**UNIDAD NACIONAL DE PROTECCIÓN - UNP**

**INFORME**

**GRUPO DE GESTIÓN DE LAS TECNOLOGÍAS**

**-GGT-**



Auditoria V1. Ecosistema UNP

Formulario en línea Individual

Desarrollo In-House

Bogotá, 25 de nov. de 2024

**CONTENIDO**

|  |  |  |
| --- | --- | --- |
| [Nomenclatura] | [Tema] | [Página] |
| A | **OBJETIVO** | 3 |
| B | **ALCANCE** | 3 |
| C | **DEFINICIONES** | 3 |
| D | **ASPECTOS RELEVANTES**  | 5 |
| E | **CONTENIDO** | 7 |
| I | **(TEMA 1)** | 7 |
| I.a | Situación analizada y gestión realizada |  |
| I.b | Riesgos asociados: [Opcional] |  |
| I.c | Alternativas de solución planteadas: [Opcional] |  |
|  | ……………………. |  |
|  | ………………… |  |
| F | **ANEXOS.**  | 13 |
|  |  |  |

1. **OBJETIVO**

El objetivo principal de este informe es documentar y demostrar cómo desde ECOSISTEMA-UNP, hemos integrado los controles de seguridad a lo largo de todas las etapas del desarrollo de software, siguiendo los estándares y requisitos establecidos por la norma ISO 27001:2022.

1. **ALCANCE**
2. El alcance principal se centra en la revisión de los controles de seguridad implementados y la efectividad de estos controles en el momento de la auditoría. Sin embargo, también es válido y beneficioso presentar escenarios futuros o supuestos, siempre y cuando tengan un propósito claro y bien definido. Este enfoque adicional puede abarcar varios aspectos, asegurando una preparación proactiva y estratégica ante posibles brechas futuras.
3. **DEFINICIONES**
* **Ciclo de Vida Seguro de Desarrollo:** Se refiere a la integración de controles de seguridad a lo largo de todas las etapas del desarrollo de software, desde la planificación hasta la implementación y el mantenimiento. Esto asegura que la seguridad se considere desde el inicio y se mantenga a lo largo del ciclo de vida del software.
* **Arquitectura de Software:** Es el diseño estructural del software que garantiza que se cumplan los principios de seguridad, soportando tanto las necesidades funcionales como no funcionales del software.
* **Análisis de Riesgos:** Proceso de identificar, evaluar y mitigar los riesgos de seguridad en el desarrollo de software. Incluye la revisión de requisitos de seguridad y la elaboración de un análisis de impacto.
* **Codificación Segura:** Consiste en aplicar técnicas y principios que previenen la introducción de vulnerabilidades durante la escritura del código. Esto incluye prácticas para evitar amenazas comunes como XSS, CSRF y SQL Inyección.
* **Pruebas de Seguridad:** Son procesos definidos para validar que los requisitos de seguridad se cumplen. Incluyen pruebas de penetración, análisis de vulnerabilidades y revisiones de código.
* **Gestión de Cambios:** Procedimientos establecidos para controlar y documentar las modificaciones realizadas al software, asegurando que estos cambios no introduzcan nuevas vulnerabilidades.
* **Desarrollo Subcontratado:** Supervisión y revisión de las actividades relacionadas con el desarrollo de sistemas tercerizados, asegurando que se apliquen los mismos estándares de seguridad que en los desarrollos in-house.
* **Separación de Entornos:** Práctica de mantener separados los entornos de desarrollo, prueba y producción para evitar comprometer los datos y la seguridad del entorno de producción.
* **Información de Prueba:** Selección, protección y gestión adecuada de la información utilizada en las pruebas para asegurar su relevancia y protección.
* **Pruebas de Auditoría:** Evaluaciones que implican la revisión de los sistemas operativos para asegurar que cumplan con los requisitos de seguridad sin impactar negativamente en las operaciones de la Unidad.
* **Evaluación de Contingencias y Planes de Respuesta:** Presentación de escenarios hipotéticos sobre posibles incidentes de seguridad y demostración de cómo los planes de contingencia y procedimientos de respuesta están preparados para manejar estos eventos.
* **Mejora Continua:** Proceso de planificar y ejecutar mejoras en el Sistema de Gestión de Seguridad de la Información (SGSI) basándose en la evaluación de riesgos y resultados de auditorías previas.
* **Pruebas de Simulación (Tabletop Exercises):** Simulaciones realizadas para evaluar la respuesta de la Unidad ante incidentes específicos, mejorando la preparación y respuesta de la Unidad.
* **Proyectos de Implementación Futura:** Planes detallados de implementación de futuros proyectos de seguridad alineados con los objetivos y políticas de la Unidad.
* **Evaluación de Nuevas Amenazas:** Análisis prospectivos sobre cómo se manejarán nuevas amenazas o cambios en el entorno tecnológico y regulatorio, integrando estas estrategias en el SGSI.
* **Objetivo del Informe de Implementación del Ciclo de Vida Seguro de Desarrollo de Software:** Documentar y demostrar cómo la unidad desde Ecosistema-unp ha integrado los controles de seguridad a lo largo de todas las etapas del desarrollo de software, asegurando el cumplimiento con los requisitos de la norma ISO 27001:2022 y la protección efectiva de la información.
1. **ASPECTOS RELEVANTES**
* **Política para el Desarrollo de Software según el Manual de políticas específicas de seguridad y privacidad de la información UNP**
* Todos los proyectos de desarrollo de software in-house y subcontratados cumplen con los requisitos de seguridad de la información establecidos.
* Se realiza una evaluación continua y actualización de las medidas de seguridad durante todo el ciclo de vida del desarrollo del software.
* La seguridad se considera un aspecto fundamental y prioritario en todas las etapas del desarrollo de software, desde la planificación hasta el mantenimiento.
* **Objetivo:** Incorporar requisitos de seguridad en todos los proyectos de desarrollo y adquisición de sistemas de información, tanto propios como de terceros.
* **Implementación:** Evaluación continua y actualización de las medidas de seguridad durante el ciclo de vida del desarrollo.
* **Presentación Auditoría Ecosistema-UNP de la ISO 27001:2022**
* **Documentación:** Requerimientos de seguridad, planificación y arquitectura, análisis de riesgos, codificación segura, pruebas de seguridad, gestión de cambios, separación de entornos, información de prueba y pruebas de auditoría.
* **Escenarios Futuros o Supuestos:** Contingencias y planes de respuesta, mejora continua, pruebas de simulación, proyectos de implementación futura y evaluación de nuevas amenazas.
* **Importancia:** Demostrar preparación y gestión proactiva de riesgos futuros, cumpliendo con los requisitos actuales y mostrando compromiso con la mejora continua.

