Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Ciclo de Vida de Desarrollo de Sistemas Seguros

24
CAPÍTULO

Ciclo de Vida de Desarrollo de Sistemas Seguros

1.0 Propósito y Beneficios

Si bien muchos lo consideran un proceso separado, la seguridad de la información es un requisito gubernamental que debe considerarse durante todo el ciclo de vida de desarrollo del sistema (SDLC por su sigla en inglés Software Development Lifecycle). Este Estándar del ciclo de vida del desarrollo de sistemas seguros define los requisitos de seguridad que deben considerarse y abordarse en cada SDLC.

Los sistemas y aplicaciones informáticas se crean para abordar las necesidades gubernamentales. Para hacerlo de manera efectiva, los requisitos del sistema deben identificarse tempranamente y abordarse como parte del SDLC. No identificar un requisito hasta el final del proceso puede tener repercusiones importantes para el éxito de un proyecto y provocar retrasos en la entrega del proyecto, implementación de un sistema inadecuado e incluso el abandono del proyecto. Además, por cada fase por la que pasa un proyecto sin identificar y abordar un requisito, más costoso y lento será solucionar los problemas que surgen debido a la omisión.

La seguridad de la información debe considerarse e integrarse adecuadamente en cada fase del SDLC. No identificar los riesgos e implementar controles adecuados puede resultar en una seguridad inadecuada, lo que podría poner a las entidades en riesgo de sufrir violaciones de datos, exposición a su reputación, pérdida de confianza pública, compromiso de sistemas/redes, sanciones financieras y/o responsabilidad legal.

2.0 Declaración de información

La seguridad es un requisito que debe incluirse en cada fase del ciclo de vida del desarrollo de un sistema. El ciclo de vida de desarrollo de un sistema que incluye actividades de seguridad definidas formalmente dentro de sus fases se conoce como SDLC seguro. Según la Política de seguridad de la información, se debe utilizar un SDLC seguro en el desarrollo de todas las aplicaciones y sistemas.

Estas actividades deben estar documentadas o referenciadas dentro de un plan de seguridad de la información asociado. La documentación debe ser suficien-

temente detallada para demostrar hasta qué punto se aplica cada actividad de seguridad. La documentación debe conservarse para fines de auditoría. Como mínimo, un SDLC debe contener las siguientes actividades de seguridad:

1. Definir roles y responsabilidades de seguridad
2. Orientar al personal sobre las tareas de seguridad del SDLC
3. Establecer un nivel de criticidad del sistema
4. Clasificar información
5. Establecer requisitos de credenciales de identidad del sistema
6. Establecer objetivos del perfil de seguridad del sistema
7. Crear un perfil del sistema
8. Descomponer el sistema
9. Evaluar vulnerabilidades y amenazas
10. Evaluar riesgos
11. Seleccionar y documentar controles de seguridad
12. Crear datos de prueba
13. Probar los controles de seguridad
14. Realizar Certificación y Acreditación
15. Gestionar y controlar el cambio
16. Medir el cumplimiento de la seguridad
17. Realizar la eliminación del sistema

No existe necesariamente una correspondencia uno a uno entre las actividades de seguridad y las fases del SDLC. Las actividades de seguridad a menudo deben realizarse de forma iterativa a medida que un proyecto avanza o recorre el SDLC. A menos que se indique lo contrario, la ubicación de las actividades de seguridad dentro del SDLC puede variar de acuerdo con el SDLC que se utiliza y las necesidades de seguridad de la aplicación o sistema. ***Apéndice A: Actividades de seguridad dentro del SDLC*** proporciona un ejemplo de correlación de las actividades de seguridad con un ciclo de vida de desarrollo de sistema genérico. ***Apéndice B: Descripción de las actividades de seguridad*** proporciona una descripción de las consideraciones y actividades de seguridad anteriores.

