI en el ONCTI puede ayudar a sistematizar el enfoque hacia la seguridad de la información, asegurando que todas las fases del ciclo de vida de las aplicaciones se alineen con prácticas de seguridad internacionalmente reconocidas.
    - El control de acceso a la información sensible, la gestión de riesgos y la auditoría de sistemas son algunos de los elementos clave de la ISO/IEC 27001 que pueden ser adoptados para mejorar la seguridad
- NIST (National Institute of Standards and Technology): proporciona directrices detalladas sobre la ciberseguridad, siendo su publicación más conocida el NIST Cybersecurity Framework, que es un conjunto de directrices destinadas a ayudar a las organizaciones a gestionar los riesgos relacionados con la seguridad cibernética

- . Se puede adoptar el marco NIST para evaluar, gestionar y reducir los riesgos cibernéticos. Esto incluye aspectos como la gestión de accesos, la detección de intrusos y la recuperación ante desastres.
- Además, el NIST SP 800-53, que proporciona un conjunto de controles de seguridad, puede ser utilizado para fortalecer la seguridad operativa de las aplicaciones.

- GDPR (Reglamento General de Protección de Datos): Aunque el GDPR es una normativa de protección de datos diseñada principalmente para la Unión Europea, su alcance global lo convierte en un estándar clave para cualquier organización que maneje datos personales de ciudadanos europeos. El GDPR establece normas estrictas sobre la recopilación, el procesamiento y la protección de datos personales.
  - Establece el derecho de los usuarios a la privacidad y la protección de datos, la notificación de violaciones de seguridad y la minimización de datos.
  - Asegurar la anonimización de los datos sensibles es una buena práctica recomendada por el GDPR.

La adopción de estas normativas no solo fortalecería la seguridad, sino que también formalizaría procesos que ahora se realizan de manera ad-hoc y no estandarizada.

5. Análisis de riesgos y amenazas más comunes en las aplicaciones web

Hay una serie de riesgos y amenazas comunes en aplicaciones web que deben analizadas e implementadas en estas aplicaciones; un entendimiento profundo de las mismas es esencial para diseñar soluciones de seguridad efectivas que protejan los sistemas del ONCTI. A continuación, se amplía este análisis con un enfoque detallado en cada tipo de amenaza y las estrategias para mitigar cada una de ellas:

- La inyección SQL ocurre cuando un atacante introduce código SQL malicioso a través de campos de entrada (por ejemplo, formularios web) que no son correctamente validados o sanitizados. Este ataque puede permitir al atacante ejecutar comandos SQL directamente en la base de datos, lo que puede resultar en acceso no autorizado a información sensible, modificación o eliminación de datos

importantes o escalamiento de privilegios si el atacante puede acceder o manipular las credenciales de administrador; la inyección de SQL se puede prevenir mediante:

- Consultas parametrizadas: Usar consultas SQL parametrizadas para asegurar que los parámetros proporcionados por los usuarios no sean tratados como código. Esta es la forma más segura de interactuar con la base de datos.
- ORMs (Object-Relational Mappers): Utilizar frameworks ORM que gestionan automáticamente la sanitización de las consultas SQL y adicionalmente hacen abstracción del motor de bases de datos utilizados; el uso de ORMs tiene la ventaja adicional de facilitar la portabilidad y el escalamiento.
- Validación de entrada: Sanear los datos de entrada mediante la validación y el escape de caracteres peligrosos, especialmente cuando se introducen directamente en las consultas SQL.

- El Cross-Site Scripting (XSS) ocurre cuando un atacante inyecta código JavaScript malicioso en una página web que es luego ejecutado por otros usuarios. Este ataque se utiliza generalmente para el robo de cookies de sesión o credenciales de usuario, la redirección a sitios maliciosos o modificar de la apariencia de la página web, generando un engaño para el usuario.
  - Escapar contenido dinámico: Asegurarse de que todo el contenido introducido por el usuario (como comentarios, entradas de formularios, etc.) sea escapado adecuadamente para que no se ejecute como código JavaScript. Esto se puede hacer utilizando funciones de escape en el lado del servidor y cliente.
  - Uso de Content Security Policy (CSP): Implementar una política de seguridad de contenido (CSP) que limite los orígenes de scripts, evitando la ejecución de scripts no confiables.
  - Validación y filtrado de entrada: Rechazar cualquier entrada que contenga etiquetas HTML o JavaScript no permitidas.
  - Evitar el uso comandos de interpretación de texto, tales como eval() en javascript o $$ en PHP ya que los mismos interpretan el texto que se les pasa como comandos de los lenguajes correspondientes.

- El Cross-Site Request Forgery (CSRF) es un ataque en el que un atacante engaña a un usuario legítimo para que ejecute acciones no deseadas en una aplicación web en la que está autenticado. Si un usuario tiene una sesión activa en un sitio vulnerable, el atacante puede enviar solicitudes maliciosas que, si no están protegidas, serán ejecutadas en el contexto de la sesión del usuario.
    - Tokens CSRF: Implementar tokens de protección CSRF. Estos tokens son únicos para cada sesión y cada formulario, y deben ser enviados en cada solicitud que modifique el estado en el servidor.
    - Validación de Origen: Asegurar que las solicitudes solo provengan de fuentes legítimas utilizando encabezados Referer y Origin.
    - Métodos HTTP seguros: Evitar que acciones críticas se realicen a través de métodos GET. Utilizar siempre métodos POST, PUT o DELETE para operaciones que cambien el estado del servidor.
- La gestión insegura de sesiones puede permitir a los atacantes secuestrar o falsificar sesiones de usuario. Esto puede ocurrir por diversas razones, como la transmisión de cookies sin cifrar, la falta de invalidación de sesión después de que un usuario cierre sesión o la previsibilidad de identificadores de sesión.
    - Cookies seguras: Utilizar el atributo HttpOnly para que las cookies no sean accesibles mediante JavaScript, y Secure para asegurar que las cookies solo se transmitan a través de conexiones seguras (HTTPS).
    - Caducidad y revocación de sesiones: Establecer un tiempo de expiración de sesión adecuado y revocar sesiones después de un periodo de inactividad.
    - Autenticación multifactor (MFA): Implementar MFA para reducir el riesgo de acceso no autorizado a las cuentas, incluso si se obtiene la cookie de sesión.
    - Protección contra el secuestro de sesión: Asegurarse de que las sesiones no sean vulnerables a ataques como session fixation, donde un atacante fija un ID de sesión antes de que el usuario inicie sesión.
- Las aplicaciones web modernas dependen en gran medida de librerías de terceros y frameworks externos. Estas dependencias pueden contener vulnerabilidades no detectadas que, si no se actualizan o gestionan correctamente, pueden ser explotadas por atacantes.

