GAP Análise Segurança da Informação e

Desenvolvimento de Sistemas

|  |  |
| --- | --- |
| **Política de Segurança** |  |
| **Política de Segurança da Informação** |  |
| Existe um documento de Política de Segurança da Informação? |  |
| A revisão da PSI são realizadas? |  |
| **Organização da Segurança da Informação** |  |
| **Organização Interna** |  |
| Existe o compromisso da gestão de segurança da informação? |  |
| Existe uma coordenação de segurança da informação? |  |
| As atribuição e responsabilidades de segurança da informação são definidas? |  |
| Existe um processo de autorização e avaliação de segurança para novas instalações de processamento de informações? Existe uma carta de Anuência |  |
| Existe um documento sobre acordos de confidencialidade entre partes? |  |
| Existe contato com as autoridades ou organizações de segurança da Informação (CERTBR)? |  |
| Existe contato com outros grupos? |  |
| Existe um processo de revisão independente da segurança da informação? Existe uma iniciativa por parte da “Matriz” um programa denominado Pathfinder |  |
| **Partes Externas** |  |
| Existe uma avaliação de risco relacionados a partes externas? |  |
| Existem procedimentos de segurança dirigidos ao lidar com clientes? |  |
| Existe procedimentos de segurança dirigindos a segurança em contratos de terceiros? |  |
| **Gestão De Ativos** |  |
| **Responsabilidade para Ativos** |  |
| Existem procedimentos de Inventário de Ativos? |  |
| Existem procedimentos referente a Propriedade de bens? |  |
| Existe uma política de Uso aceitável dos ativos? |  |
| **Classificação da informação** |  |
| Existe uma diretrizes de classificação das informações? |  |
| As informações e documentos da organização são rotulados e possuem tratamento da informação? |  |
| **Recursos Humanos Segurança** |  |
| **Antes da contratação de um empregado** |  |
| Existe a definição clara de Papéis e responsabilidades? |  |
| Existe um documento de Termos e condições do emprego? |  |
| Os funcionários contratados possuem conhecimento e são capacitados em relação à aspectos de segurança da informação e diligência? |  |
|  |  |
| **Durante o emprego** |  |
| Existem critérios de responsabilidades e gestão sobre os funcionários em relação à segurança da informação? |  |
| Os colaboradores possuem consciência da segurança da informação, educação e formação? |  |
| Existe um processo formal e documentado sobre questões disciplinares? |  |
| **Rescisão ou mudança de emprego** |  |
| Existe o termo de responsabilidades sobre rescisão ou mudança de emprego? |  |
| Existe um procedimento formal de devolução dos ativos? |  |
| Existe um procedimento formal de remoção de direitos de acesso? |  |
| **Segurança Física e Ambiental** |  |
| **Áreas seguras** |  |
| Existem controles de proteção do perímetro? |  |
| Existe o controles de entrada física? |  |
| Existem controles de proteção dos escritórios, salas e instalações? |  |
| Existem controles proteção contra ataques externos e ambientais? |  |
| Existem controles de trabalho em relação as áreas seguras? |  |
| Existem Áreas de acesso público, de entrega e de carregamento? |  |
| **Equipamento de segurança** |  |
| Mapa Localização e proteção do equipamento? R. Topologia |  |
| Existe utilitários de apoio? |  |
| O cabeamento de segurança é protegido? |  |
| Existe procedimento de Manutenção de equipamentos? |  |
| Existe algum procedimento de segurança e proteção em caso de de equipamentos fora da organização? |  |
| Existe um procedimento de eliminação segura ou reutilização de equipamentos? |  |
| Existe um procedimento de remoção de propriedade? |  |
| **Comunicação e Gestão de Operações** |  |
| **Procedimentos e responsabilidades operacionais** |  |
| Os procedimentos operacionais documentados? |  |
| Existem procedimentos de Gestão de Mudanças? |  |
| Existem um procedimento sobre segregação de função? R. Existe, mas não documentado |  |
| Existe a separação de desenvolvimento, teste e produção? |  |
| **Terceiro gestão de prestação de serviços** |  |
| Existem processos de gestão sobre os serviço de terceiros? |  |
| Existem processos de monitoramento e avaliação de serviços de terceiros? |  |
| Existem processos para gerenciar mudanças nos serviços de terceiros?R. Não existe uma documentação sobre procedimentos. |  |
| **Planejamento do sistema e validação** |  |
| Existe um procedimento sobre gerenciamento de capacidades? TI não é envolvida, apenas sistema |  |
| Existe um processo formal sobre validação dos sistemas da organização? R. Com base em checklist |  |
| Segurança da documentação dos sistemas |  |
| **Proteção contra códigos maliciosos e móvel** |  |
| Existem controles contra códigos maliciosos? |  |