Finalmente, es importante señalar que el proceso SDLC seguro es integral por intención, para garantizar la debida diligencia, el cumplimiento y la documentación adecuada de los controles y consideraciones relacionados con la seguridad. Diseñar la seguridad en los sistemas requiere una inversión de tiempo y recursos. El grado en que se aplica la seguridad al proceso SDLC debe ser proporcional a la clasificación (sensibilidad de los datos y criticidad del sistema) del sistema que se está desarrollando y los riesgos que este sistema puede introducir en el entorno general. Esto asegura valor al proceso de desarrollo y entregable. En términos generales, el mejor retorno de la inversión se logra aplicando rigurosamente la seguridad dentro del proceso SDLC a proyectos de alto riesgo y alto costo. Cuando se determina que un proyecto no aprovechará todo el proceso SDLC seguro (por ejemplo, en un proyecto de menor riesgo/costo), se debe documentar la

justificación y las actividades de seguridad que no se utilizan deben identificarse y aprobarse como parte del proceso formal de aceptación de riesgos.

Nota: La clasificación de datos no se puede utilizar como único factor determinante de si el proyecto es o no de bajo riesgo/costo. Por ejemplo, los sitios web públicos no pueden considerarse proyectos de bajo riesgo/costo incluso si todos los datos son públicos. Existe el riesgo de que el sitio web se vea comprometido al inyectar malware y comprometer las máquinas de los visitantes o al cambiar el contenido del sitio web para afectar la reputación de la administración pública.

3.0 Cumplimiento

Los empleados que violen esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

4.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
02/09/2024	Documento inicial, primera revisión	Alejandro Castro Pablo Zalazar
17/09/2024	Revisión y correcciones menores	Alejandro Castro Pablo Zalazar

5.0 Documentos relacionados

Publicación especial del NIST 800-30, Guía para realizar evaluaciones de riesgos

Publicación especial del NIST 800-53, Controles de seguridad y privacidad para organizaciones y sistemas de información federales

Publicación especial del NIST 800-53A, Guía para evaluar los controles de seguridad en organizaciones y sistemas de información: creación de planes de evaluación eficaces

La siguiente tabla muestra la ubicación de las actividades de seguridad dentro de las fases de un SDLC de muestra. La ubicación real de las actividades de seguridad dentro del ciclo de vida de desarrollo del sistema puede variar de acuerdo con el SDLC real que se utiliza en un proyecto y las necesidades de seguridad particulares de la aplicación o sistema. Las publicaciones del NIST en la tercera columna de esta tabla son documentos recomendados para brindar orientación en la ubicación y ejecución de tareas de seguridad dentro del ciclo de vida de desarrollo del sistema. Estos documentos están disponibles en el sitio web del NIST (http://csrc.nist.gov/publications/PubsSPs.html).

Figura A-1: Ubicación de las actividades de seguridad dentro de las fases del SDLC

PMG del estado de Nueva York Fase SDLC	Actividad de seguridad	Publicaciones del NIST
Iniciación del sistema	• Definir roles y responsabilidades de seguridad • Orientar al personal sobre las tareas de seguridad del SDLC • Establecer un nivel de criticidad del sistema • Clasificar información (preliminar) • Establecer requisitos de nivel de garantía del sistema • Establecer objetivos del perfil de seguridad del sistema (preliminar) • Crear un perfil del sistema (preliminar)	• SP800-12 • SP800-14 • SP800-35 • SP800-27 • SP800-47 • SP800-60 • SP800-63 • FIPS 199

PMG del estado de Nueva York Fase SDLC	Actividad de seguridad	Publicaciones del NIST
Análisis de requisitos del sistema	• Establecer objetivos del perfil de seguridad del sistema (iterativo) • Clasificar información (iterativo) • Descomponer el sistema (preliminar)	• SP800-23 • SP800-30 • SP800-36 • SP800-53 • SP800-55 • SP800-64 • FIPS 140-2
Diseño de sistemas	• Crear un perfil del sistema (iterativo) • Descomponer el sistema (iterativo) • Evaluar vulnerabilidades y amenazas (preliminar) • Evaluar riesgos (preliminar) • Seleccionar y documentar controles de seguridad (preliminares)	
Construcción del sistema	• Crear datos de prueba • Evaluar vulnerabilidades y amenazas (iterativo) • Evaluar riesgos (iterativo) • Seleccionar y documentar controles de seguridad (iterativo) • Probar controles de seguridad	• SP800-35 • SP800-36 • SP800-37 • SP800-51 • SP800-53 • SP800-53A • SP800-55 • SP800-56 • SP800-57 • SP800-61 • SP800-64
Implementación del sistema	• Medir el cumplimiento de la seguridad • Perfil de seguridad del sistema de documentos • Requisitos y controles de seguridad de documentos	
Aceptación del sistema	• Realizar la Certificación y Acreditación del Sistema	
Operaciones y mantenimiento	• Medir el cumplimiento de la seguridad (periódico) • Gestionar y controlar el cambio • Realizar Certificación y Acreditación del Sistema (iterativo)	• SP800-26 • SP800-31 • SP800-34 • SP800-37 • SP800-53A • SP800-55

