LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Boas Práticas em Segurança da Informação:
Padrões Frameworks e Controles de Segurança da Informação

Olá pessoal! Como vimos na publicação anterior, é imprescindível que a instituições se orientem por um conjunto de documentos para melhorar o gerenciamento de riscos de segurança cibernética.

Assim, passaremos a apresentar as normas ABNT NBR ISO/IEC mais importantes na construção de uma política de segurança da informação sólida e confiável.

ABNT NBR ISO/IEC 27001:2013. Sistemas de gestão da segurança da informação

É uma norma do comitê técnico formado pela ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), aprovada e traduzida pela Associação Brasileira de Normas Técnicas (ABNT) - e transformada em uma Norma Brasileira (NBR) - de gestão de segurança da informação. São apresentados os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de gestão da Segurança da Informação (SGSI), bem como os requisitos para avaliação e tratamento de riscos de segurança da informação, sempre com o foco nas necessidades da organização.

A ABNT NBR ISO/IEC 27001:2013 é dividida em 11 seções e Anexo A, sendo que as seções de 0 a 3 são introdutórias (não obrigatórias), e as seções de 4 a 10 são obrigatórias. Controles do Anexo A devem ser implementados apenas se declarados como apropriados e aplicáveis na Declaração de Aplicabilidade.

A SEF/MG possui o processo de Autorização da Emissão da Nota Fiscal Eletrônica certificado na norma ISO/IEC 27001:2013 desde 2014. Isso demonstra o compromisso da organização com a Segurança da Informação dos contribuintes do Estado de Minas Gerais.

Fique ligado nas próximas publicações para conhecer as demais normas que preferencialmente devem orientar a política de segurança da informação nas entidades.

Até a próxima!

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Boas Práticas em Segurança da Informação:
Padrões Frameworks e Controles de Segurança da Informação

Prezados colegas e colaboradores, hoje continuamos a abordagem às normas ABNT NBR ISO/IEC mais importantes na construção de uma política de segurança da informação sólida e confiável.

ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de segurança da Informação

Estipula melhores práticas para apoiar a implantação do SGSI, com diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Esta norma contém 14 seções de controles de segurança da informação, de um total de 35 objetivos de controles e 114 controles. A parte principal da norma se encontra distribuída nas seguintes seções:

- Seção 5 – Política de Segurança da Informação;
- Seção 6 – Organização da Segurança da Informação;
- Seção 7 – Gestão de ativos;
- Seção 8 – Segurança em recursos humanos;
- Seção 9 – Segurança física e do ambiente;
- Seção 10 – Segurança das operações e comunicações;
- Seção 11 – Controle de acesso;
- Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas;
- Seção 13 – Gestão de incidentes de segurança da informação;
- Seção 14 – Gestão da continuidade do negócio; e
- Seção 15 – Conformidade.

Até a próxima publicação, quando seguiremos apresentando as normas que devem orientar a política de segurança da informação nas entidades!

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Boas Práticas em Segurança da Informação:
Padrões Frameworks e Controles de Segurança da Informação

Estimados colegas, apresentamos mais uma análise, em linhas gerais, das normas ABNT NBR ISO/IEC relevantes na construção de uma política de segurança da informação segura e confiável.

ABNT NBR ISO/IEC 27005:2019. Gestão de riscos de segurança da informação.

Esta norma apresenta diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um SGSI, conforme a NBR ISO/IEC 27001.

As atividades do processo de gestão de riscos de segurança da informação, apresentadas na Seção 6, são detalhadas nas seguintes seções:

- Seção 7 - definição do contexto;
- Seção 8 - processo de avaliação de riscos;
- Seção 9 - tratamento do risco de segurança da informação;
- Seção 10 - aceitação do risco de segurança da informação;
- Seção 11 - comunicação e consulta do risco de segurança da informação; e
- Seção 12 - monitoramento e análise crítica de riscos de segurança da informação.

Os anexos apresentam Informações adicionais para as atividades de gestão de riscos de segurança da informação:

- Anexo A - Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação;
- Anexo B - Identificação e valoração dos ativos e a avaliação do impacto são discutidas;
- Anexo C - Exemplos de ameaças comuns;
- Anexo D - Vulnerabilidades e métodos para avaliação de vulnerabilidades;
- Anexo E - Exemplos de abordagens para o processo de avaliação de riscos de segurança da informação;
- Anexo F - Restrições relativas à modificação do risco; e
- Anexo G - Diferenças nas definições entre a NBR ISO/IEC 27005:2011 e a NBR ISO/IEC 27005:2019.

Até a próxima publicação, quando seguiremos apresentando as normas que devem orientar o processo de elaboração da política de segurança da informação nas entidades!

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Boas Práticas em Segurança da Informação:
Padrões Frameworks e Controles de Segurança da Informação

Olá, pessoal! Concluiremos nesta publicação a abordagem às normas ABNT NBR ISO/IEC mais relevantes na construção de uma política de segurança da informação sólida e confiável.

ABNT NBR ISO/IEC 31000:2018. Gestão de riscos - Diretrizes.

É um documento com recomendações para gerenciar riscos enfrentados pelas organizações, podendo ser personalizado para qualquer contexto. A versão do ano de 2018 apresenta um guia mais claro e conciso, com o intuito de ajudar as organizações a usar os princípios de gerenciamento de risco para melhorar o planejamento e tomar melhores decisões.

ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.

Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Visa a gestão da privacidade no contexto da organização.

Nas próximas publicações, serão apresentados outros documentos/normas importantes na elaboração e execução da política de informação, sobretudo na esfera do governo estadual de Minas Gerais.

Não perca!