Criptografia e Segurança da Informação

Criptografia

António Santos

ISTEC

Tópicos

Mecanismos de Segurança

- Aplicar as atualizações de segurança recomendadas
- Utilizar e atualizar com frequência os programas antivírus e antispyware
- Realizar cópias de segurança com regularidade
- Utilizar senhas robustas e diferentes em cada aplicação

Mecanismos de Segurança

- Procurar enviar/transferir a sua informação de forma encriptada
- Não partilhar a informação do seu computador com outros
- Não compartilhar ou divulgar as suas passwords com os outros
- Ser responsável e cuidadoso na utilização da Internet e do correio eletrónico

Mecanismos de Segurança

- Ser cuidadoso na utilização de equipamentos de armazenamento externos
- Informar no caso de incidentes com vírus, roubos ou perdas de informação
- Estar ciente que todos os atos praticados têm consequências

Mecanismos de Segurança

- Utilizar um firewall.
- Bloquear o computador quando se ausentar
- Não utilizar software ilegal ou de compartilhamento de arquivos.

Normas ISO para Gestão do Risco dos SI

Normas ISO para Gestão do Risco dos Sistemas de Informação apresentam soluções para as organizações se precaverem de riscos, por forma a cuidarem dos seus sistemas de informação da melhor forma possivel.

Norma ISO IEC 17799

Política de segurança da informação (Security Policy)

- Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Norma ISO IEC 17799

Organizando a segurança da informação (Organization of Information Security)

- Infra-estrutura da segurança da informação - Gerir a segurança da informação dentro da organização;
- Partes externas - Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acedidas, processadas, comunicadas ou geridas por partes externas;
- Manter a segurança da informação quando a responsabilidade do seu processamento é delegada noutras organizações.

Norma ISO IEC 17799

Gestão de ativos (Asset Management)

- Responsabilidade pelos ativos - Alcançar e manter a proteção adequada dos ativos da organização;
- Classificação da informação - Assegurar que a informação receba um nível adequado de proteção.

Norma ISO IEC 17799

Segurança em recursos humanos (Human Resources Security)

- Antes da contratação - Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos;
- Durante a contratação - Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano;

Norma ISO IEC 17799

Segurança física e do ambiente (Physical and Environmental Security)

- Áreas seguras - Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.
- Segurança de equipamentos - Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

Norma ISO IEC 17799

Gestão das operações e comunicações (Comunications and Operations Management)

- Procedimentos e responsabilidades operacionais - Garantir a operação segura e correta dos recursos de processamento da informação.
- Gestão de serviços terceirizados - Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.
- Planeamento e aceitação dos sistemas - Minimizar o risco de falhas nos sistemas.
- Proteção contra códigos maliciosos e códigos móveis - Proteger a integridade do software e da informação.
- Cópias de segurança - Manter a integridade e

Norma ISO IEC 17799

Controle de acessos (Access Control)

- Requisitos de negócio para controle de acesso - Controlar acesso à informação.
- Gestão de acesso do utilizador - Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.
- Responsabilidades dos utilizadores - Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.
- Controle de acesso à rede - Prevenir acesso não autorizado aos serviços de rede.
- Controle de acesso ao sistema operativo - Prevenir acesso não autorizado aos sistemas operativos.

Norma ISO IEC 17799

Aquisição, desenvolvimento e manutenção de sistemas de informação (Information Systems Acquisition, Development and Maintenance)

- Requisitos de segurança de sistemas de informação - Garantir que segurança é parte integrante de sistemas de informação
- Processamento correto nas aplicações - Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.
- Controles criptográficos - Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.
- Segurança dos arquivos do sistema - Garantir a segurança de arquivos de sistema.

Norma ISO IEC 17799

Gestão de incidentes de segurança da informação (Information Security Incident Management)

- Notificação de fragilidades e eventos de segurança da informação - Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.
- Gestão de incidentes de segurança da informação e melhorias - Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

Norma ISO IEC 17799

Gestão da continuidade do negócio (Business Continuity Management)

- Aspectos da gestão da continuidade do negócio, relativos à segurança da informação - Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

Norma ISO IEC 17799

Conformidade (Compliance)

- Conformidade com requisitos legais - Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
- Conformidade com normas e políticas de segurança da informação e conformidade técnica - Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.
- Considerações quanto à auditoria de sistemas de informação - Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.

Norma ISO/IEC 27002

Políticas de segurança da informação (Information security policies)

- Direção de gestão para segurança da informação - Fornecer à direção de gestão e suporte a segurança da informação, de acordo com os requisitos comerciais, as leis e regulamentos relevantes.

Norma ISO/IEC 27002

Organização da segurança da informação (Organization of information security)

- Organização interna - Estabelecer uma estrutura de gestão para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.
- Dispositivos móveis e teletrabalho - Garantir a segurança do teletrabalho e do uso de dispositivos móveis.