PMG del estado de Nueva York Fase SDLC	Actividad de seguridad	Publicaciones del NIST
Disposición	• Preservar la información • Desinfectar los medios • Deseche el hardware y el software	• SP800-12 • SP800-14 • SP800-35 • SP800-36 • SP800-64

1. Definir roles y responsabilidades de seguridad

Se deben definir roles de seguridad y cada actividad de seguridad dentro del SDLC debe asignarse claramente a uno o más roles de seguridad. Estos roles deben estar documentados e incluir a las personas responsables de las actividades de seguridad asignadas a cada rol. ***Apéndice C: Roles de seguridad dentro del SDLC*** proporciona pautas para definir roles de seguridad y asignar actividades de seguridad a roles.

2. Orientar al personal sobre las tareas de seguridad del SDLC

Todas las partes involucradas en la ejecución de las actividades de seguridad del SDLC de un proyecto o política pública deben comprender el propósito, los objetivos y los entregables de cada actividad de seguridad en la que participan o de la que son responsables.

3. Establecer el nivel de criticidad del sistema

Al iniciar una aplicación o sistema, se debe establecer la criticidad del sistema. El nivel de criticidad debe reflejar el valor gubernamental de la función proporcionada por el sistema y el daño potencial que podría resultar de una pérdida de acceso a esta funcionalidad.

4. Clasificar información

Según la Política de Seguridad informática, toda la información contenida, manipulada o que pase por un sistema o aplicación debe estar clasificada. La clasificación debe reflejar la importancia de la confidencialidad, integridad y disponibilidad de la información.

5. Establecer requisitos de credenciales de identidad del sistema

Todas las aplicaciones o sistemas que requieran autenticación deben establecer una credencial de identidad de usuario. La credencial de identidad debe reflejar el nivel de confianza requerido de que la persona que intenta acceder al sistema

es quien dice ser y el posible impacto en la seguridad e integridad del sistema si la persona no es quien dice ser.

6. Establecer objetivos del perfil de seguridad del sistema

Al iniciar una aplicación o sistema, se deben identificar y documentar los objetivos del perfil de seguridad. Estos objetivos deben establecer la importancia y relevancia de los conceptos de seguridad identificados (***Apéndice D: Conceptos de seguridad***) al sistema e indicar el alcance y el rigor con el que cada concepto de seguridad debe incorporarse o reflejarse en el sistema y el software. Cada concepto de seguridad debe considerarse a lo largo de cada fase del ciclo de vida y se debe documentar cualquier consideración o necesidad especial.

El propósito detrás de establecer perfiles de seguridad del sistema y monitorearlos a lo largo del ciclo de vida es ser consciente de la prioridad relativa, el peso y la relevancia de cada concepto de seguridad en cada fase del ciclo de vida del sistema. Las entidades deben verificar que los objetivos del perfil de seguridad consideren adecuadamente todos los mandatos de seguridad nacionales, provinciales y externos que el sistema debe cumplir.

7. Perfilar el sistema

El sistema o aplicación que se está desarrollando debe ser perfilado iterativamente por equipos técnicos dentro del SDLC. Un perfil de sistema es una descripción general de alto nivel de la aplicación que identifica los atributos de la aplicación, como la topología física, los niveles lógicos, los componentes, los servicios, los actores, las tecnologías, las dependencias externas y los derechos de acceso. Este perfil deberá actualizarse a lo largo de las distintas fases del SDLC.