**Objetivo del Informe de Implementación del Ciclo de Vida Seguro de Desarrollo de Software según ISO 27001:2022**

* **Asegurar la Conformidad:** Evidenciar el cumplimiento con la norma ISO 27001:2022.
* **Proteger la Información:** Garantizar la protección de la confidencialidad, integridad y disponibilidad de la información.
* **Documentar Procesos:** Proveer documentación detallada de los procesos de desarrollo seguro.
* **Mejora Continua:** Mostrar esfuerzos en la mejora del SGSI.
* **Preparación para Auditorías:** Facilitar la preparación y evidencia para auditorías.
* **Fomentar la Concienciación:** Aumentar el conocimiento sobre la importancia de la seguridad de la información.
* **Soporte a la Gestión:** Proveer información para la toma de decisiones informadas sobre la gestión de riesgos.
1. **CONTENIDO.**
2. **Controles Específicos según ISO 27001:2022 para Formulario en línea Individual.**
3. Situación analizada y gestión realizada:

**8.25 - Ciclo de Vida de Desarrollo Seguro:** **Control:** Establece que las organizaciones deben implementar estándares de seguridad a lo largo del ciclo de vida completo del desarrollo de software. **Implementación en Formulario en línea Individual:**

* Definir y seguir estándares de seguridad desde la fase de diseño hasta el despliegue del Formulario en línea Individual.
* Realizar revisiones periódicas y actualizaciones de seguridad durante todo el ciclo de vida del Formulario en línea Individual.

