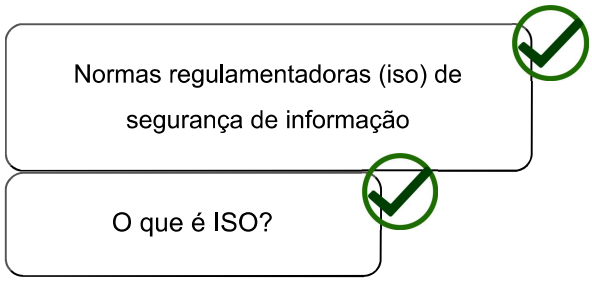
TRILHA DE APRENDIZAGEM

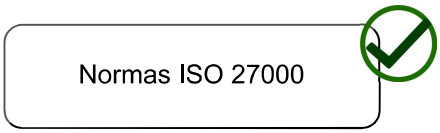
MALWARES E TIPOS DE VÍRUS

VÍRUS – ANTIVÍRUS E BACKUPS

PROBLEMAS DE INVASÕES E COMO TRATÁ-LOS

NORMAS REGULAMENTADORAS (ISO) DE SEGURANÇA DE INFORMAÇÃO





Normas ISO 27000

Vamos conhecer as normas da ISO 27000.

•ISO/IEC 27000

É a introdução à “amília; é a norma básica que inclui o vocabulário, glossário que trata sobre a Gestão da Segurança de Informação.

•ISO/IEC 27001

Publicada em outubro de 2005 essa norma trata sobre os requisitos para que um Sistema de Gestão de Segurança da Informação esteja correto. Essa ISO define quais são os requisitos para o sistema, e o descreve como sendo um sistema de organização baseado na prevenção, além definir a segurança da informação como conhecemos;

•A ISO 27001

Se a empresa quiser obter um certificado de segurança, essa norma é a que deve, em primazia, ser observada, ela é considerada uma ISO aditável, a única quando falamos das normas aditáveis que definem requisitos de SGSI.

•ISO/IEC 27002

Recomendável que seja feito o seu uso junto com a ISO 27001, essa norma trata das políticas que auxiliam a gestão e a colocação de um Sistema de Segurança da Informação. Essa norma é a única em que você poderá tirar certificados profissionais.

•ISO/IEC 27003

Enquanto a ISO 27001 dita apenas os requisitos para um sistema de segurança de informação, a ISO 27003 trata das diretrizes, isto é, dá o “passo a passo” para a criação de um SGSI.

•ISO/IEC 27004

Essa ISO define métricas, isto é, metas para o alcance da segurança da informação e de sua gestão, por isso ela é tão importante quando uma empresa deseja acompanhar de perto os seus resultados.

•ISO/IEC 27006

Ela define o que uma empresa de auditoria deve levar em consideração quando deseja validar o sistema de gestão de segurança da informação de uma empresa X.

•ISO/IEC 27007

Ela deve ser usada em conjunto com a ISO 27006, já que trata dos padrões que a auditoria

deve seguir.

•ISO/IEC 27008

Enquanto a ISO 27007 foca nos requisitos que a auditoria deve levar em consideração com o SGSI, essa trata exatamente do controle de segurança.

•ISO/IEC 27009

É uma norma que foca nas indústrias que desejam trabalhar com essa adequação.

•ISO/IEC 27011

Refere-se especialmente ao rito de segurança que deve ser feito por empresas que trabalham com telecomunicações, isto é, *call-center* entre outros.

•ISO/IEC 27013

Ela trata da integração das normas 27001 e 27002, observando como deve ser a implementação delas de maneira conjunta.

•ISO/IEC 27015

Pode ser considerada uma norma que complementa a 27002, e trata da segurança no mercado financeiro.

•ISO/IEC 27016

Aborda os pontos de segurança da informação no que concernem a economia em um todo.

•ISO/IEC 27017

Trata especificamente sobre a segurança em computação na nuvem, ou *cloud computing*.

•ISO/IEC 27018

É uma norma complementadora à 27017, e trata basicamente sobre a PII, a privacidade quando se trata de *cloud computing*, ou computação na Nuvem.

•ISO 27031

Trata de conceitos da segurança de informações no TIC.

•ISO 27033-4

Trata de ameaças de segurança no que se relacionam a *gateways* e informações no que concerne a segurança de redes.

•ISO 27033-5

Fala sobre a proteção de redes utilizando VPN.