8. Descomponer el sistema

El sistema o aplicación debe descomponerse en componentes más finos y su mecánica (es decir, el funcionamiento interno) debe documentarse. Esta actividad se realizará de forma iterativa dentro del SDLC. La descomposición incluye la identificación de límites de confianza, puntos de entrada y salida de información, flujos de datos y códigos privilegiados.

9. Evaluar vulnerabilidades y amenazas

Las evaluaciones de vulnerabilidad deben realizarse de forma iterativa dentro del proceso SDLC. Las evaluaciones de amenazas deben considerar no solo las amenazas técnicas, sino también las administrativas y físicas que podrían tener un impacto negativo potencial en la confidencialidad, disponibilidad e integridad del sistema. Las evaluaciones de amenazas deben considerar y documentar las fuentes de amenazas, las motivaciones de las fuentes de amenazas y los méto-

dos de ataque que potencialmente podrían representar amenazas a la seguridad del sistema.

Las evaluaciones de amenazas deben cumplir con todos los mandatos nacionales y provinciales relevantes que la Repartición debe cumplir y seguir las mejores prácticas globales, incluida la documentación de los procesos de evaluación. Las evaluaciones de amenazas y los resultados del modelado de amenazas subyacentes que respaldan la evaluación también deben estar completamente documentados. ***Apéndice E: Recursos para la evaluación de amenazas y riesgos*** incluye una lista de recursos recomendados para realizar evaluaciones de amenazas.

10. Evaluar el riesgo

Las evaluaciones de riesgos deben realizarse de forma iterativa dentro del proceso SDLC. Estos comienzan como un proceso informal de alto nivel al comienzo del SDLC y se convierten en un proceso formal e integral antes de poner un sistema o software en producción.

Las amenazas y vulnerabilidades identificadas en las evaluaciones de amenazas deben abordarse en las evaluaciones de riesgos. Las evaluaciones de riesgos deben basarse en el valor de la información en el sistema, la clasificación de la información, el valor de la función gubernamental proporcionada por el sistema, las amenazas potenciales al sistema, la probabilidad de que ocurra, el impacto de la falla del sistema y las consecuencias del fallo de los controles de seguridad.

Los riesgos identificados deben gestionarse adecuadamente evitando, transfiriendo, aceptando o mitigando el riesgo. Está prohibido ignorar el riesgo. Las evaluaciones de riesgos deben cumplir con todos los mandatos nacionales y provinciales relevantes que la Repartición debe documentar y cumplir.

Las evaluaciones de riesgos deben revisarse y actualizarse periódicamente según sea necesario cada vez que se modifique la evaluación de la amenaza subyacente o cuando se realicen cambios significativos en el sistema. ***Apéndice E: Recursos para la evaluación de amenazas y riesgos*** incluye una lista de recursos recomendados para realizar evaluaciones de riesgos.

11. Seleccionar y documentar controles de seguridad

Se deben implementar controles de seguridad adecuados para mitigar los riesgos que no se evitan, transfieren o aceptan. Los controles de seguridad deben justificarse y documentarse con base en las evaluaciones de riesgos, las evaluaciones de amenazas y el análisis del costo de implementar un control de seguridad potencial en relación con la disminución del riesgo que se logra al implementar el control.

La documentación de los controles debe ser lo suficientemente detallada para permitir la verificación de que todos los sistemas y aplicaciones cumplen con las políticas de seguridad relevantes y para responder eficientemente a nuevas amenazas que puedan requerir modificaciones a los controles existentes.

El riesgo residual debe documentarse y mantenerse en niveles aceptables. Se debe realizar una aceptación formal del riesgo, con la aprobación del CISO o responsable de seguridad, para los riesgos medianos y altos que persisten después de que se hayan implementado los controles de mitigación.

Los requisitos de control de seguridad deben revisarse y actualizarse periódicamente según sea necesario cada vez que se modifique el sistema o la evaluación de riesgos subyacente.

12. Crear datos de prueba

Se debe crear un proceso para el desarrollo de datos de prueba significativos para todas las aplicaciones. Debe haber un proceso de prueba disponible para que las aplicaciones realicen pruebas de seguridad y regresión.

