Unidad 4 / Escenario 7

Lectura fundamental

Política y proceso de seguridad en el ciclo de desarrollo

Contenido

Palabras clave: implementación, seguridad, ciclo, desarrollo, consejos, sensibilización, motivación.

1. Introducción

En esta última unidad abordaremos un tema muy importante para una adecuada implementación de seguridad en el ciclo de desarrollo de software: la documentación.

La documentación es una actividad básica, pues como en cualquier actividad empresarial, es importante tenerla para obtener resultados repetibles y medibles. Cuando no se tiene documentación, las personas tienden a realizar las actividades como ellos creen que es la mejor manera de hacerlo, en algunos casos obteniendo resultados de menor calidad a los esperados.

Existe documentación de seguridad en el ciclo de desarrollo con diferentes niveles de detalle y diferentes objetivos. En este escenario abordaremos dos de estos tipos de documentación, las políticas y los procesos.

En el escenario siguiente complementaremos esta documentación mediante la definición de procedimientos y manuales técnicos de seguridad en el ciclo de desarrollo.

2. Documentación en el ciclo de desarrollo de software

La documentación en seguridad en el ciclo de desarrollo básicamente se elabora teniendo en cuenta el nivel de detalle técnico que incluye cada uno de los documentos. Existen cuatro tipos de ellos, la política, el proceso, el procedimiento y el manual técnico, los dos primeros constituyen el "que", los dos últimos constituyen el "como". Lo anterior se puede modelar desde el punto de vista gráfico como una pirámide, como se observa a continuación:

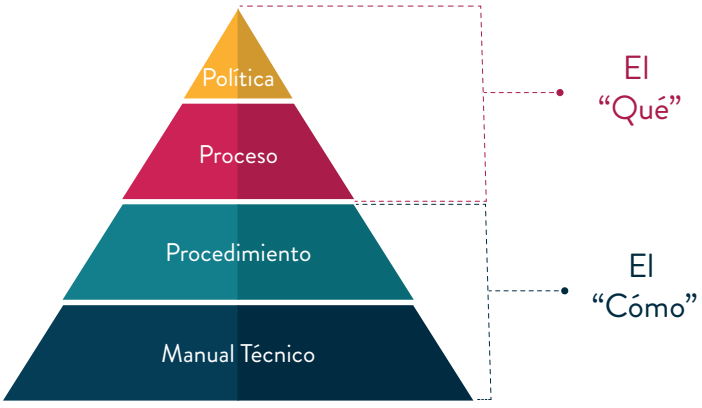


Figura 1. Representación gráfica de la documentación

Fuente: elaboración propia

A mayor nivel de detalle, los documentos son más largos, por lo que se deduce que la política es el documento con menor cantidad de letra, sin embargo, es el punto de partida para el desarrollo de los demás documentos.

De igual manera es importante hablar de la audiencia, a medida que aumenta el detalle de la documentación, se reduce la audiencia objetivo del documento. Por ejemplo, un manual técnico está pensado en personal con conocimientos y competencias técnicas especializadas, lado contrario a una política que está pensada en una audiencia más general.

¿Sabía qué...?

La documentación de seguridad soporta el cumplimiento de estándares como ISO 27001.

3. Ciclo de vida de desarrollo de políticas

Antes de entrar en materia de lo que es una política de seguridad en el ciclo de desarrollo de software, debemos comprender cuál es el ciclo de vida que tienen las políticas en general, aplicable inclusive a otros dominios de la seguridad de la información, como control de acceso, riesgos o seguridad en redes.

El ciclo de vida de desarrollo de políticas abarca las fases de desarrollo, implementación, mantenimiento y eliminación, fases que se detallan a continuación:

3.1. Desarrollo

La etapa de desarrollo de una política inicia con la creación de un borrador del documento, el cuál debe ser elaborado idealmente por un experto en la materia o una empresa especializada. Se recomienda en esta fase, tomar en referencia estándares, normas, leyes o buenas prácticas relacionadas.

Una vez se cuenta con el borrador de la política, es necesario realizar una revisión del documento, de manera que otro profesional o empresa certifique que el documento está completo y se adecua al objetivo del mismo. Es posible que de esta revisión se realicen observaciones o recomendaciones, las cuáles deben ser ajustadas validando previamente su pertenencia.

Con el documento ya ajustado, el siguiente paso es lograr la aprobación del documento. Por buena práctica, las políticas son documentos de alto nivel, con poco detalle y en un lenguaje entendido por la gran mayoría de las personas. Estos documentos deben ser aprobados por el nivel jerárquico más alto dentro de una empresa o institución, es decir por la alta dirección. En este sentido, es necesario presentar y sustentar el documento para que este sea firmado por la alta dirección, dándole así el nivel de importancia requerido.

3.2. Implementación

El entregable de la etapa de desarrollo de la política es un documento aprobado, sin embargo debe ser debidamente comunicado para que pueda ser una realidad y no un documento sin utilidad.

