Centro Universitário de Anápolis - UniEvangélica
Engenharia de Computação
Disciplina: Gerência de Configuração de Software
Docente: Renata Dutra Braga
Acadêmicos: Éber Lucas e Sidney Junio
7º Período

GCO6 - O armazenamento, o manuseio e a liberação de itens de configuração e baselines são controlados

Todos os componentes ou produtos de trabalho que forem itens de configuração, tanto de trabalhos quanto de processos, são armazenados no sistema de Gerência de Configuração, seguindo as especificações definidas para cada tipo de item de configuração. Além disso, o acesso a esses componentes ou produtos de trabalho é controlado, tanto sob o ponto de vista de concorrência quanto sob o ponto de vista de autorização, evitando que aconteça retrabalho ou que informações sensíveis sejam acessadas por pessoas não autorizadas. Assim, controles são estabelecidos para registrar (por exemplo, fazer check-in) e retirar (por exemplo, fazer check-out) itens do sistema de Gerência de Configuração, bem como para gerenciar a concorrência no uso/manuseio, por exemplo, por meio do estabelecimento de ramos (branches).

Evidências: uso do GITHUB, GITLAB ou SVN para armazenar itens de configuração e restringir acesso de informações sensíveis através do uso de restrição de perfis de usuários. Também através dos Sistemas citados o uso de Branchs e merge.

Em situações onde existem informações sensíveis armazenadas no sistema de Gerência de Configuração e em que esse sistema é acessado por meios inseguros, por exemplo, Internet, é necessário que canais de segurança sejam estabelecidos, por exemplo, SSL (Secure Sockets Layer), evitando que pessoas externas ao processo tenham acesso a essas informações. Vale ressaltar que o mero estabelecimento de mecanismos de autorização não é suficiente para fornecer níveis adequados de segurança nesses cenários. Caso a organização esteja implementado o Nível C de maturidade do MR-MPS-SV, o processo de Gerência da MR-MPS-SV – Guia de Implementação – Parte 2:2013 27/66 Segurança da Informação (GSI) deverá ser envolvido para as questões relativas aos riscos de segurança da informação.

Evidência: uso de um canal criptografado (protocolo) entre um servidor web e um navegador (browser) para garantir que todos os dados transmitidos sejam sigilosos e seguros, por exemplo: SSL e suas demais versões.

É necessário, ainda, estabelecer um controle para a liberação de baseline aos interessados e autorizados, contendo tanto versões para a produção quanto produtos de trabalho fechados, incluindo o empacotamento e a entrega. A liberação de uma baseline para o cliente só ocorre após autorização do CCC (Comitê de Controle de Configuração) e execução dos procedimentos de auditoria. Além disso, é importante o estabelecimento de rastreabilidade entre a baseline que originou a liberação, a liberação propriamente dita e o cliente que recebeu a liberação. Caso a organização esteja implementado o Nível C de maturidade do MR-MPS-SV, estes procedimentos devem ser executados de acordo com o que está definido no processo Gerência de Liberação (GLI).

Evidência: o uso do GITLAB realiza o controle de baseline através do administrador do projeto cadastrado no Sistema de Gerenciamento, uma vez que ele possui histórico da distribuição das baselines e controla a sua distribuição. Algumas decisões que devem ser tomadas junto ao Comitê e após uma auditoria.