tecnologia a serviço da cidade
procempa

Normas para Desenvolvimento de Aplicações e Sistemas

Junho, 2022

Normas para Desenvolvimento de Aplicações e Sistemas

1. Não é permitida a transferência de dados confidenciais para processamento ou armazenamento em serviços externos, de terceiros não contratados formalmente pela companhia ou cliente para tal finalidade e sem obrigação legal.
2. Armazenamento e transferências de dados confidenciais devem ser sempre criptografadas com mecanismos aprovados pela Equipe de Segurança da Informação.
3. Os sistemas deverão gerar registros (logs) de todos os eventos de segurança. Devem ser utilizados para este fim recursos do sistema operacional, banco de dados, aplicação ou de sistema de segurança específico (SIEM), quando disponível. Para fins de investigação ou auditoria, os registros deverão conter ao menos as seguintes informações: identificação da aplicação, função, usuário, equipamento ou endereços IP usados, momento da ocorrência (timestamp) e as operações de dados relevantes. Informações confidenciais não devem ser registradas em log sem estarem criptografadas. Deve-se observar a Política de Retenção de Registros vigente, respeitando normas e legislação.
4. No desenvolvimento e manutenção de sistemas é obrigatório o uso do software e repositório de controle e versionamento de arquivos (como fontes, modelos, documentos, diagramas, páginas web) aprovado pela companhia.
5. Cada desenvolvedor é responsável pela integridade dos arquivos de sistema que estão sendo trabalhados, devendo manter cópias e utilizar áreas de trabalho em servidores designados.
6. Todo o desenvolvedor de aplicações deverá seguir, quando disponíveis e forem aplicáveis, as recomendações de segurança para o desenvolvimento.

Normas para Administração de Servidores

1. Todas as instalações de novos servidores deverão seguir procedimentos padrões (pacotes, Service Packs, Hot Fixes obrigatórios);
2. Após sua instalação o responsável deverá encaminhar à Equipe de Segurança solicitação para verificação complementar do servidor;
3. As atualizações de segurança necessárias serão encaminhadas pela Equipe de Segurança aos responsáveis por cada Servidor;
4. A instalação das atualizações de segurança deverá ser realizada pelo responsável direto de cada servidor, seguindo as orientações de segurança no que tange ao backup antes do procedimento, adequação de horário e plano de recuperação de falhas;
5. Acessos remotos devem ser feitos sempre usando mecanismos criptografados. Devem ser desativados os serviços de acesso remoto que não usam criptografia, tais como TELNET, FTP e VNCSERVER;
6. Os equipamentos utilizados devem possuir sistema operacional atualizado e com recursos de segurança.
7. A ativação de novos serviços de rede será condicionada a uma análise de riscos (a ser realizada pela Equipe de Segurança), onde, no mínimo, os seguintes aspectos serão considerados: requisitos de segurança do serviço, objetivo, alvo do serviço, forma de acesso, forma da administração e volume de tráfego
8. Não é permitida a instalação de serviços de rede não autorizados pela Equipe de Segurança.
9. Todo o tráfego de informações confidenciais por meio compartilhado será protegido através de criptografia;
10. Sistemas de proteção de acesso (firewall) devem ser utilizados para permitir apenas às redes ou máquinas alvo dos serviços o acesso aos mesmos;
11. Ferramentas de detecção de intrusos devem monitorar as redes, emitindo alertas e registros sobre possíveis tentativas de invasão.