7COMm

People and tech to transform

Política de Segurança da Informação Coorporativa

2021

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CORPORATIVA

Proprietário: Grupo 7COMm	Aprovado por: Comitê de Segurança da Informação
Última data de aprovação: 09/05/2022	

Sumário

1. OBJETIVO 3
2. DESTINATÁRIOS 4
3. RESPONSABILIDADES 4
4. DIRETRIZES 6
5. SANÇÕES 19
6. GLOSSÁRIO TÉCNICO 20

1. OBJETIVO

Política de Segurança da Informação do Grupo 7COMm objetiva estabelecer os **princípios** e **diretrizes** de Segurança da Informação visando garantir a **confidencialidade**, **integridade** e **disponibilidade das informações**, dos ativos, sistemas e recursos de processamento associados com as informações de sua propriedade e/ou sob sua guarda, sendo o seu cumprimento obrigatório **por todos** que utilizam as informações, recursos e/ou demais ativos tangíveis ou intangíveis da empresa.

Estabelece **regras**, **padrões** e **melhores práticas** para garantir a proteção das **informações disponibilizadas para o desempenho das atividades profissionais** e o cumprimento das legislações e regulamentações **vigentes**.

Certificar-se de que o Grupo 7COMm tenha padrões, procedimentos e controles adequados de Segurança da Informação em vigor para mitigar o risco de Segurança da Informação e garantir o cumprimento de todas as legislações, regulamentos e normas relevantes de Proteção de Dados e Privacidade.

2. DESTINATÁRIOS

Esta política se aplica a todos os diretores, administradores, funcionários, estagiários, aprendizes, colaboradores e visitantes do Grupo 7COMm e terceiros envolvidos, que atuam em nome do Grupo 7COMm, como por exemplo prestadores de serviços, revendas e parceiros comerciais que possuam acesso à rede ou utilizem o ambiente de processamento do Grupo 7COMm e de seus clientes

Aplica-se também a todos os ativos de informações e equipamentos de informática, de propriedade do Grupo 7COMm ou não, e que contenham informações pertinentes ao negócio da instituição.

3. RESPONSABILIDADES

3.1 Diretoria Executiva e Presidência

3.1.1 Analisar e apoiar os projetos de Segurança da Informação ajudando a manter o desenvolvimento da área sempre aliada a continuidade aos negócios e interesses estratégicos do Grupo 7COMm.

3.1.2 Aprovar, observar e fazer cumprir esta PSI que contempla os princípios básicos, diretrizes e responsabilidades do processo de segurança da informação.

3.1.3 Garantir a implementação desta Política, zelando pela observância de seus princípios e diretrizes em todas as suas decisões.

3.2 Gestores e Líderes de Área

3.2.1 Conhecer, observar e fazer cumprir as normas da PSI bem como suas boas práticas, procedimentos envolvidos e orientar os liderados no dia a dia de trabalho.

3.2.2 Informar aos responsáveis pela Tecnologia da Informação e ou Segurança da informação por e-mail, canais de denúncia ou pessoalmente sobre todo e qualquer evento, comportamento ou incidente que comprometa a segurança da informação.

3.3 Setor de Tecnologia da Informação

3.3.1 O Setor de Tecnologia da informação está subordinada à Governança de TI.

3.3.2 Programar, executar e guardar esta política atuando nos seus desdobramentos e na divulgação permanente e sistemática do seu conteúdo às partes interessadas.

3.3.3 Revisar e atualizar anualmente a política de segurança, adequando a realidade tecnológica.

3.3.4 Registrar e tratar incidentes de segurança e alterações no ambiente através dos recursos computacionais disponíveis obedecendo aos procedimentos operacionais vigentes.

3.4 Quadro Corporativo

3.4.1 Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação bem como as demais normas e procedimentos de segurança aplicáveis.

3.4.2 Comunicar à Gerência de Tecnologia da Informação qualquer evento que viole esta política ou possa colocar em risco a segurança das informações ou dos recursos computacionais do Grupo 7COMm.