  - Gestión de dependencias: Utilizar herramientas como npm audit, composer audit o Snyk para auditar y gestionar las dependencias, y actualizar regularmente las librerías a versiones libres de vulnerabilidades conocidas.
  - Principio de "mínimos privilegios": Asegurarse de que las librerías y dependencias solo tengan acceso a los recursos estrictamente necesarios para su funcionamiento.
  - Evaluación de seguridad: Antes de integrar una librería o framework en la aplicación, realizar una evaluación de seguridad para verificar su fiabilidad y evaluar sus riesgos inherentes.
- Los ataques DoS/DDoS intentan hacer que un servidor, servicio o red sea inaccesible mediante el envío de un volumen masivo de tráfico o solicitudes maliciosas, lo que sobrecarga el sistema.
  - Distribución de carga (Load Balancing): Utilizar balanceadores de carga para distribuir las solicitudes entrantes a través de varios servidores, reduciendo la posibilidad de que un solo servidor se vea sobrecargado.
  - CDN y protección contra DDoS: Implementar una red de entrega de contenido (CDN) con medidas integradas de mitigación de DDoS, como las ofrecidas por Cloudflare o AWS Shield.
  - Limitar la tasa de solicitudes: Usar mecanismos de rate limiting para restringir la cantidad de solicitudes que un usuario o dirección IP puede realizar en un corto período de tiempo.
- Una configuración incorrecta o insegura de los servidores, bases de datos y aplicaciones web puede exponer datos sensibles o permitir que los atacantes obtengan acceso a recursos críticos.
  - Configuración segura: Asegurar que los servidores web y bases de datos no expongan información innecesaria, como detalles de errores o configuraciones predeterminadas.
  - Revisión de seguridad en el ciclo de vida: Implementar procesos de auditoría de configuración de seguridad durante el ciclo de vida del desarrollo y en cada nuevo entorno de producción.

- Uso de herramientas de configuración automática: Herramientas como Chef o Ansible para automatizar la implementación de configuraciones seguras.

6. Desarrollo Seguro (SDL)

. EL Desarrollo Seguro (SDL – Secure Development Lifecycle) es un enfoque de desarrollo de software que integra las mejores prácticas de seguridad en cada fase del ciclo de vida del software, desde la planificación y el diseño hasta las pruebas y el mantenimiento. La idea principal es identificar, mitigar y prevenir las vulnerabilidades de seguridad de forma temprana en el proceso de desarrollo, en lugar de intentar remediarlas después de que la aplicación esté en producción. El objetivo del SDL es garantizar que la seguridad sea una parte integral del proceso de desarrollo y que no se trate como una consideración secundaria o posterior. Sus fases son:

- Planificación: Identificación de los requisitos de seguridad y la creación de una estrategia de seguridad.
  - Evaluación de riesgos: Identificar amenazas potenciales que puedan afectar a las aplicaciones, como ciberataques, pérdida de datos o fallos de infraestructura.
  - Definición de políticas de seguridad: Establecer políticas claras sobre gestión de contraseñas, accesos de usuario, protección de datos sensibles y respuesta ante incidentes.
  - Planificación de la integración de la seguridad en el ciclo de vida del software.
- Diseño: Incorporación de medidas de seguridad en la arquitectura de la aplicación; en esta fase, se integran controles de seguridad en la arquitectura y el diseño de la aplicación, lo cual incluye:
  - Modelado de amenazas: Anticipar posibles vectores de ataque, como inyecciones SQL, XSS o CSRF, y diseñar defensas adecuadas.
  - Definición de controles de acceso: Garantizar que solo los usuarios autorizados tengan acceso a funciones y datos sensibles.
  - Diseño de resiliencia: Asegurarse de que la aplicación sea capaz de resistir y recuperarse de ciberataques.
- Desarrollo: Implementación de código seguro y validación constante, utilizando las mejores prácticas de seguridad, entre las que se incluye:

- Codificación segura: Evitar el uso de funciones inseguras que puedan introducir vulnerabilidades.
- Validación de entradas: Validar y sanear todas las entradas de los usuarios para evitar inyecciones SQL, XSS y otras amenazas comunes.
- Control de versiones seguro: Usar herramientas como Git para mantener un control adecuado de los cambios en el código y garantizar que las versiones anteriores no presenten vulnerabilidades.

- Pruebas: Evaluación de la seguridad mediante pruebas dinámicas y estáticas antes de que el aplicativo sea desplegado, entre las cuales se encuentran:
  - Pruebas de penetración: Simular ataques para evaluar la seguridad de la aplicación.
  - Análisis dinámico: Evaluar el comportamiento de la aplicación durante la ejecución para encontrar vulnerabilidades no detectadas en el código fuente.
  - Revisión de código: Hacer revisiones de seguridad regulares al código para detectar posibles problemas.
- Despliegue: Implementación de controles de seguridad post-despliegue:
  - Configuración segura de servidores y bases de datos.
  - Implementación de parches de seguridad.
  - Revisión de configuraciones para asegurar que no haya puertos abiertos innecesarios o servicios no utilizados que puedan ser explotados.
- Mantenimiento y actualización: Evaluación continua y actualización de las aplicaciones para corregir vulnerabilidades a medida que surgen nuevas amenazas; entre las actividades a efectuar tenemos:
  - Monitoreo continuo: Supervisar el tráfico y las actividades del sistema en busca de anomalías.
  - Gestión de incidentes de seguridad: Tener procedimientos claros para responder a incidentes de seguridad.
  - Actualización de software: Asegurarse de que las aplicaciones se mantengan al día con las últimas correcciones de seguridad.

