POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO - DIRETRIZES Políticas de segurança da informação definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
Requisitos Base
Estratégia do negócio;
Regulamentações, legislação e contratos;
Ambiente de ameaça da segurança da informação, atual e futuro.
Declarações
Definição da segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
Procedimentos para o tratamento dos desvios e exceções.
Documento da política de segurança da informação - TÓPICOS ESPECÍFICOS
Controle de acesso (ver 9);
Classificação e tratamento da informação (ver 8.2);
Segurança física e do ambiente (ver 11);
Tópicos orientados aos usuários finais:
Uso aceitável dos ativos (ver 8.1.3);
Mesa Limpa e Tela Limpa (ver 11.2.9);
Transferência de informações (ver 13.2.1);
Dispositivos móveis e trabalho remoto (ver 6.2);
Restrições sobre o uso e instalação de software (ver 12.6.2);
Backup (ver 12.3);
Transferência da informação (ver 13.2);
Proteção contra códigos maliciosos (ver 12.2);
Gerenciamento de vulnerabilidades técnicas (ver 12.6.1);
Controles criptográficos (ver 10);
Segurança nas comunicações (ver 13);
Proteção e privacidade da informação de identificação pessoal (ver 18.1.4);
Relacionamento na cadeia de suprimento (ver 15).
Analise crítica da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Analise crítica em intervalos planejados ou quando mudanças significativas ocorrerem;
Mapeamento dos incidentes que violam as regras da PSI.

Legenda
TÍTULO;
EXECUTADO;
NÃO EXECUTADO;
EXECUTADO INFORMALMENTE.

ORGANIZANDO DA SEGURANÇA DA INFORMAÇÃO Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.
Responsabilidades e papéis pela segurança da informação
O gestor responsável por cada ativo ou processo de segurança da informação tenha atribuições definidas e os detalhes dessa responsabilidade sejam documentados; PROPRIETÁRIO DOS SISTEMAS
Os níveis de autorização sejam claramente definidos e documentados;
Aprove as atribuições de tarefas e responsabilidades específicas para a segurança da informação por toda a organização;
Inicie planos e programas para manter a conscientização da segurança da informação;
Assegure que a implementação dos controles de segurança da informação tem uma coordenação.
Segurança da informação no gerenciamento de projetos
Os objetivos de segurança da informação sejam contemplados nos objetivos do projeto;
Uma avaliação dos riscos de segurança da informação seja conduzida em estágios iniciais do projeto para identificar os controles que são necessários;
A segurança da informação seja parte integrante de todas as fases da metodologia do projeto.
Política para o uso de dispositivo móvel
Registros dos dispositivos móveis;
Restrições quanto à instalação de softwares;
Requisitos para as versões dos softwares e aplicações de patches;
Controle de acesso;
Técnicas criptográficas;
Proteção contra códigos maliciosos;
Uso dos serviços web e aplicações web.

Legenda
TÍTULO;
EXECUTADO;
NÃO EXECUTADO;
EXECUTADO INFORMALMENTE.