| Existem controles contra códigos móveis? |  |
| **Back-up** |  |
| Existem procedimentos definidos sobre as informações de back-up? |  |
| **Gestão de segurança de rede** |  |
| Existem mecanismos de controle e gestão da Rede? |  |
| Existem mecanismos de segurança dos serviços de rede? |  |
| **A manipulação de mídia** |  |
| Existe um procedimento sobre mídias removiveis? |  |
| Existe um procedimento sobre Descarte de mídia |  |
| Existe um procedimento sobre tratamento das informações nas midías removeis? |  |
| **Intercâmbio de informações** |  |
| Políticas e procedimentos de intercâmbio de informações? R. Apenas NDA |  |
| Acordos de intercâmbio? |  |
| Mídia física em trânsito? |  |
| Troca de Mensagens eletrônicas em formato/canal seguro? |  |
| Existem Sistemas de troca de informações de negócios com terceiros? |  |
| **Serviços de comércio eletrônico** |  |
| Comércio eletrônico? |  |
| Transações on-line? |  |
| Existe publicidade das informações disponíveis? |  |
| **Monitoração** |  |
| Existe o log de auditoria? |  |
| A organização possui sistema de monitoramento? Parcial Apenas Servidor, não aplicações |  |
| Existe Proteção das informações de log? N Por quanto tempo essa informação é retida? |  |
| Existe um administrador e operador registos? |  |
| Existe o Registro de falhas e erros? |  |
| Os dispositivos possuem sincronização do relógio? |  |
| Já houve a necessidade de uso do Log para questões legais, técnicas e de segurança da informação? |  |
| **Controle De Acesso** |  |
| **Requisitos de negócio para controle de acesso** |  |
| Existe uma política de controle de acesso? |  |
| **Gerenciamento de acesso do usuário** |  |
| Existe o registro do usuário? |  |
| Existe um gerenciamento de privilégios? |  |
| Existe um gerenciamento de senhas do usuário? |  |
| Existe um procedimento de revisão dos direitos de acesso do usuário? |  |
| **Responsabilidades de usuários** |  |
| Existe uma política de senhas e de uso de senha? |  |
| Existem equipamentos para utilização autónoma? |  |
| Existe uma política de mesa e tela limpa? 5S |  |
| **Controle de acesso à rede** |  |
| Existe uma política de uso de serviços de rede? |  |
| Existe uma autenticação do usuário para uso de conexões externas? IN? OUT? |  |
| Existe um controle de identificação dos equipamentos na rede? |  |
| Existe proteção de diagnóstico e porta de configuração remota? |  |
| Existe segregação de redes? |  |
| Existe o controle de conexão de rede? |  |
| Existe o controle sobre questões de roteamento de rede? |  |
| **Controle de acesso do sistema operacional** |  |
| Existe um procedimento de logon seguro? |  |
| Existe controle de Identificação de usuário e autenticação? |  |
| Existe um sistema de gerenciamento de senhas? |  |
| Existe controle sobre a utilização de utilitários do sistema e novas instalações? |  |
| Existe controle de timeout de sessão? |  |
| Existe controle de limitação de tempo de conexão? |  |
| Existe controle de limitação de acesso simultâneo? |  |
| **Controle de aplicativos e acesso à informação** |  |
| Existem controles de restrição de acesso à informação? |  |
| Existe o Isolamento de sistemas sensíveis? |  |
| **Computação móvel e teletrabalho** |  |
| Existem procedimentos sobre computação móvel e comunicações? |  |
| Existem procedimentos sobre Teletrabalho/Home Office? |  |
| **Sistemas de informação de aquisição, desenvolvimento e manutenção** |  |
| **Os requisitos de segurança dos sistemas de informação** |  |
| Existem procedimentos sobre análise de requisitos de segurança e especificações? |  |
| **Processamento correto em aplicações** |  |
| Existem controles de Validação de entrada de dados? |  |
| Existem controle sobre o processamento interno dos sistemas? |  |
| Existem procedimentos de validação da integridade da mensagem/dados? |  |
| Existem procedimentos sobre validação de dados de saída? |  |
| **Controles criptográficos** |  |
| Existe uma política sobre o uso de controles criptográficos? |  |
| Existe um sistema de gerenciamento de chaves? |  |
| **Segurança de arquivos do sistema** |  |
| Existe o controle de software operacional? |  |
| Existem mecanismos de proteção de dados de teste do sistema? |  |
| Existem procedimentos sobre o controle de acesso ao código-fonte do programa? |  |
|  |  |
| **Segurança nos processos de desenvolvimento e de apoio** |  |
| Existem procedimentos de controle de alteração? Existe a ferramenta de controle de versionamento/Backup de código |  |
| Existem um procedimento de Avaliação técnica das aplicações após mudanças no sistema operacional? |  |
| Existe um procedimento de restrições sobre mudanças em pacotes de software? |  |
| Existem um procedimento sobre vazamento de informações? |  |