**8.26 - Requisitos de Seguridad de la Aplicación:** **Control:** Los requisitos de seguridad deben ser identificados, especificados y aprobados durante el desarrollo o la adquisición de aplicaciones. **Implementación en Formulario en línea Individual:**

* Identificar los requisitos de seguridad específicos del Formulario en línea Individual.
* Asegurar que estos requisitos sean aprobados y documentados antes del desarrollo.

**8.27 - Arquitectura del Sistema y Principios de Ingeniería:** **Control:** Los principios para la ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información. **Implementación en Formulario en línea Individual:**

* Diseñar la arquitectura del Formulario en línea Individual siguiendo principios de seguridad.
* Documentar y aplicar estos principios durante todo el proceso de desarrollo.

**8.28 - Codificación Segura:** **Control:** Los principios de codificación segura deben aplicarse al desarrollo del software. **Implementación en Formulario en línea Individual:**

* Utilizar técnicas de codificación segura para evitar vulnerabilidades comunes como XSS, CSRF y SQL Inyección.
* Revisar y probar el código del Formulario en línea Individual para asegurar que cumple con las prácticas de codificación segura.

**8.29 - Pruebas de Seguridad en el Desarrollo y Aceptación:** **Control:** Los procesos de pruebas de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo. **Implementación en Formulario en línea Individual:**

* Definir un plan de pruebas de seguridad específico para el Formulario en línea Individual.
* Realizar pruebas de seguridad durante el desarrollo y antes de la aceptación final.

**8.30 - Desarrollo Subcontratado:** **Control:** La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas tercerizados. **Implementación en Formulario en línea Individual:**

* Monitorear y revisar todas las actividades de desarrollo del Formulario en línea Individual subcontratado.
* Asegurar que los desarrolladores subcontratados cumplan con los estándares de seguridad de la Unidad.

**8.31 - Separación de los Entornos de Desarrollo, Prueba y Producción:** **Control:** Los entornos de desarrollo, prueba y producción deben estar separados y protegidos. **Implementación en Formulario en línea Individual:**

* Mantener entornos separados para el desarrollo, prueba y producción del Formulario en línea Individual.
* Proteger cada entorno con controles de seguridad adecuados para evitar compromisos.
1. Riesgos asociados: [Opcional]
* []
1. Alternativas de solución planteadas: [Opcional]
* []
1. **Auditoria de la norma ISO 27001:2022 enfocada en el ciclo de vida de desarrollo seguro**
2. Situación analizada y gestión realizada:

Presentamos una serie de documentos y evidencias que demuestren que se han implementado y mantenido los controles de seguridad adecuados a lo largo de todas las etapas del desarrollo de software. A continuación, se detalla lo que se presentar:

1. Documentación de Requerimientos:

* Detalles de los requisitos de seguridad identificados y aprobados durante la fase de especificación.
* Documentación que demuestran cómo estos requisitos se han integrado en el proceso de desarrollo.

2. Planificación y Arquitectura:

* Diagramas de arquitectura del sistema que muestren cómo se han incorporado los controles de seguridad.
* Documentación de los principios de ingeniería de sistemas seguros aplicados.

3. Análisis de Riesgos:

* Análisis de riesgos específico para el desarrollo del software, que identifique posibles amenazas y vulnerabilidades.
* Planes de mitigación y documentación sobre cómo se abordan estos riesgos.

4. Codificación Segura:

* Procedimientos y guías de codificación segura que el equipo de desarrollo debe seguir.
* Revisiones de código que evidencien la aplicación de técnicas de codificación segura.

5. Pruebas de Seguridad:

* Planes de pruebas de seguridad que describan los tipos de pruebas realizadas (análisis de vulnerabilidades, pruebas de penetración).
* Resultados de pruebas de seguridad que demuestren la identificación y corrección de vulnerabilidades.

6. Gestión de Cambios:

* Procedimientos de gestión de cambios que muestren cómo se controlan y documentan las modificaciones al software.
* Registros de cambios aprobados, con detalles sobre su impacto en la seguridad.

7. Desarrollo o integración Subcontratado: (En Proceso)

* Evidencia de la supervisión y monitoreo de cualquier desarrollo subcontratado.
* Documentación de los acuerdos de seguridad con los proveedores y el cumplimiento de estos acuerdos.