Los datos de producción confidenciales no deben utilizarse con fines de prueba. Si se utilizan datos de producción, las Reparticiones deben cumplir con las políticas y estándares nacionales y provinciales y externos aplicables con respecto a la protección y eliminación de datos de producción.

13. Probar los controles de seguridad

Los controles deben probarse minuciosamente en entornos de preproducción que sean idénticos, en la medida de lo posible, al entorno de producción correspondiente. Esto incluye el hardware, el software, las configuraciones del sistema, los controles y cualquier otra personalización.

El proceso de prueba, incluidas las pruebas de regresión, debe demostrar que los controles de seguridad se han aplicado correctamente, se han implementado y están funcionando correctamente y contrarrestando las amenazas y vulnerabilidades para las que están destinados. El proceso de prueba también debe incluir pruebas de vulnerabilidad y demostrar la corrección de vulnerabilidades críticas antes de poner el sistema en producción.

Se debe observar una separación adecuada de funciones a lo largo de los procesos de prueba, como garantizar que diferentes personas sean responsables del desarrollo, el control de calidad y la acreditación.

14. Realizar Acreditación

El plan de seguridad del sistema debe ser analizado, actualizado y aceptado por la Director de Ciberseguridad (DC) o responsable de seguridad).

15. Gestionar y controlar el cambio

Se debe seguir un proceso formal de gestión de cambios cada vez que se modifica un sistema o aplicación para evitar impactos negativos directos o indirectos que el cambio pueda imponer. El proceso de gestión de cambios debe garantizar que las actividades de seguridad del SDLC se consideren y realicen, si corresponde, y que los controles y documentación de seguridad del SDLC que se vean afectados por el cambio estén actualizados.

16. Medir el cumplimiento de la seguridad

Las aplicaciones y sistemas deben someterse a evaluaciones periódicas de cumplimiento de seguridad para garantizar que reflejen una postura de seguridad acorde con la definición de riesgo aceptable. Las evaluaciones del cumplimiento de la seguridad deben incluir evaluaciones del cumplimiento de los estándares de cumplimiento nacionales y provinciales y externos que la Repartición debe cumplir.

Las evaluaciones del cumplimiento de la seguridad deben realizarse después de los cambios en el sistema y las aplicaciones y periódicamente como parte del monitoreo continuo del cumplimiento del sistema.

17. Realizar la eliminación del sistema

La información contenida en aplicaciones y sistemas debe protegerse una vez que un sistema haya llegado al final de su vida útil. La información debe conservarse de acuerdo con los mandatos nacionales y provinciales aplicables u otros requisitos de retención. La información sin requisitos de retención debe descartarse o destruirse y los medios desechados deben desinfectarse de acuerdo con los estándares nacionales y provinciales aplicables para eliminar la información residual.

La responsabilidad de cada actividad de seguridad dentro del SDLC se debe asignar a uno o más roles de seguridad. Para lograr esto, la definición predeterminada de una función SDLC se puede ampliar para incluir responsabilidades de seguridad y/o se pueden definir nuevas funciones de seguridad para abarcar actividades de seguridad. En todos los casos, la asignación de funciones de las actividades de seguridad y la identificación de las personas a las que se les asigna la responsabilidad de dichas funciones deben estar claramente documentadas.

Con el fin de utilizar una definición coherente de funciones en varios SDLC, se recomienda encarecidamente que las Reparticiones utilicen como directrices las publicaciones del Instituto Nacional de Estándares y Tecnología (NIST). De relevancia específica para la definición de roles y marcos de SDLC son:

- Publicación especial del NIST 800-37 Rev. 2 Marco de gestión de riesgos para organizaciones y sistemas de información: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad

La composición de un sistema y software desde una perspectiva de seguridad es su perfil de seguridad e incluye los siguientes conceptos de seguridad, que deben considerarse y documentarse como parte de un proceso SDLC seguro.