| Existe um procedimento sobre desenvolvimento de software terceirizado? |  |
| **Vulnerability Management Técnico** |  |
| Existe um Controle de vulnerabilidades técnicas? |  |
| **Gestão de incidentes de segurança da informação** |  |
| **Relatar eventos e fraquezas de segurança da informação** |  |
| Existe um procedimento formal para relatar eventos de segurança da informação? |  |
| Existe documentos reportando pontos fracos? |  |
| **Gestão de incidentes de segurança da informação e melhorias** |  |
| Existem procedimentos sobre gestão de incidentes com responsabilidades e procedimentos? |  |
| Existem um processo formal de aprendizado sobre os incidentes de segurança da informação? |  |
| Existe procedimentos sobre forense computacional em caso de incidentes? |  |
| **Gestão de Continuidade de Negócios** |  |
| **Aspectos da gestão de continuidade de negócios de segurança da informação (EM DESENVOLVIMENTO)** |  |
| A segurança da informação está incluindo no processo de gestão de continuidade de negócios existentes? |  |
| A continuidade dos negócios e avaliação de riscos |  |
| Desenvolvimento e implementação de planos de continuidade, incluindo a segurança da informação |  |
| Estrutura de planejamento de continuidade de negócios |  |
| Teste de manutenção e reavaliação dos planos de continuidade de negócios |  |
| **Compliance** |  |
| **Cumprimento dos requisitos legais** |  |
| Existem procedimentos/politicas para Identificação da legislação aplicável? |  |
| Existem documentos e/ou procedimentos sobre direitos de Propriedade Intelectual (DPI)? |  |
| Existem Proteção de registros da organização? |  |
| Existem Proteção de dados e privacidade de informações pessoais? |  |
| Existem procedimentos de Prevenção do uso indevido das instalações de processamento de informação? |  |
| Existem procedimentos de regulamentação de controles de criptografia? |  |
| **Conformidade com as políticas e normas de segurança e conformidade técnica** |  |
| Existem procedimentos de Conformidade com as políticas e normas de segurança? |  |
| Existem procedimentos de Verificação de conformidade técnica? |  |
| **Sistemas de informação e considerações de auditoria** |  |
| Existem procedimentos de gestão sobre os Sistemas de informação e controles de auditoria? |  |
| Existem ferramentas de auditoria de sistemas de informação? |  |

|  |  |
| --- | --- |
| **Avaliação de sistemas de informação** |  |
|  |  |
| **Desenvolvimento de Sistemas** |  |
| Os usuários do sistema estão envolvidos na especificação da aplicação? |  |
| O analista responsável é identificado? |  |
| O analista documenta as reuniões, inclusive as deliberações? |  |
| O formato, meio e distribuição das informações são especificados? |  |
| O ambiente da aplicação (hardware e software) é especificado? |  |
| Os requisitos de segurança da informação são apropriadamente considerados? |  |
| Os controles internos são incorporados ao desenho do sistema? |  |
| **Aquisição de Sistemas** |  |
| Os usuários descrevem as especificações das funções imprescindíveis do sistema? |  |
| As especificações são revistas pela gerência? |  |
| Um número considerável de fornecedores mais considerados no mercado é convidado para apresentar propostas? |  |
| A decisão por um fornecedor específico leva em consideração os critérios de análise de custo/benefícios? |  |
| **Desenvolvimento de Sistemas** |  |
| Os programas são desenvolvidos de maneira consistentes e de acordo com os padrões de programação segura? |  |
| A codificação de novos programas ou alteração de programas está sujeita a revisão? |  |
| Programas novos ou alterados são colocados em produção antes de estarem autorizados pelos gestores? |  |
| **Testes de Sistemas** |  |
| Existe rotina e procedimentos para testar aplicativos novos ou alterados? |  |
| Os testes são executados com dados hipotéticos? |  |
| A geração de massa de teste é feita por meio de ferramenta específica? |  |
| Os testes são realizados, completados e analisados antes do sistema ser colocado em produção? |  |
| Os usuários revisam os resultados do teste e dão aceite formal antes do sistema ser colocado em produção? |  |
| **Documentação de Sistemas** |  |
| A documentação é atualizada e reflete exatamente o sistema em produção? |  |
| A documentação é suficientemente detalhada para suportar as futuras modificações no sistema? |  |
| As instruções ao usuário são suficientemente detalhadas para permitir a correta utilização do sistema? |  |
| A documentação sigilosa é armazenada em área segura? |  |
| **Segurança de Sistemas** |  |
| O código fonte é armazenado de foram segura? |  |
| As alterações nos códigos são controladas? |  |
| Os times de desenvolvimento realizam desenvolvimento fora da empresa? |  |
|  |  |