Norma ISO/IEC 27002

Segurança de recursos humanos (Human resource security)

- Antes do emprego - Garantir que funcionários e contratados compreendam suas responsabilidades e sejam adequados para as funções para as quais são considerados.
- Durante o emprego - Para garantir que funcionários e contratados estejam cientes e cumpram as suas responsabilidades de segurança da informação.
- Rescisão e mudança de emprego - Proteger os interesses da organização como parte do processo de alteração ou rescisão do emprego.

Norma ISO/IEC 27002

Gestão de ativos (Asset management)

- Responsabilidade por ativos - Identificar ativos organizacionais e definir responsabilidades de proteção apropriadas.
- Classificação das informações - Garantir que as informações recebam um nível adequado de proteção, de acordo com a sua importância para a organização.
- Manuseio dos suportes de informação - Impedir a divulgação, modificação, remoção ou destruição não autorizada de informações armazenadas nos suportes de informação.

Norma ISO/IEC 27002

Controle de acesso (Access control)

- Requisitos comerciais de controle de acesso - Limitar o acesso a informações e recursos de processamento de informações.
- Gestão de acesso do utilizador - Para garantir o acesso autorizado do utilizador e impedir o acesso não autorizado a sistemas e serviços.
- Responsabilidades do utilizador - Responsabilizar os utilizadores pela proteção das suas informações de autenticação.
- Controle de acesso ao sistema e aplicativos - Impedir o acesso não autorizado a sistemas e aplicativos.

Norma ISO/IEC 27002

Criptografia (Cryptography)

- Controles criptográficos - Garantir o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e/ou integridade das informações.

Norma ISO/IEC 27002

Segurança física e ambiental (Physical and environmental security)

- Áreas seguras - Impedir o acesso físico não autorizado, danos e interferência nas informações e instalações de processamento de informações da organização.
- Equipamento - Evitar perda, dano, roubo ou comprometimento de ativos e interrupção das operações da organização.

Norma ISO/IEC 27002

Operações de Segurança (Operations security)

- Procedimentos e responsabilidades operacionais - Garantir operações corretas e seguras das instalações de processamento de informações.
- Proteção contra malware - Garantir que as informações e os recursos de processamento de informações estejam protegidos contra malware.
- Backup - Proteger contra perda de dados.
- Logging e monitorização - Registrar eventos e gerar evidências.
- Controle de software operacional - Garantir a integridade dos sistemas operativos.
- Gestão técnico de vulnerabilidades - Impedir a exploração de vulnerabilidades técnicas.

Norma ISO/IEC 27002

Segurança das comunicações (Communications security)

- Gestão de segurança de rede - Garantir a proteção das informações nas redes e suas instalações de processamento de informações de suporte.
- Transferência de informações - Manter a segurança das informações transferidas dentro de uma organização e com qualquer entidade externa.

Norma ISO/IEC 27002

Aquisição, desenvolvimento e manutenção de sistemas (System acquisition, development and maintenance)

- Requisitos de segurança dos sistemas de informação - Garantir que a segurança da informação é uma parte integrante dos sistemas de informação em todo o ciclo de vida. Isso também inclui os requisitos para sistemas de informação que prestam serviços em redes públicas.
- Segurança no desenvolvimento e processos de suporte - Garantir que a segurança das informações seja projetada e implementada no ciclo de vida do desenvolvimento dos sistemas de informação.
- Dados do teste - Garantir a proteção dos dados usados no teste.

Norma ISO/IEC 27002

Relações com fornecedores (Supplier relationships)

- Segurança da informação nos relacionamentos com fornecedores - Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores.
- Gestão da entrega de serviços ao fornecedor - Manter um nível acordado de segurança da informação e entrega de serviços, de acordo com os contratos com os fornecedores.

Norma ISO/IEC 27002

Gestão de incidentes de segurança da informação (Information security incident management)

- Gestão de incidentes e melhorias na segurança da informação - Garantir uma abordagem consistente e eficaz da gestão de incidentes de segurança da informação, incluindo a comunicação sobre eventos e pontos fracos da segurança.

Norma ISO/IEC 27002

Aspectos da segurança de informação da gestão de continuidade de negócios (Information security aspects of business continuity management)

- Continuidade da segurança da informação - A continuidade da segurança da informação deve ser incorporada nos sistemas de gestão de continuidade de negócios da organização.
- Redundâncias - Para garantir a disponibilidade de recursos de processamento de informações.

Norma ISO/IEC 27002

Conformidade (Compliance)

- Cumprimento dos requisitos legais e contratuais - Evitar violações das obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e a quaisquer requisitos de segurança.
- Revisões de segurança da informação - Garantir que a segurança da informação seja implementada e operada de acordo com as políticas e procedimentos organizacionais.