•ISO 27033-6

Trata sobre as técnicas e desenhos no que concernem a redes sem fio, sinais e frequências de rádio.

•ISO 27034-1

Essa primeira norma introduz a segurança relativa a aplicações, e trata, basicamente, sobre os conceitos fundamentais aplicados na prática.

•ISO 27034-2

Essa segunda parte trata das associações normativas que trabalham com a segurança de aplicações.

•ISO 27034-3

É um passo a passo do processo de gestão de segurança de aplicações.

•ISO 27034-4

Relacionada também com aplicações, esta norma trata sobre os requisitos para segurança.

•ISO 27034-5

Trata sobre a segurança de aplicativos, cuidando de protocolos de gestão.

•ISO 27034-6

É utilizada apenas para aplicações especificas e é basicamente um guia para a realização delas.

•ISO 27035

Incluindo um guia para criar políticas de gestão de incidentes, essa ISO trata sobre como essa gestão deve ocorrer e cobre as chamadas vulnerabilidades de sistema. Ela trata de maneira mais aprofundada as seções da ISO 27002.

•ISO 27036

Relacionada com as TIC – Tecnologia de Informação e Comunicação, essa norma oferece as diretrizes sobre a avaliação e riscos no que concerne ao fornecimento e aquisição de produtos relacionados às TIC.

•ISO 27037

É a norma que os peritos forenses normalmente mais se atem, já que ela trata das orientações gerais de provas forenses de cunho digital.Essas diretrizes vão desde o momento da identificação da prova até o da preservação, passando pela coleta.

•ISO 27038

Essa norma trata das diretrizes de uma redação digital, observando desde a redação propriamente dita até seu compartilhamento no ambiente digital. Por ser uma norma bastante especifica ela é publicada em sua maioria apenas em casos raros.

•ISO 27039

É um guia que trata desde a confecção até a instalação de sistemas IDS – *Intrusion Detection Systems* -, ou seja, trata dos sistemas que trabalham com a detecção de intrusos.

•ISO 27040

Dita as características da segurança da informação relacionadas a *storage*, ou seja, infraestrutura.

•ISO 27041

Trata dos métodos utilizados para realizar a investigação de dados computacionais, ela integra o rol de normas que tratam da falha de sistema, já que a perícia é realizada quando há falha e a empresa precisa conhecer o problema para tentar solucioná-lo.

•ISO 27042

Trata sobre a interpretação das evidências de caráter digital, isto é, ela fornece a base para que os peritos forenses trabalhem, e deve ser respeitada por eles, já que a desrespeitar pode ocasionar a desconfiança da perícia. Ela difere da 27043 por tratar da interpretação e não do

recolhimento das evidências. Ela integra todo o rol de normas que tratam sobre a perícia no caso de falha na segurança.

•ISO 27043

Como a ISO 27035, essa trata de incidentes de segurança, isso é, quando a segurança falha essa norma trata do processo investigativo para esses incidentes. Essa norma deverá ser empregada por empresas de perícia que, por exemplo, vão investigar o vazamento de dados ou a falha de um sistema X.

•ISO 27044

Trata em específico das diretrizes para a administração de eventos de segurança da informação, os chamados SIEM.

•ISO 27799

Foca especialmente em segurança da informação no que concerne a empresas que tratam de saúde. Concluímos nosso capítulo após conhecer as ISOs da Segurança da Informação.

resumindo:
E então? Gostou do que lhe mostramos? Aprendeu mesmo tudinho? Agora, só para termos certeza de que você realmente entendeu o tema de estudo deste capítulo, vamos resumir tudo o que vimos. Observamos o que são as normas regulamentadoras, cada uma encarregada de traçar regras sobre um determinado assunto dos sistemas operacionais e sistemas da informação, assim, você como profissional da área deve conhece-las e saber a sua aplicabilidade.

Referências

CHAVES, E. O. C.; FALSARELLA,O. M. Os sistemas de informação
e sistemas de apoio à decisão. Revista do Instituto de Informática, v. 3, n. 1, 1995.

AS NORMAS da família ISSO 2700. **Portal GSTI**, 2013. Disponível em: https://bit.ly/3tW5y47. Acesso em: 30 nov. 2021.

LOVEJOY, W. Integrated operations: a proposal for operations management teaching and reserarch. Production and Operations Management. v. 7, 1996.

Voltar