8. Separación de Entornos:

* Políticas y procedimientos que aseguren la separación de los entornos de desarrollo, prueba y producción.
* Evidencia de controles implementados para proteger estos entornos.

9. Información de Prueba:

* Documentación sobre la selección, protección y gestión de la información utilizada en las pruebas.
* Registros que aseguren la protección de la información operativa durante las pruebas.

10. Pruebas de Auditoría y/o locales:

* Planificación y registros de pruebas de auditoría que involucren la evaluación de los sistemas operativos.
* Acuerdos entre el evaluador y la gerencia sobre cómo se minimizará el impacto de estas pruebas en las operaciones.

11. Sensibilización y Conocimiento:

* Evidencia de la sensibilización en seguridad del personal involucrado en el desarrollo de software.
* Documentos que demuestren la concienciación y cumplimiento de las políticas de seguridad por parte del equipo de desarrollo.

12. Escenarios Futuros y Supuestos: (En Proceso)

* Evaluación de contingencias y planes de respuesta para posibles incidentes de seguridad.
* Planes de mejora continua y proyectos de implementación futura alineados con los objetivos de la Unidad.
* Pruebas de simulación y análisis prospectivos sobre nuevas amenazas.
* Escenarios y Documentos anexos: Formulario en línea Individual

Para un desarrollo in-house como el Formulario en línea Individual, presentamos unos en formatos ya definidos y otros en proceso:

* Diagramas de arquitectura específicos del formulario que incluyan controles de seguridad.
* Resultados de análisis de riesgos y planes de mitigación específicos para el formulario.
* Evidencia de la aplicación de técnicas de codificación segura durante el desarrollo del formulario.
* Registros de pruebas de seguridad realizadas específicamente en el formulario y las correcciones implementadas.
* Procedimientos de gestión de cambios y registros que detallen las modificaciones al formulario.
* Supervisión y cumplimiento de acuerdos de seguridad con cualquier proveedor involucrado en el desarrollo del formulario.
* Políticas de separación de entornos y evidencia de su aplicación específica al desarrollo del formulario.
* Protección de la información utilizada en las pruebas del formulario.
* Pruebas de auditoría locales y acuerdos sobre la minimización del impacto en las operaciones relacionadas con el formulario.
* Evidencia de la sensibilización del personal en la seguridad del Formulario en línea Individual.
1. Riesgos asociados: [Opcional]
* []
1. Alternativas de solución planteadas: [Opcional]
* []
1. **[Responsabilidades en el Desarrollo de Software In-House]**
2. Situación analizada y gestión realizada:

**✓ Arquitectura de Software:** Definimos una arquitectura segura y robusta que cumple con los principios de seguridad y que soporta las necesidades funcionales y no funcionales del software. Esta etapa incluye la evaluación de riesgos y la implementación de medidas de mitigación.

**✓ Análisis:** Llevamos a cabo un análisis exhaustivo para identificar y evaluar riesgos de seguridad. Esto incluye la revisión de requisitos de seguridad y la elaboración de un análisis de impacto para comprender cómo los cambios pueden afectar a la seguridad.

**✓ Diseño:** El diseño del software se realiza siguiendo principios de seguridad, asegurando que todas las decisiones de diseño consideren la protección de la información. Se documentan todos los controles de seguridad que se integrarán en el software.

**✓ Cifrado de Datos:** Implementamos cifrado robusto para proteger los datos sensibles tanto en tránsito como en reposo. Esto incluye la selección de algoritmos de cifrado adecuados y la gestión segura de claves criptográficas, Anonimizarían y cifrados tópicos (token y demás).

**✓ Especificación de Requerimientos:** Detallamos los requisitos de seguridad durante la fase de especificación, asegurando que todas las necesidades de seguridad sean identificadas, documentadas y aprobadas antes de comenzar el desarrollo.

**✓ Controles de Seguridad de la Información:** Establecemos y mantenemos controles de seguridad de la información a lo largo del ciclo de vida del desarrollo. Estos controles incluyen la autenticación, autorización, auditoría y monitoreo continuo de las aplicaciones.