9. CONTROLE DE ACESSO
9.1 REQUISITOS DO NEGÓCIO PARA CONTROLE DE ACESSO Limitar o acesso à informação e aos recursos de processamento da informação.
Política de controle de acesso
Política para disseminação e autorização da informação, por exemplo, o princípio "necessidade de conhecer" e níveis de segurança e a classificação das informações (ver 8.2);
Gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis;
Segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;
Procedimento para autorização formal de pedidos de acesso (ver 9.2.1);
Análise periódica de direitos de acesso (ver 9.2.5);
Remoção de direitos de acesso por mudança de lotação ou exoneração (ver 9.2.6);
Arquivo dos registros de todos os eventos significantes, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta;
Regras para o acesso privilegiado (ver 9.2.3).
9.1.2 Política de Acesso às redes e aos serviços de rede
Discriminar redes e serviços de redes que são permitidos de serem acessados;
Procedimentos de autorização para determinar quem tem permissão para acessar quais redes e serviços de redes;
Procedimentos e controles de gerenciamento para proteger o acesso a conexões e serviços de redes;
Requisitos de autenticação do usuário para acessar vários serviços de rede;
Monitoramento do uso dos serviços de rede.
9.2 GERENCIAMENTO DE ACESSO DO USUÁRIO Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.
9.2.1 Registro e cancelamento de usuário
O uso de um ID de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações; o uso compartilhado de ID de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e convém que seja aprovado e documentado;
A imediata remoção ou desabilitação do ID de usuário que tenha deixado a organização, seja servidor ou estagiário (ver 9.2.5);
Identificação e remoção, de forma periódica, ou a desabilitação de usuários redundantes com ID diferentes, casos de servidores que ascenderam de nível;
9.2.3 Gerenciamento de direitos de acesso privilegiados
Mapeamento dos direitos de acesso privilegiados, associados a cada sistema ou processo, por exemplo, sistema operacional, sistemas de gerenciamento de banco de dados e cada aplicação, e de categorias de usuários para os quais estes necessitam ser concedido;
Os direitos de acesso privilegiado sejam concedidos a usuários conforme a necessidade de uso e com base em eventos alinhados com a política de controle de acesso (ver 9.1.1), baseado nos requisitos mínimos para sua função;
Os direitos de acesso privilegiados sejam atribuídos a um ID de usuário diferente daqueles usados nas atividades normais do negócio. As atividades normais do negócio não sejam desempenhadas usando contas privilegiadas;
Direitos de acesso privilegiado devem ser analisados criticamente a intervalos regulares, para verificar se eles estão alinhados com as suas obrigações;
Procedimentos específicos sejam estabelecidos e mantidos para evitar o uso não autorizado de ID de usuário de administrador genérico, de acordo com as capacidades de configuração dos sistemas;
Para o ID de usuário de administrador genérico, a confidencialidade da informação de autenticação secreta seja mantida quando for compartilhada (por exemplo, mudanças de senhas com frequência e tão logo quanto possível, quando um usuário privilegiado deixa a organização ou muda de função, comunicação entre os usuários privilegiados por meio de mecanismos apropriados).
9.2.4 Gerenciamento da informação de autenticação secreta de usuários
Solicitar aos usuários a assinatura de uma declaração, para manter a confidencialidade da informação de autenticação secreta e manter as senhas de grupos de trabalho, exclusivamente com os membros do grupo; esta declaração assinada pode ser incluída nos termos e condições da contratação (ver 7.1.2);
Garantir, onde os usuários necessitam manter suas próprias informações de autenticação secreta, que lhes sejam fornecidas uma informação de autenticação secreta temporária, as quais o usuário é obrigado a alterá-la no primeiro uso;
Informação de autenticação secreta temporária seja única para uma pessoa e que não seja fácil de ser adivinhada;
9.2.5 Análise crítica dos direitos de acesso de usuário **Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.**
Os direitos de acesso de usuários sejam revisados em intervalos regulares e depois de quaisquer mudanças, como promoção, remanejamento ou exoneração(ver 7);
Autorizações para direitos de acesso privilegiado especial sejam revisadas em intervalos mais frequentes;
As alocações de privilégios sejam verificadas em intervalo de tempo regular para garantir que privilégios não autorizados não foram obtidos.
9.3 RESPONSABILIDADES DOS USUÁRIOS Tornar os usuários responsáveis pela proteção das suas informações de autenticação.
9.3.1 Uso da informação de autenticação secreta
Manter a confidencialidade da informação de autenticação secreta, garantindo que ela não é divulgada para quaisquer outras partes, incluindo autoridades e lideranças;
Disseminar a necessidade de evitar manter anotadas as informações de autenticação secreta (por exemplo, papel, arquivos ou dispositivos móveis);
Alterar a informação de autenticação secreta, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;

Legenda
TÍTULO;
EXECUTADO;
NÃO EXECUTADO;
EXECUTADO INFORMALMENTE.