Figura D-1: Conceptos de seguridad

Concepto	Descripción
Confidencialidad	Proteger contra la divulgación de información no autorizada
Integridad	Proteger contra modificaciones no autorizadas, involuntarias o incorrectas de software o datos.
Disponibilidad	Garantizar la disponibilidad de los sistemas y la información.
Autenticación	El proceso de establecer confianza en la identidad de los usuarios o sistemas de información.
Autorización	Establecer derechos de acceso a los recursos.
Auditoría/Registro	Crear un registro histórico de las acciones de los usuarios y de los procesos críticos del sistema.
Gestión de sesiones	Asegurar de que una sesión mantenga la confidencialidad y la integridad de la información intercambiada entre un sistema y un usuario autenticado.
Gestión de errores y excepciones	Asegurar de que el comportamiento involuntario y poco confiable del sistema se maneje de forma segura. Esto ayuda a garantizar la protección contra amenazas a la confidencialidad, la integridad y la disponibilidad.
Gestión de parámetros de configuración	Asegurar de que los parámetros configurables necesarios para que se ejecute el software o un sistema estén adecuadamente protegidos.
Privilegios mínimos	Asignar sólo los derechos mínimos permitidos a un sujeto que solicita acceso a un recurso durante el menor tiempo necesario.
Separación de privilegios	Asegurar de que se cumplan varias condiciones antes de otorgar permisos a un objeto.
Defensa en profundidad	Colocar capas de defensas de seguridad en una aplicación para reducir la posibilidad de un ataque exitoso.

Concepto	Descripción
Fallar de forma segura	Asegurar de que la confidencialidad y la integridad de un sistema permanezcan intactas incluso aunque se haya perdido la disponibilidad del sistema debido a una falla del sistema.
Economía de mecanismos	Mantener la implementación y el diseño del sistema lo más simple posible.
Mediación Completa	Requerir comprobaciones de acceso a un objeto cada vez que un sujeto solicite acceso, especialmente para objetos críticos para la seguridad.
Diseño abierto	Utilizar mecanismos de protección reales para proteger la información confidencial; no confíe en un diseño o implementación confiables para proteger la información (también conocido como “seguridad a través de la oscuridad”).
Mecanismos menos comunes	Evitar que varios sujetos compartan mecanismos para otorgar acceso a un recurso.
Aceptabilidad psicológica	Asegurar de que la funcionalidad de seguridad sea fácil de usar y transparente para el usuario.
Aprovechar los componentes existentes	Promover la reutilización de componentes existentes. Reutilizar código probado y validado y bibliotecas estándar en lugar de crear código personalizado.
Eslabón más débil	Identificar y proteger los componentes más débiles de un sistema.
Punto único de fallo	Eliminar cualquier fuente única de compromiso total.

La información relativa a estos conceptos está disponible públicamente en el sitio web patrocinado por la Oficina de Seguridad Cibernética y Comunicaciones del Departamento de Seguridad Nacional (DHS) de EE. UU. En https://buildsecurityin.us-cert.gov.

Para garantizar la alineación con los mandatos de cumplimiento gubernamental y ayudar a asegurar la prestación eficiente y efectiva de servicios de seguridad, se recomienda el uso de estándares reconocidos globalmente relacionados con marcos basados en riesgos y prácticas seguras del ciclo de vida del desarrollo de sistemas.

En particular, se recomienda encarecidamente el uso de los estándares NIST, especialmente para entidades que deben cumplir con mandatos de seguridad nacionales. Las siguientes publicaciones del NIST brindan orientación recomendada para implementar marcos de gestión de riesgos y realizar evaluaciones de riesgos y amenazas.

- Publicación especial del NIST 800-39, Gestión del riesgo de seguridad de la información: organización, misión y vista del sistema de información
- Publicación especial del NIST 800-37 Rev. 2 Marco de gestión de riesgos para organizaciones y sistemas de información: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad
- Publicación especial del NIST 800-30, Guía para realizar evaluaciones de riesgos
- Publicación especial del NIST 800-53, Controles de seguridad y privacidad para organizaciones y sistemas de información federales
- Publicación especial del NIST 800-53A, Guía para evaluar los controles de seguridad en organizaciones y sistemas de información: creación de planes de evaluación eficaces

Las publicaciones del NIST están disponibles en el sitio web del Instituto Nacional de Estándares y Tecnología (http://csrc.nist.gov/publications/PubsSPs.html).