La comunicación de la política debe realizarse por los medios de los cuales disponga la empresa o institución, teniendo al menos las siguientes opciones:

- Por medios digitales: como correo electrónico, intranet, sistemas de gestión documental, etc.
- Por medios físicos: imprimiendo el documento y entregándolo físicamente.
- Realizando reuniones o capacitaciones de presentación de la política.

Una vez comunicada la política, se recomienda que los responsables por la implementación de las diferentes clausulas y controles firmen un recibido de la política, donde se comprometen a realizar todas las gestiones relacionadas con la implementación, entre ellos recursos, capacitación, tiempo, etc.

Durante la fase de implementación es posible que no todo se pueda llevar a cabo o implementar, si existe una justificación valida de negocio, esto se documentará como una excepción.

3.3. Mantenimiento

Durante la etapa de mantenimiento de la política se revisa que la misma siga siendo adecuada para la empresa o entidad, así como la realización de un monitoreo que se puede lograr así:

- Realizando auditorías de cumplimiento
- Contratando a un consultor externo a la organización
- Realizando la medición de indicadores aplicables a la política

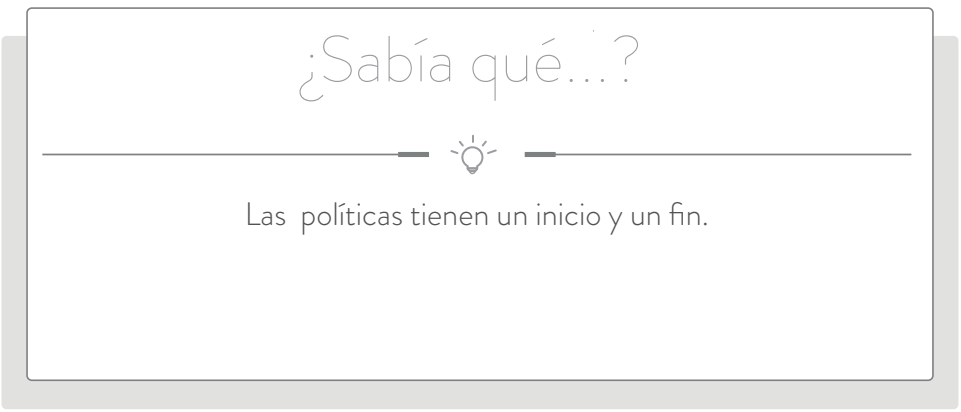
De estas actividades se pueden generar observaciones u oportunidades de mejora que permitirán actualizar la política. Se recomienda realizar al menos una revisión anual del documento.

Las actualizaciones o modificaciones de la política se deben comunicar como se estableció en la etapa de implementación.

3.4. Eliminación

Si el documento ya no es aplicable a la organización, sea cual sea la causa, es necesario declarar o definir el documento como obsoleto. Una vez se ha definido este estado, se debe comunicar que el documento ya no es válido, de manera que las personas que tenían a cargo su operación interrumpan las actividades relacionadas.

Con objetivos de auditoría, se recomienda guardar una copia de la política y las evidencias que demostraban su implementación y operación.



4. Política de seguridad en el ciclo de desarrollo de software

La política de seguridad en el ciclo de desarrollo de software es un documento de alto nivel que expresa las intensiones de la alta dirección con respecto a la seguridad que debe incluir todas las nuevas aplicaciones (o cambios sobre ellas) que se desarrollen al interior de una empresa o entidad.

La política puede incluir varias cláusulas, entre ellas observemos algunos ejemplos:

- "Todo desarrollo de software deben seguir el proceso de desarrollo seguro definido por la organización".

- “Los desarrollos entregados a clientes deben estar debidamente probados y certificados con respecto a su seguridad”.
- “La organización pondrá a disposición de sus desarrolladores los recursos y capacidades requeridas para lograr un software seguro”.

Como se puede ver, el lenguaje es bastante entendible y no utiliza ningún tipo de tecnicismo.

Estructura de la política

La política de seguridad en el ciclo de desarrollo, como cualquier otra política de seguridad de la información, debe incluir al menos las siguientes secciones:

- **Título:** estableciendo el nombre apropiado, que de indicios de su contenido.
- **Control de cambios:** indicando la versión del documento, la fecha y un detalle de los cambios.
- **Contenido:** es la política como tal, incluye el clausulado relacionado con seguridad en el ciclo de desarrollo de software.
- **Sección de autores:** incluye los nombres y/o las firmas de las personas que elaboraron, revisaron y aprobaron el documento.
- **Referencia:** se pueden incluir referencias a estándares o buenas prácticas relacionadas como PCI DSS (PCI Security Standards Council, 2016) o ISO/IEC 27001 (International Organization for Standardization, 2013).

Adicionalmente el documento generalmente tiene una codificación, de acuerdo con los procesos de gestión documental que tenga la empresa o la entidad.