Quando as senhas são usadas como informação de autenticação secreta, selecione senhas de qualidade com um tamanho mínimo que sejam: 1)fáceis de lembrar; 2)não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário; 3)não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário); 4)isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos; 5)caso a senha seja temporária, ela deve ser mudada no primeiro acesso (log-on)

Não compartilhar a informação de autenticação secreta de usuários individuais;

Garantir adequada proteção de senhas quando as senhas são usadas como informação de autenticação secreta em procedimentos automáticos de acesso (log-on) e são armazenadas;

11 SEGURANÇA FÍSICA E DO AMBIENTE

11.1 ÁREAS SEGURAS

Objetivo: Prevenir o acesso fisico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

11.1.1 Perimetro de segurança física

Perímetros de segurança claramente definidos e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro;

Perímetros de um edifício ou de um local que contenha as instalações de processamento da informação sejam fisicamente sólidos (ou seja, o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão); as paredes externas do local devem ser de construção robusta e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle, por exemplo, barras, alarmes, fechaduras etc.; as portas e janelas sejam trancadas quando estiverem sem monitoração, e que uma proteção externa para as janelas seja considerada, principalmente para as que estiverem situadas no andar térreo;

Uma área de recepção, ou outro meio para controlar o acesso físico ao local ou ao edifício; o acesso aos locais ou edifícios deve ficar restrito somente ao pessoal autorizado;

Barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado;

Instalações de processamento da informação gerenciadas pela organização fiquem fisicamente separadas daquelas que são gerenciadas por partes externas.

11.1.2 Controles de entrada física

A data e hora da entrada e saída de visitantes registradas, e todos os visitantes sejam supervisionados; as permissões de acesso só devem concedidas para finalidades específicas e autorizadas; A identidade dos visitantes seja autenticada por meios apropriados;

Convém que o acesso às áreas em que são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado pela implementação de controles de acesso apropriados, por exemplo, mecanismos de autenticação de dois fatores, como, cartões de controle de acesso e PIN (personal identification number);

Uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acessos e mantidos e monitorados de forma segura;

Às partes externas que realizam serviços de suporte, seja concedido acesso restrito às áreas seguras ou as instalações de processamento da informação sensíveis, somente quando necessário; este acesso deve ser autorizado e monitorado;

Os direitos de acesso a áreas seguras devem ser revistos e atualizados em intervalos regulares, e revogados quando necessário (ver 9.2.4 e 9.2.5).

11.1.3 Segurança em escritórios, salas e instalações

Instalações devem ser localizadas de maneira a evitar o acesso do público;

A identificação e localização das instalações que processam informações sensíveis, não devem ficar facilmente acessíveis a qualquer pessoal não autorizada.

11.1.4 Proteção contra ameaças externas e do meio-ambiente

Áreas que processam informações sensíveis devem evitar danos oriundos de fogo, inundação, terremoto, explosão, manifestações civis e outras formas de desastre natural ou provocado pela natureza.

11.1.5 Trabalhando em áreas seguras

O pessoal só tenha conhecimento da existência de áreas seguras ou das atividades nelas realizadas, apenas se for necessário;

Seja evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal intencionadas;

As áreas seguras, não ocupadas, sejam fisicamente trancadas;

Não seja permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.

11.1.6 Áreas de entrega e de carregamento

O acesso a uma área de entrega e carregamento a partir do exterior do prédio fique restrito ao pessoal identificado e autorizado;

As áreas de entrega e carregamento devem projetadas de tal maneira que seja possível carregar e descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício;

Os materiais entregues sejam inspecionados e examinados para detectar a presença de explosivos, materiais químicos ou outros materiais perigosos, antes de serem transportados da área de entrega e carregamento para o local de utilização;

11.2 EQUIPAMENTOS

Objetivo: Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.

11.2.1 Escolha do local e proteção do equipamento

As instalações de armazenagem devem ser protegidas de forma segura para evitar acesso não autorizado;

Diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação;

As condições ambientais, como temperatura e umidade, devem monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação;

11.2.2 Utilidades

Estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade;

Seja avaliado regularmente quanto á sua capacidade para atender ao crescimento do negócio e ás interações com outras utilidades;

Sejam inspecionadas e testadas regularmente para assegurar o seu adequado funcionamento;

Seja alarmada para detectar mal funcionamento, quando necessário;

Tenham múltiplas alimentações com rotas físicas diferentes.

11.2.3 Segurança do cabeamento

As linhas de energia e de telecomunicações que entram nas instalações de processamento da informação devem ser subterrâneas (ou fiquem abaixo do piso) sempre que possível, ou recebam uma proteção alternativa adequada;

Os cabos de energia sejam segregados dos cabos de comunicações, para evitar interferências;

Para sistemas sensíveis ou críticos, convém que os seguintes controles adicionais, sejam considerados: 1)instalação de condultes blindados e salas ou caixas trancadas em pontos de inspeção e pontos terminais;2)utilização de blindagem eletromagnética para a proteção dos cabos;3)realização de varreduras técnicas e inspeções físicas para detectar a presença de dispositivos não autorizados conectados aos cabos;4)acesso controlado aos painéis de conexões e ás salas de cabos.