7. Herramientas y frameworks en uso

El stack tecnológico en el ONCTI incluye Python 3.7+, PHP 8.2+ y NodeJS 20.x para el backend, con los frameworks Flask y Django en el caso de Python, Laravel para el caso

de PHP y Express.js para el caso de NodeJS; en el frontend se utiliza HTML5 y Javascript Vanilla, con los frameworks Vue.js 3.x y Jquery 3.x; para los estilos, se usan los frameworks Bootstrap y Tailwind. Este conjunto de tecnologías ofrece una gran flexibilidad, pero también conlleva la necesidad de asegurar que cada componente sea protegido contra amenazas comunes:

Laravel y Django incluyen características integradas como la protección contra inyecciones SQL y Cross-Site Scripting (XSS), pero los desarrolladores deben asegurarse de que estas funciones estén correctamente habilitadas.

NodeJs es particularmente sensible a vulnerabilidades en los paquetes de terceros; es esencial realizar auditorías regulares de dependencias mediante herramientas como npm audit para identificar y corregir vulnerabilidades conocidas.

PostgreSQL, como motor de base de datos, debe estar configurado con políticas de acceso estrictas, utilizando cifrado en tránsito y en reposo para proteger la información crítica, así como el uso de un puerto no estándar.

8. Capacitación del equipo de desarrollo

   El equipo de desarrollo del ONCTI no ha recibido capacitación formal en prácticas de seguridad. Esto representa un riesgo considerable, ya que los desarrolladores pueden no estar al tanto de las mejores prácticas para proteger el código contra amenazas.

   Para mejorar la seguridad, se recomienda implementar programas de capacitación continua que incluyan:

   - Formación en seguridad de aplicaciones: Enseñando sobre vulnerabilidades comunes, cómo mitigarlas, y el uso de herramientas de análisis estático y dinámico del código.
   - Capacitación en estándares: Familiarizar al equipo con normativas como OWASP y ISO 27001.
   - Entrenamiento en criptografía: Asegurar que el equipo entienda cómo y cuándo aplicar técnicas de cifrado de datos.

9. Colaboración con SUSCERTE y auditorías de seguridad

El ONCTI colabora actualmente con SUSCERTE, una entidad encargada de evaluar la seguridad de las aplicaciones antes de su despliegue. Esta colaboración es un primer paso importante, pero para maximizar su efectividad, es esencial que el ONCTI también adopte una postura proactiva hacia la seguridad; para ello podemos indicar:

- Pruebas de penetración: Estas pruebas deben realizarse regularmente para identificar posibles vulnerabilidades que puedan ser explotadas.
- Revisiones de código: Implementar revisiones internas y externas de código, idealmente integradas en el ciclo de desarrollo, utilizando herramientas para ello herramientas de revisión que puedan integrarse en el código o bien puedan ser desplegadas como plataformas en servidores propios dentro de la misma red.
- Monitoreo post-despliegue: Aunque no se realizan actualmente, es fundamental implementar sistemas de monitoreo que permitan detectar anomalías en las aplicaciones después de su despliegue.

Lo anterior puede ser agrupado en las categorías de protocolos generales, protocolos estructurales, protocolos de programación y protocolos funcionales o procedimentales de la siguiente manera:

1. Protocolos Generales
   1.1. Estándares y normativas de seguridad
      1.1.1. Implementación de normativas como OWASP, ISO/IEC 27001 y NIST en el ciclo de vida del desarrollo.
      1.1.2. Adopción de Desarrollo Seguro, integrando principios de Seguridad por Diseño y Defensa en Profundidad.
      1.1.3. Establecimiento de políticas de seguridad en el ciclo de vida del desarrollo (SDLC), asegurando la revisión, actualización y auditoría continua del código.
      1.1.4. Capacitación del equipo de desarrollo
      1.1.5. Formación continua del equipo en mejores prácticas de seguridad, criptografía y gestión de dependencias.
      1.1.6. Capacitación en gestión de vulnerabilidades, prevención de ataques y uso de herramientas de auditoría de código.

1.1.7. Colaboración con entidades de auditoría interna

1.1.7.1. Colaboración con SUSCERTE para realizar auditorías de seguridad y pruebas de penetración en aplicaciones antes de su despliegue.

1.1.8. Revisión post-despliegue

1.1.8.1. Establecimiento de protocolos de monitoreo continuo de aplicaciones post-despliegue para detectar anomalías y realizar actualizaciones periódicas de seguridad.

2. Protocolos Estructurales

2.1. Diseño de sistemas robustos y segregación de servicios

2.2. Asegurar que las arquitecturas de aplicaciones sean modulares y seguras, minimizando la superficie de ataque mediante principios de separación de responsabilidades.

2.3. Segregación de bases de datos y capas de servicio para limitar el acceso a la información crítica, implementando políticas de cifrado en tránsito y en reposo.

2.4. Mantenimiento continuo y parches de seguridad

2.5. Implementación de un proceso de actualización continua de las bibliotecas y frameworks utilizados (Laravel, Flask, Django, Node.js, etc.), asegurando que se apliquen los parches de seguridad tan pronto como sean lanzados.

2.6. Monitoreo y pruebas de penetración

2.7. Implementar un sistema de monitoreo continuo de los sistemas, revisando logs y comportamientos anómalos para prevenir ciberataques.

