

What is System/ Security Lifecycle?

The System/Security Lifecycle is a process that helps keep a system secure throughout its development and use. It focuses on finding sa mga possible na mga risks and threats early on and making sure security measures are in place to protect the system. So it's about actively applying security measures and continuously managing them para ma reduce ang risk sa mga cyberattacks. Meaning mag take ka ug mga necessary na steps to ensure na ang system is safeguarded from potential threats or attacks. This process continues throughout the life of the system, ensuring na ang system is secure from start to finish.

So the difference between SecSDLC and SDLC is:

SDLC, it focuses on the process of designing, testing, and deploying software systems. Security is often considered only at the end of the development cycle, mostly during testing and deployment. Meaning di pa kay prioritize and security during sa development, instead, ayha na dayun ang security after mahuman ang system sa pag designed o pag developed.

On the other hand SecSDLC Security is integrated into every phase, so gikan sa planning to design to testing and maintenance, ensuring na ang system is secure from the start to the end. Sa SecSDLC, Security is prioritized during sa development process.

So example is nag develop ka ug online banking system. So kung I follow nimo ang ang SDLC ra, mag design ka sa system, implement ka ug mga features ug later na dayun nimo hunahunaon ang security. But with SecSDLC, security is built into every phase, for example, encryption for transactions, kanang I convert niya ang data into a secure format na readable lang o ma access lang sa sa naay correct na decryption key. Authentication measures, it is used to confirm ang identity sa users na mo try ug access system.

ORIGIN AND HISTORY

the **System Development Life Cycle (SDLC)** was created in the 1960s to help businesses efficiently manage the increasing complexity of data processing systems. So before, software development lacked a structured process. Developers would build systems, without clear planning, documentation. Tungod kay ang security threats kay gakahitabo na, **SecSDLC** was developed to ensure that security is considered right from the start of creating the software.

(Geoffrey Elliott, in *Global Business Information Technology*, explains that large corporations adopted **SDLC** because they needed a structured approach to handle complex business systems that processed vast amounts of data.)

The SDLC is sometimes called waterfall methodology because each step must be completed before moving to the next step o phase.