11.2.4 Manutenção dos equipamentos

A manutenção dos equipamentos é realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

A manutenção e os consertos dos equipamentos só sejam realizados por pessoal de manutenção autorizado;

Registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas;

Convém que sejam implementados controles apropriados, na época programada para a manutenção do equipamento, dependendo da manutenção ser realizada pelo pessoal local ou por pessoal externo à organização; onde necessário, informações sensíveis sejam eliminadas do equipamento, ou o pessoal de manutenção seja de absoluta confiança;

Atendimento a todas as exigências de manutenção estabelecidas nas garantias;

Antes de colocar o equipamento em operação, após a sua manutenção, convém que ele seja inspecionado para garantir que o equipamento não foi alterado indevidamente e que não está em mau funcionamento.

11.2.5 Remoção de ativos

Identificação de servidores, fornecedores e partes externas que tenham autorização para permitir a remoção de ativos para fora do local;

Estabelecimento de limites de tempo para a retirada de equipamentos do local, e a devolução seja controlado;

É recomendado que fosse feito um registro da retirada e da devolução de ativos, quando do seu retorno;

11.2.6 Segurança de equipamentos e ativos fora das dependências da organização

Os equipamentos e mídias removidos das dependências da organização não fiquem sem supervisão em lugares públicos;

Os controles para as localidades fora das dependências da organização, como, o trabalho em casa e localidades remotas e temporárias, sejam determinados por uma avaliação de riscos, devendo ser aplicados controles adequados para cada caso, por exemplo, arquivos trancáveis, política de "mesa limpa", controles de acesso a computadores, e comunicação segura com o escritório (ver também ISO/IEC 27033);

Quando o equipamento fora das dependências da organização é transferido entre diferentes pessoas ou partes externas, convém que seja mantido um registro para definir a cadeia de custodia do equipamento, incluindo pelo menos os nomes e organizações daqueles que são responsáveis pelo equipamento.

11.2.7 Reutilização e alienação segura de equipamentos (descarte ou reutilização)

O processo de encriptação é suficientemente robusto e cobre o disco por completo (incluindo slack space, swap files, etc)

As chaves criptográficas são de um tamanho considerável para resistir um ataque de força bruta;

As chaves criptográficas são guardadas de forma confidencial (por exemplo, nunca armazenada no mesmo disco).

11.2.8 Equipamento de usuário sem monitoração

Encerrar as sessões ativas, a menos que elas possam ser protegidas por meio de um mecanismo de bloqueio, por exemplo tela de proteção com senha;

Efetuar a desconexão de serviços de rede ou aplicações, quando não for mais necessário;

Proteger os computadores ou dispositivos móveis contra uso não autorizado através de tecla de bloqueio ou outro controle equivalente, por exemplo, senha de acesso, quando não estiver em uso.

11.2.9 Política de mesa limpa e tela limpa

As informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, são guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado;

Os computadores e terminais são mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados;

Legenda
TÍTULO;
EXECUTADO;
NÃO EXECUTADO;
EXECUTADO INFORMALMENTE.

12 SEGURANÇA NAS OPERAÇÕES

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

12.1.2 Gestão de mudanças

Identificação e registro das mudanças significativas;

Planejamento e testes das mudanças;

Avaliação de impactos potenciais, incluindo impactos de segurança da informação, de tais mudanças;

Procedimento formal de aprovação das mudanças propostas;

Verificação de que os requisitos de segurança da informação foram atendidos;

Legenda
TÍTULO;
EXECUTADO;
NÃO EXECUTADO;
EXECUTADO INFORMALMENTE.

Comunicação dos detalhes das mudanças para todas as pessoas relevantes;
Procedimentos de recuperação, incluindo procedimentos e responsabilidades para interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.
Provisão de um processo emergencial de mudança para permitir uma implementação rápida e controlada de mudanças, necessárias para resolver um incidente (ver 16.1).