2.8. Realización de pruebas de penetración periódicas para simular ataques y evaluar la resiliencia del sistema.

2.9. Autenticación multifactor (2FA)

2.10. Desarrollar una solución in-house para la autenticación de dos factores, que no dependa de servicios externos, utilizando tokens generados localmente o vía SMS dentro de la infraestructura interna.

2.11. Verificación de correo electrónico

2.12. Implementación de sistemas internos de verificación de correo que validen las direcciones de email antes de permitir el acceso a las aplicaciones, evitando la dependencia de servicios externos.

3. Protocolos de Programación

3.1. Uso de prácticas seguras en la programación, como el manejo adecuado de entradas del usuario, validación de formularios y protección contra ataques de inyección SQL y Cross-Site Scripting (XSS).

3.2. Implementación de análisis estático y dinámico del código para identificar vulnerabilidades durante el desarrollo.

3.3. Gestión de dependencias

3.4. Auditoría constante de las dependencias utilizadas en el backend (Laravel, Django, Node.js, Flask, etc.) con herramientas como npm audit o composer audit para identificar y solucionar vulnerabilidades de terceros.

3.5. Implementar soluciones de CAPTCHA propias para proteger formularios de accesos no autorizados, evitando la sobrecarga de tráfico malicioso en las aplicaciones.

3.6. Uso de algoritmos de cifrado robustos para almacenar información sensible, como contraseñas o datos personales, utilizando técnicas como bcrypt o Argon2.

3.7. Aplicación de medidas de validación estricta para los datos que ingresa el usuario, minimizando la posibilidad de ataques de inyección de código.

4. Protocolos Funcionales o Procedimentales

4.1. Establecer un sistema de revisión de código colaborativa para asegurar que todas las contribuciones sean evaluadas con un enfoque en seguridad.

4.2. Uso de herramientas y plataformas de despliegue local para realizar análisis automatizados del código en busca de posibles vulnerabilidades.

4.3. Implementación de gestión segura de sesiones, asegurando el cifrado de cookies y tokens de autenticación, así como la configuración de timeouts de sesión para prevenir accesos no autorizados.

4.4. Desarrollar procedimientos para realizar actualizaciones regulares en las aplicaciones después de su despliegue, asegurando la corrección de vulnerabilidades a medida que se descubren.

4.5. Establecer una política de mantenimiento continuo, que incluya revisiones programadas y pruebas de seguridad constantes.

4.6. Gestión de acceso y privilegios

4.7. Aplicación de un sistema de control de acceso basado en roles (RBAC) para garantizar que solo los usuarios autorizados puedan acceder a ciertas funcionalidades o datos críticos dentro de las aplicaciones.

4.8. Auditoría continua de permisos y accesos para detectar posibles errores en la asignación de roles.

4.9. Auditoria y loggin de las acciones en la base de datos, mediante triggers automáticos de las acciones INSERT, UPDATE y DELETE en el motor de bases de datos

4.10. Auditoria y loggin de los ingresos y egresos de los usuarios, así como los intentos fallidos de ingreso y las salidas por vencimiento de sesión, que incluyan la dirección ip desde la cual se hizo el ingreso o el intento fallido de ingreso

Marco legal y administrativo del Caso de Estudio

La implementación de protocolos de seguridad en el desarrollo de aplicaciones del Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI) debe sustentarse en un sólido marco legal, conforme a la normativa venezolana vigente. Este marco incluye leyes, reglamentos y disposiciones vinculadas a la protección de la información, seguridad cibernética y gestión de tecnologías de la información y comunicación (TICs) en organismos del Estado.

1. Constitución de la República Bolivariana de Venezuela (CRBV)
   1.1. El marco legal base en Venezuela se encuentra en la Constitución de la República Bolivariana de Venezuela (CRBV), la cual establece los derechos fundamentales que protegen la privacidad y la seguridad de la información. Entre los artículos relevantes destacan:

   1.2. Artículo 28: Garantiza a los ciudadanos el acceso a la información personal almacenada en registros oficiales y prohíbe el uso de tecnologías de la información que atenten contra la intimidad de las personas.

   1.3. Artículo 60: Establece el derecho a la privacidad, prohibiendo interferencias arbitrarias en la vida privada de los ciudadanos y el uso indebido de la información personal.

   1.4. Artículo 110: Declara que el Estado garantizará el desarrollo de la ciencia, la tecnología, el conocimiento y la innovación en función del interés general, además de asegurar el acceso a la información.

2. Ley de Infogobierno
   2.1. La Ley de Infogobierno (Gaceta Oficial N° 40.274 del 17 de octubre de 2013) establece normas para el uso de tecnologías de información por parte de los órganos y entes del Estado. Los siguientes aspectos de esta ley son aplicables a los protocolos de seguridad:

   2.2. Artículo 30: Indica que los órganos del Estado deben asegurar la confidencialidad, integridad y disponibilidad de la información, garantizando la protección adecuada contra accesos no autorizados, pérdidas o alteraciones.

2.3. Artículo 38: Obliga a la administración pública a cumplir con los estándares y normativas de seguridad de la información, lo que se relaciona con la adopción de protocolos de desarrollo seguro.

2.4. Artículo 44: Exige el uso de software libre en todos los desarrollos tecnológicos de la administración pública, siempre que sea posible, lo que podría influir en el tipo de licenciamiento de los protocolos desarrollados.

2.5. En este sentido, los protocolos de seguridad podrían licenciarse bajo una licencia de software libre, como la GNU General Public License (GPL), permitiendo su libre uso, modificación y distribución dentro del Estado, promoviendo su transparencia y adaptación conforme a las necesidades de seguridad.