**✓ Calidad de Software:** Implementamos prácticas de aseguramiento de la calidad que incluyen pruebas de seguridad para identificar y corregir vulnerabilidades en el software. Esto garantiza que el software cumpla con los requisitos de seguridad antes de su despliegue.

**✓ Estandarización de los Mensajes de Error y Eventos de Seguridad:** Desarrollamos una estandarización de los mensajes de error y eventos de seguridad para asegurar que se comuniquen de manera adecuada, sin revelar información sensible que pueda ser aprovechada por atacantes.

**✓ Documentación Técnica y de Usuario:** Proporcionamos documentación detallada que incluye manuales técnicos y de usuario. Esta documentación asegura que todos los aspectos de seguridad del software sean comprendidos y seguidos por los usuarios y administradores.

1. Riesgos asociados: [Opcional]
* []
1. Alternativas de solución planteadas: [Opcional]
* []
1. **ANEXOS.**

GTE-FT-05 V2 Informe formulario solicitud análisis de riesgo - Ruta Individual V.1 (1)

**GTE-FT-36-V3 Identificación Valoración y Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

**GTE-FT-46-V1 Declaración Aplicabilidad-SOA**

**GTE-FT-41-V Formato Solicitud de Servidores**

**GTE-FT-39-V2 Formato de Registro y Valoración de Activos de Seguridad de la Información**

**GTE-FT-18 V1 Formato de Solicitud de Cambios en Proyectos**

**GTE-FT-20-V2 Formato Pruebas Sistemas de Información**

**Anexos Adicionales Del Proceso.**

**Cordialmente,**

## [JEAVER ALEXANDER VERGARA FERNANDEZ].

##  [CIBERSEGURIDAD – ECOSISTEMA-UNP]

##  [Grupo GGT]

##  [OAPI]

##  Unidad Nacional de Protección

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

***Archívese en:***

| **VERSIÓN INICIAL** | **DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO** | **FECHA** | **VERSIÓN****FINAL** |
| --- | --- | --- | --- |
| 00 | Se creó el presente documento para orientar el diligenciamiento del Informe de Estado y Gestión de GGTST. Grupo de Gestión Tecnológica y Soporte Técnico | 29/07/2016 | 01 |
| 01 | Se realizan modificaciones al formato  | 29/08/2018 | 02 |
| 02 | Se realiza actualización del formato se hace redefinición de los ítems de contenido para hacerlo de fácil utilización en los diferentes temas tratados por el proceso. incluyendo cambio de logos, actualización del instructivo y actualización en el nombre del grupo interno de trabajo a Grupo de Gestión de las Tecnologías GGT | 12/11/2024 | 03 |

**NO IMPRIMIR**

| **INSTRUCTIVO** |
| --- |
| **CAMPO** | **DESCRIPCION DEL CAMPO** |
| Portada | Escribir el nombre del tema a desarrollar y fecha de elaboración del documento  |
| Tabla de Contenido | Realizar la identificación de los temas a tratar dentro del documento |
| Objetivo | Describir de forma clara y detallada del propósito del documento, el cual responde a las preguntas ¿para qué fue creado? o ¿con qué finalidad se creó? El objetivo inicia con un verbo en infinitivo, por ejemplo: definir, establecer, entre otros |
| Alcance | Describe la trascendencia o delimitación que se le quiere dar al documento desde donde inicia hasta donde finaliza.  |
| Definiciones | Explicar los términos usados en el texto que se consideran necesarios para un mejor entendimiento del documento |
| Aspectos relevantes | Relacionar los aspectos significativos que impactan el Estado y la Gestión Tecnológica |
| Contenido | El contenido del Informe debe describir cada uno de los temas y/o actividades desarrolladas, de manera concreta, incluyendo especificaciones técnicas de ser necesario.     Para cada uno de los eventos y/o actividades incluidas en el Informe, es necesario que se detalle:  1. Situación analizada y gestión realizada [X]
2. Riesgos asociados [Opcional]
3. Alternativas de solución planteadas [Opcional]
 |
| ANEXOS | En caso de ser requerido para claridad de los temas tratados en el informe detallar los anexos soporte del informe |
| Archívese en | Diligencie la de disposición final (almacenamiento) del documento ya sea físico o Digital cumpliendo los lineamientos y directrices establecidos por Gestión Documental |