Generalmente la política es un documento no muy largo, pues al ser directrices gerenciales y de alto nivel no ocupan mucho texto, generalmente no exceden las diez hojas de contenido.

Otro punto importante es el tema del etiquetado del documento. Generalmente estos documentos no salen de las organizaciones, por lo que se deben etiquetar o marcar de alguna manera. Como ejemplo, veamos a continuación una “marca de agua” que indica que el documento es de uso interno:

Mediante esta técnica se busca proteger de alguna manera el documento. De igual forma, algunas organizaciones deciden asegurar más el documento mediante alguna de las siguientes técnicas:

- Contraseña de acceso
- Cifrado

- Firma digital
- Doble factor de autenticación

Figura 2. Marca de agua

Fuente: elaboración propia

Será decisión de la organización implementar los controles que requiera, teniendo en cuenta la criticidad que tiene para ella el que este documento sea accedido por personas no autorizadas.

¿Sabía qué...?

La política de seguridad en el ciclo de desarrollo debe ser idealmente aprobada por el director, gerente general o CEO de la compañía o entidad.

5. Proceso de seguridad en el ciclo de desarrollo de software

El proceso de seguridad en el ciclo de desarrollo es el documento que sigue en el nivel de la pirámide de documentación que definimos. Antes de entrar en materia, debemos tener claro que en general un proceso es un conjunto de actividades que convierten entradas en salidas.

El proceso de seguridad en el ciclo de desarrollo incluye más detalle que la política, y se escribe de acuerdo a las definiciones propias de cada empresa. Las actividades y sus agrupaciones están relacionadas entre sí, como se observa en el siguiente ejemplo:

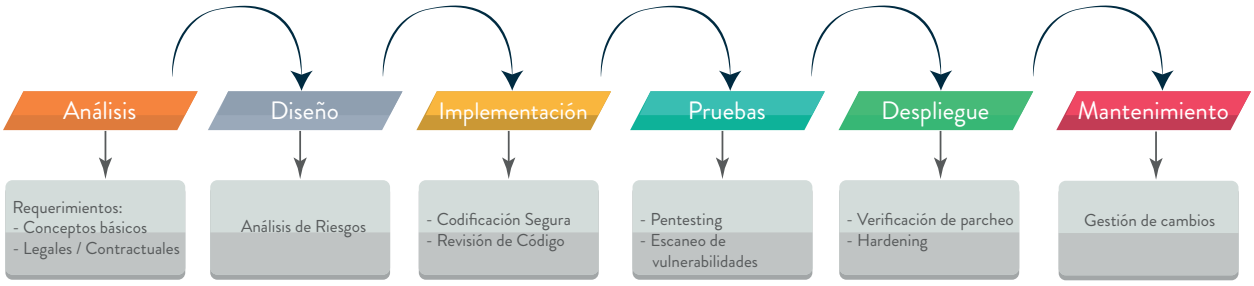


Figura 3. Ejemplo de proceso de seguridad en el ciclo de desarrollo

Fuente: elaboración propia

En este caso, se han definido 6 etapas o fases que componen el proceso. Para cada una de ellas se debe describir su objetivo y su descripción. Posteriormente se describe también cuál es el objetivo y en que consisten las actividades de cada etapa.

Como se puede ver, el proceso es la puerta de entrada a elementos nuevos que no se incluyen en la política, entre ellos:

- Conceptos técnicos
- Diagramas de proceso
- Relaciones entre elementos

En síntesis...

Existe documentación que soporta la implementación de la seguridad en el ciclo de desarrollo de software.

Es importante recordar que al igual que para la política de seguridad, se pueden incluir cláusulas o textos que indican como se ejecuta el proceso, por ejemplo: “El ciclo de desarrollo seguro de software incluye actividades de seguridad a realizar para las fases de análisis, diseño, implementación, pruebas, despliegue y mantenimiento”. Tampoco se debe olvidar que el proceso hace parte de la definición del “que” y no del “como”, por lo que si bien es un poco más detallado, no lo hace con un nivel de profundidad elevado.

Finalmente es importante recordar que al igual que a la política, este documento debe contar con los niveles de protección que defina la organización, preferiblemente como resultado de un análisis de riesgos.

Referencias

PCI Security Standards Council. (2016). *Requisitos y procedimientos de evaluación de seguridad.* Recuperado de https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_3_es-LA.pdf?agreement=true&time=1512747614564

International Organization for Standardization. (2013). *Sistemas de Gestión de Seguridad de la Información*. Recuperado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Seguridad en el Ciclo de Desarrollo

Unidad 4: Políticas sobre la seguridad en el ciclo de desarrollo en la empresa

Escenario 7: Política y proceso de seguridad en el ciclo de desarrollo

Autor: Miguel Ángel Zambrano Puentes

Asesor Pedagógico: Edwin Mojica Quintero

Diseñador Gráfico: Brandon Steven Ramírez Carrero

Asistente: Ginna Quiroga