3. Ley Orgánica de Telecomunicaciones

3.1. La Ley Orgánica de Telecomunicaciones (Gaceta Oficial N° 36.970 del 12 de junio de 2000) regula los servicios de telecomunicaciones, incluyendo aquellos que implican la transmisión y recepción de datos a través de redes públicas y privadas. Las disposiciones relevantes incluyen:

3.2. Artículo 17: Exige que los prestadores de servicios de telecomunicaciones adopten medidas de seguridad para proteger la privacidad de las comunicaciones, asegurando la integridad de los sistemas de información.

3.3. Artículo 37: Establece la necesidad de contar con medidas de protección cibernética, lo cual refuerza la obligatoriedad de los protocolos de seguridad en redes y sistemas de información de organismos públicos.

4. Ley Orgánica de Seguridad de la Nación

4.1. La Ley Orgánica de Seguridad de la Nación (Gaceta Oficial N° 37.594 del 18 de diciembre de 2002) promueve la protección y defensa del Estado venezolano, abarcando también aspectos de la seguridad de la información y el ciberespacio. Relacionada con los protocolos de seguridad, esta ley destaca:

4.2. Artículo 7: Define la seguridad de la nación como un conjunto de acciones orientadas a la protección de la integridad del territorio y de los recursos, lo que incluye la seguridad de la infraestructura tecnológica y la información del Estado.

4.3. Artículo 15: Establece que la defensa del Estado incluye el resguardo de los sistemas de información y la protección contra amenazas cibernéticas, especialmente en organismos estratégicos como el ONCTI.

5. Ley Orgánica de Ciencia, Tecnología e Innovación (LOCTI)

5.1. La Ley Orgánica de Ciencia, Tecnología e Innovación (LOCTI) (Gaceta Oficial N° 6.151 del 18 de noviembre de 2014) regula el desarrollo de la ciencia, la tecnología y la innovación en Venezuela, promoviendo la soberanía tecnológica. Los aspectos relevantes para la seguridad incluyen:

5.2. Artículo 9: Establece que los desarrollos tecnológicos financiados por el Estado deben garantizar la seguridad y soberanía tecnológica.

5.3. Artículo 10: Promueve la innovación segura y la creación de tecnologías que resguarden los recursos estratégicos del país, como la información recolectada por el ONCTI.

6. Regulaciones y Directrices de SUSCERTE

6.1. La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) es el ente encargado de regular los sistemas de seguridad informática y ciberseguridad en Venezuela. SUSCERTE emite directrices sobre certificación de seguridad, firmas electrónicas y protección de datos en sistemas informáticos. Dentro de las regulaciones aplicables, destacan:

6.2. Resolución 025: Establece los lineamientos de ciberseguridad para organismos públicos, que deben seguir estándares internacionales de seguridad como los de ISO 27001.

6.3. Normas para la protección de infraestructura crítica: Incluyen la protección de bases de datos y sistemas de comunicación, lo cual es crucial en los desarrollos de aplicaciones del ONCTI.

7. Centro Nacional de Tecnologías de Información (CNTI)
   7.1. El CNTI emite normativas y directrices sobre el uso de tecnologías de la información y promueve la adopción de software libre en la administración pública. Las normas del CNTI relacionadas con seguridad incluyen:

   7.2. Política Nacional de Seguridad de la Información: Establece los criterios para la gestión de seguridad en entornos tecnológicos del Estado, incluyendo la auditoría, control de acceso y mantenimiento continuo de las aplicaciones y sistemas.

   7.3. Directrices de software libre: Promueven la utilización de software bajo licencias abiertas, lo que respalda la adopción de protocolos de seguridad licencias como la GPL o AGPL, que garantizan la transparencia y control del código.

8. El ONCTI, como ente de seguimiento de la política nacional en ciencia, tecnología e innovación, debe garantizar que los datos obtenidos y gestionados a través de sus sistemas y aplicaciones sigan principios de seguridad, privacidad y soberanía tecnológica. De acuerdo con las leyes mencionadas, el ONCTI tiene la obligación de implementar medidas de seguridad en sus aplicaciones para proteger la integridad y confidencialidad de la información, en línea con los objetivos de la LOCTI y la Ley de Infogobierno.
9. El Ministerio del Poder Popular para la Ciencia y Tecnología es responsable de la ciberseguridad en el ámbito de la ciencia y la tecnología en Venezuela. Las políticas del MPPCyT relacionadas con la ciberseguridad y protección de la información abarcan la creación de un ecosistema tecnológico soberano que garantice la seguridad de la infraestructura crítica, como las aplicaciones desarrolladas por el ONCTI; en conjunto con SUSCERTE y CNTI, dicta las normas y estándares que deben seguirse para asegurar que los desarrollos tecnológicos del Estado estén protegidos contra amenazas cibernéticas y cumplan con los requisitos de confidencialidad, integridad y disponibilidad.
10. De acuerdo con el Artículo 44 de la Ley de Infogobierno, el uso de software libre es obligatorio en la administración pública venezolana. Por lo tanto, los protocolos de seguridad desarrollados en el contexto del ONCTI deben licenciarse bajo una licencia de software libre, como la GNU General Public License (GPL) o la GNU Affero General Public License (AGPL). Estas licencias garantizan:

10.1.1. Transparencia: El código fuente estará disponible para ser examinado y auditado por cualquier usuario del Estado.

10.1.2. Adaptabilidad: Se permite la modificación del código para adecuarlo a nuevas amenazas y necesidades.

10.1.3. Redistribución: El software puede ser distribuido a otros entes del Estado o a comunidades interesadas en su adopción.

Relación entre el Marco Legal y las Bases Teóricas

Desde una perspectiva teórica, los protocolos de seguridad deben abordar aspectos esenciales como la confidencialidad, integridad, disponibilidad, autenticidad y no repudio, que son pilares fundamentales de la seguridad de la información. Estos principios buscan asegurar que la información no sea accedida por usuarios no autorizados (confidencialidad), que los datos no sean alterados (integridad), que la información esté disponible cuando se necesite (disponibilidad), que se pueda verificar la identidad de las partes involucradas (autenticidad), y que no se puedan negar transacciones o acciones realizadas (no repudio). A partir de estos conceptos, la implementación de prácticas como la encriptación de datos, el uso de firmas electrónicas, el control de accesos y la autenticación adquieren una importancia crítica.

Estas bases teóricas encuentran sustento en el marco legal venezolano. Por ejemplo, la Ley de Infogobierno en su artículo 30 establece la obligatoriedad de asegurar la confidencialidad, integridad y disponibilidad de la información en los órganos del Estado, alineándose directamente con los principios teóricos de la seguridad de la información. La exigencia de garantizar la protección contra accesos no autorizados y el uso de tecnologías seguras resalta la necesidad de aplicar controles rigurosos, como el uso de certificación electrónica y mecanismos de autenticación robusta, aspectos que también son regulados por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) a través de normas de certificación y seguridad informática.

En cuanto al desarrollo de protocolos específicos, los sistemas de autenticación multifactorial o la validación de formularios mediante patrones de verificación son medidas alineadas con estos principios y pueden implementarse conforme a los lineamientos de la Ley de

Infogobierno, que prioriza la seguridad en la transmisión de información. Específicamente, los organismos públicos están obligados a cumplir con estándares nacionales e internacionales, tales como la ISO 27001 para la gestión de la seguridad de la información, como lo exige SUSCERTE en sus directrices. La aplicación de mecanismos como la validación de entrada de datos o la protección de redes internas mediante firewalls también responde a estas normativas.

Autenticación, Verificación y Protocolos de Seguridad

Desde el punto de vista práctico, los mecanismos de autenticación y verificación (por ejemplo, autenticación de dos factores o sistemas de captchas), aunque fundamentales en cualquier esquema de seguridad, deben ajustarse al marco legal vigente. En Venezuela, la adopción de tecnologías que dependen de plataformas externas, como los servicios de Google o redes globales, puede estar restringida por normativas que promueven el uso de tecnologías nacionales o de software libre, como lo establece el CNTI y la Ley de Infogobierno. De acuerdo con el Artículo 44 de la Ley de Infogobierno, el uso de software libre es prioritario en la administración pública venezolana, por lo que los protocolos de seguridad deben diseñarse con esta limitación en mente, optando por tecnologías que puedan ser desplegadas localmente y que cumplan con los criterios de soberanía tecnológica.

Protección de la Información y Soberanía Tecnológica

El concepto de soberanía tecnológica, fundamental en el marco de la Ley Orgánica de Ciencia, Tecnología e Innovación (LOCTI), se vincula directamente con la necesidad de desarrollar tecnologías que no dependan de proveedores externos o servicios que no puedan ser controlados por el Estado venezolano. Esta ley refuerza la importancia de que los desarrollos tecnológicos, incluidos los protocolos de seguridad, estén alineados con la protección de los recursos estratégicos del país, como los sistemas de información gestionados por el Observatorio Nacional de Ciencia, Tecnología e Innovación (ONCTI).

Por lo tanto, el marco legal y las bases teóricas de la seguridad de la información se complementan para asegurar que los sistemas y protocolos que se implementen en las aplicaciones del ONCTI, o cualquier otro organismo del Estado, cumplan con los más altos estándares de seguridad, manteniendo la confidencialidad y disponibilidad de la información

mientras se asegura la soberanía tecnológica. Al no depender de plataformas externas, el Estado garantiza que los datos críticos no estén sujetos a jurisdicciones extranjeras o a posibles amenazas de control externo.

Licenciamiento y Transparencia

Finalmente, en términos de licenciamiento de los protocolos de seguridad, el marco legal también establece que los desarrollos tecnológicos del Estado venezolano deben regirse bajo licencias de software libre, como la GPL (General Public License) o la AGPL (Affero General Public License). Estas licencias aseguran la transparencia en el código fuente, permitiendo que los protocolos de seguridad puedan ser auditados y mejorados por otros organismos o actores dentro de la administración pública, promoviendo la innovación abierta y asegurando el cumplimiento de los principios de seguridad de la información y soberanía que dicta la Ley de Infogobierno.

Marco Metodológico

Enfoque, Tipo y Modalidad de Investigación

El Caso de Estudio parte de un enfoque empírico que toma como apoyo una investigación documental, observacional y cuasi experimental de tipo cuantitativa.

Población y Muestra

La población, es el conjunto finito o infinito de personas o elementos que poseen características comunes cuya opinión es fundamental para reconocer necesidades, carencias o limitaciones en el entorno de estudio.

Por ejemplo: La cantidad total de trabajadores de una gerencia. Dicha población es finita y según Arias (2012), “la población finita es la agrupación en la que se conoce la cantidad de unidades que la integran” (p. 82).

Tabla 1: Distribución de la población de trabajadores

Trabajadores de la Oficina de Tecnologías de la Información y la Comunicación - ONCTI	Cantidad
Ingenieros(as)	2
Licenciados(as) en Computación	1
Programadores(as)	4
Total	7

Muestra

Se refiere a una porción o subconjunto de una población. Se selecciona a través del muestreo de probabilístico / aleatorio o de manera no probabilística o intencionada.

Arias (2012) define el muestreo probabilístico / aleatorio como aquel en el cual se calcula la probabilidad “que tiene cada elemento de integrar la muestra”.

Así mismo, Arias (2012) explica que el muestreo intencional u opinático es aquel en el cual “la selección de los elementos es escogidos con base en criterios o juicios de los investigadores” (p. 85)

Tabla 2: Distribución de la muestra de trabajadores seleccionada

Trabajadores de la Oficina de Tecnologías de la Información y la Comunicación - ONCTI	Cantidad
Ingenieros(as)	1
Licenciados(as) en Computación	1
Programadores(as)	2
Total	4

Técnicas e Instrumentos de Recolección de Datos

Para compilar la opinión de los trabajadores que conforman la muestra, deben establecerse las técnicas y los instrumentos que servirán como recolectores de tales datos.

Siguiendo con Arias (2012) “se entenderá por técnica, el procedimiento o forma particular de obtener datos o información” (p. 67), y el instrumento “es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información” (p. 69)

Validez y Confiabilidad

Todo instrumento de recolección de datos debe reunir dos requisitos fundamentales: validez y confiabilidad. Estas cualidades, minimizan posibles incidencias de error, sesgo o ambigüedad.

Validez

La validez asegura que el instrumento realizado realmente mida la variable definida. Asimismo, Arias (2012) enuncia que “la validez del cuestionario significa que las preguntas o ítems deben tener una correspondencia directa con los objetivos de la investigación. Es decir, las interrogantes consultarán sólo aquello que se pretende conocer o medir” (p.79).

Para ello se utiliza la técnica denominada Juicio de Expertos, la cual permite que los instrumentos sean evaluados de forma objetiva por especialistas en la materia, razón por la cual en el Anexo C se coloca un modelo.

Confiabilidad

La confiabilidad, asegura la consistencia de los datos obtenidos de parte de los individuos que forman parte de la muestra.
De acuerdo con el tipo de preguntas que se coloquen en el cuestionario, se calculará la confiabilidad. Si las preguntas son dicotómicas, se utilizará el coeficiente de confiabilidad de Kuder-Richardson. Si son son policotómicas, se utilizarán escalas tipo Likert, por lo tanto, se someten a la prueba de confiabilidad u homogeneidad del coeficiente Alfa de Cronbach.

Variables y dimensiones

Para el diseño de los cuestionarios, es necesario precisar las variables y las dimensiones que conforman el caso de estudio. En la tabla 3, se coloca un cuadro de operacionalización de variables y dimensiones como ejemplo, para facilitar su definición y elaboración.

Recuerde que puede apoyarse en su docente mediador o jurado de apoyo, para realizar este tópico.

Tabla de operacionalización de variables y dimensiones.

Tabla N.º 3a

Objetivo General	Proponer el Diseño De Protocolos De Seguridad A Nivel De Código Y Procedimientos En El Desarrollo De Aplicaciones Del Observatorio Nacional De Ciencia, Tecnología E Innovación		
Variables	Independiente: Propuesta de diseño de protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del ONCT		
	Dependiente: La mejora en la protección de la información y la integridad de los datos		
Objetivos Específicos	**Dimensiones**	**Indicadores**	**Ítems**
OBJETIVO ESPECÍCO 1 Realizar una revisión teórico-conceptual de los aspectos involucrados en la propuesta de protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del ONCTI.	Institucional	Aspectos Organizacionales	1. Existencia de políticas de seguridad dentro del ONCTI relacionadas con el desarrollo de software. 2. Nivel de cumplimiento de normativas internas de seguridad en la gestión de aplicaciones dentro de la organización. 3. Alineación con estándares nacionales e internacionales (como la Ley de Infogobierno y OWASP). 4. Presencia de un equipo institucional encargado de revisar las normativas de seguridad de las aplicaciones.
	Educativa	Formación ocupacional	1. Nivel de capacitación del personal de desarrollo en prácticas de seguridad informática. 2. Existencia de programas formativos sobre seguridad para los desarrolladores y otros empleados involucrados en la creación y mantenimiento de aplicaciones. 3. Tasa de participación de los empleados en talleres o formaciones sobre seguridad de software. 4. Evaluación del impacto de la formación en la mejora de la seguridad de las aplicaciones.
	Tecnológica	Competencias tecnológicas para el uso de las TIC	1. Uso de estándares y herramientas de seguridad como OWASP, NIST, o ISO 27001 en el desarrollo de aplicaciones. 2. Existencia de recursos tecnológicos disponibles para realizar auditorías y pruebas de seguridad en las aplicaciones. 3. Tecnologías utilizadas para mitigar vulnerabilidades comunes (como inyecciones SQL, XSS, etc.). 4. Acceso a herramientas especializadas (como escáneres de vulnerabilidades o plataformas de pruebas de penetración).

Tabla N.º 3b

Objetivos Específicos	Dimensiones	Indicadores	Ítems
OBJETIVO ESPECÍCO 2 Diagnosticar los aspectos generales y estructurales relacionados con la propuesta de protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del ONCTI.	Institucional	Aspectos Organizacionales	1. Identificación de riesgos en la seguridad de las aplicaciones en el contexto organizacional. 2. Evaluación de la infraestructura institucional en términos de protección de datos y procesos. 3. Existencia de auditorías internas de seguridad realizadas en el desarrollo de aplicaciones. 4. Evaluación de la capacidad institucional para responder a incidentes de seguridad..
	Educativa	Formación ocupacional	1. Conocimiento del personal sobre los riesgos de seguridad en el desarrollo de software. 2. Capacitación sobre la importancia de las políticas de seguridad en el desarrollo de aplicaciones. 3. Nivel de conciencia en el personal sobre amenazas comunes en el desarrollo de software, como el phishing o ataques de inyección. 4. Participación en simulaciones o ejercicios de respuesta a incidentes.
	Tecnológica	Competencias tecnológicas para el uso de las TIC	1. Existencia de controles técnicos para mitigar vulnerabilidades específicas en el código y el desarrollo de aplicaciones. 2. Evaluación del uso de herramientas automatizadas para detectar vulnerabilidades en aplicaciones y sistemas. 3. Acceso a infraestructuras seguras para realizar pruebas de seguridad. 4. Uso de prácticas de desarrollo seguro (como el ciclo de vida de desarrollo de software con seguridad integrada).

Tabla N.º 3c

Objetivos Específicos	Dimensiones	Indicadores	Ítems
OBJETIVO ESPECÍCO 3 Diseñar los protocolos de seguridad a nivel de código y procedimientos en el desarrollo de aplicaciones web del ONCTI, categorizados por: generales, estructurales, de programación y funcionales.	Institucional	Aspectos Organizacionales	1. Aprobación institucional de protocolos de seguridad para el desarrollo de aplicaciones. 2. Incorporación de protocolos de seguridad en los procedimientos institucionales establecidos. 3. Capacitación sobre las nuevas políticas y protocolos de seguridad dentro de la organización. 4. Documentación y comunicación de los protocolos a todas las áreas relevantes de la organización.
	Educativa	Formación ocupacional	1. Entrenamiento sobre los nuevos protocolos de seguridad aplicados en el ONCTI. 2. Nivel de comprensión y adopción de los protocolos por parte del personal de desarrollo. 3. Tasa de implementación de los protocolos de seguridad en el código y los procedimientos de desarrollo. 4. Evaluación del impacto educativo de las capacitaciones y talleres en la aplicación efectiva de los protocolos de seguridad.
	Tecnológica	Competencias tecnológicas para el uso de las TIC	1. Implementación de herramientas tecnológicas específicas para aplicar los protocolos de seguridad, como sistemas de monitoreo, auditoría o control de versiones. 2. Automatización de procesos de seguridad en el ciclo de vida de las aplicaciones. 3. Aseguramiento de que los protocolos se alineen con tecnologías emergentes como la protección de datos en la nube y el uso de contenedores. 4. Evaluación de la efectividad de las herramientas implementadas para detectar fallos de seguridad.

Tabla N.º 3d

Objetivos Específicos	Dimensiones	Indicadores	Ítems
OBJETIVO ESPECÍCO 4 Implementar pruebas de penetración y auditorías de seguridad para validar la efectividad de los protocolos de seguridad diseñados en un entorno controlado.	Institucional	Aspectos Organizacionales	1. Aprobación y ejecución de auditorías de seguridad por parte de la alta dirección. 2. Nivel de involucramiento de la institución en la supervisión de la implementación de las pruebas de penetración. 3. Existencia de una política institucional que regule las pruebas de seguridad. 4. Capacitación en auditorías de seguridad dentro de los equipos técnicos de la organización.
	Educativa	Formación ocupacional	1. Capacitación del personal de desarrollo y seguridad sobre las mejores prácticas en pruebas de penetración. 2. Participación en talleres prácticos sobre cómo realizar y reaccionar ante auditorías de seguridad. 3. Nivel de conocimiento adquirido por los equipos sobre los resultados de las pruebas de penetración y cómo aplicarlos. 4. Evaluación de los aprendizajes obtenidos de los ejercicios de prueba y penetración.
	Tecnológica	Competencias tecnológicas para el uso de las TIC	1. Implementación de herramientas de pruebas de penetración como Kali Linux, OWASP ZAP, o Burp Suite. 2. Realización de pruebas de penetración en diferentes fases del ciclo de desarrollo. 3. Detección y resolución de vulnerabilidades durante las auditorías de seguridad. 4. Evaluación de las métricas de efectividad de las auditorías, como el número de vulnerabilidades detectadas y corregidas..

Tabla N.º 3e

Objetivos Específicos	Dimensiones	Indicadores	Ítems
OBJETIVO ESPECÍCO 5 Capacitar al equipo de desarrollo del ONCTI sobre las mejores prácticas en seguridad informática, asegurando que los nuevos protocolos sean adoptados y aplicados correctamente.	Institucional	Aspectos Organizacionales	1. Existencia de un plan institucional para la capacitación continua en seguridad informática. 2. Participación de líderes y directivos en la implementación de las capacitaciones sobre seguridad. 3. Evaluación del impacto institucional de las capacitaciones en el desempeño de los equipos de desarrollo. 4. Nivel de cumplimiento de los protocolos de seguridad por parte del personal capacitado.
	Educativa	Formación ocupacional	1. Tasa de asistencia a cursos de formación en seguridad informática y mejores prácticas de desarrollo seguro. 2. Nivel de conocimiento alcanzado por los desarrolladores sobre las herramientas y técnicas de seguridad. 3. Evaluaciones de desempeño post-capacitación para medir la efectividad de la formación. 4. Nivel de satisfacción de los participantes con los programas de capacitación.
	Tecnológica	Competencias tecnológicas para el uso de las TIC	1. Uso de plataformas tecnológicas de formación (como plataformas en línea o simuladores de seguridad). 2. Aplicación práctica de las mejores prácticas de seguridad en los proyectos de desarrollo. 3. Desarrollo de documentación interna para guiar al equipo de desarrollo en la implementación de los protocolos de seguridad. 4. Implementación de un sistema de retroalimentación para asegurar que los protocolos sean seguidos en todos los niveles de desarrollo.

ANEXOS

A. CRONOGRAMA

Fase	Actividad	Responsables	Duración (sem)
1. Análisis y diagnóstico	Revisión teórica y de estándares (OWASP, ISO 27001, NIST)	Analista de seguridad	1 semana
	Diagnóstico de riesgos y vulnerabilidades en sistemas actuales	Equipo de seguridad	2 semanas
2. Diseño de Protocolo	Definición de categorías de protocolos (generales, estructurales, de programación, funcionales)	Líder del proyecto	1 semana
	Diseño de protocolos de seguridad y procedimientos específicos	Equipo de desarrollo	2 semanas
3. Implementación	Implementación de protocolos en entornos de desarrollo (según categorías definidas)	Equipo de desarrollo	3 semanas
	Configuración de herramientas de auditoría y revisión de código	Equipo de infraestructura	2 semanas
4. Pruebas y Validación	Pruebas de penetración y simulaciones de ataques	Equipo de seguridad	2 semanas
	Validación y ajustes con base en los resultados de pruebas	Equipo de desarrollo	2 semanas
5. Capacitación y Documentación	Capacitación del equipo de desarrollo en prácticas de seguridad	Consultor de seguridad	1 semana
	Documentación final de protocolos y entrega de resultados	Líder del proyecto	1 semana