3.4.3 Compreender o papel da segurança da informação em suas atividades diárias e participar dos programas de conscientização.

3.5 Prestadores de Serviços, Revendas, Parceiros Comerciais e Visitantes

3.5.1 Entender, respeitar e seguir a PSI disponibilizada pelo Grupo 7COMm a partir do momento que possuir acesso à rede ou utilizar o ambiente de processamento do Grupo 7COMm e de seus clientes.

4. DIRETRIZES

4.1. Acesso à Rede Corporativa

Grupo 7COMm fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa.

4.1.1. Fica estabelecido que a **norma de gestão de acessos IAM, NOR SEG 001/21** é complementar a esta política por possuir um detalhamento do processo.

4.1.2. Toda conta de acesso é pessoal do usuário a qual foi delegada e intransferível.

4.1.3. O usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.

4.1.4. Para garantir a segurança das informações, o Grupo 7COMm pratica o bloqueio de acessos às contas de rede e e-mail nas seguintes situações: solicitações emergenciais, ataques ou risco cibernético e desligamento

4.1.5. É proibido o uso de notebooks, computadores, tablets que sejam particulares na rede corporativa que não estejam seguindo as normas do BYOD (*Bring Your Own Device*).

4.1.6. Equipamentos pessoais de visitantes, fornecedores e prestadores de serviço deverão se conectar à rede de visitantes (WIFI – Guest).

4.1.7. É proibida a instalação de qualquer equipamento na rede sem a devida autorização da gerência de tecnologia da informação.

4.1.8. Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo Grupo 7COMm

4.2 Senhas De Acesso

Toda senha de acesso **é pessoal do usuário** a qual foi delegada e intransferível. Desta forma, o **usuário é integralmente responsável por sua utilização**, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua senha de acesso.

Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

4.2.1 As senhas possuem validade de 90 (noventa) dias. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha.

4.2.1 As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 8 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais; a nova senha não poderá ser igual a qualquer uma das últimas 10 senhas utilizadas.

4.2.2 Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo por, no mínimo, 30 (trinta) minutos;

4.2.3 Ao ingressar no quadro corporativo do Grupo 7COMm, todos usuários e usuários terceiros recebem um "usuário" e "senha temporária" para iniciar suas atividades. A senha temporária deve ser alterada no primeiro acesso sendo composta dentro dos padrões mencionados nesta política.

4.2.4 Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pela área responsável pela Segurança da Informação e aplicação das sanções e punições previstas na Política de Segurança da Informação, conforme a gravidade da violação. Caso a conta do colaborador seja envolvida em um possível incidente a conta poderá ser bloqueada de imediato.

4.2.5 **Recomendações de Senha de Acesso:** na criação de uma nova senha, usuários devem estar atentos às seguintes recomendações:

4.2.5.1 Não utilizar nenhuma parte de sua credencial na composição da senha;

4.2.5.2 Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil

obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;

4.2.5.3 Não utilizar repetição ou sequência de caracteres, números ou letras;

4.2.5.4 Qualquer parte ou variação do nome do Grupo 7COMm;

4.2.5.5 Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

4.3 Uso de Arquivos, Diretórios e Armazenamento de Dados

4.3.1 Todas as solicitações de acesso aos dados devem ser processadas de acordo com o procedimento de gestão e acesso vigente do Grupo 7COMm e prazos especificados pela legislação pertinente.

4.3.2 Nesta política são abordadas regras básicas para o uso protegido e adequado dos dados do Grupo 7COMm, detalhamentos e regras mais técnicas e específicas serão tratadas na norma de gestão da informação.

4.3.3 As concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso tendo cada qual acesso somente às informações que sejam necessárias ao desenvolvimento de suas atividades profissionais.

4.3.4 O gestor de cada sistema/ plataforma é quem deve autorizar o acesso aos dados, além de realizar revisões periodicamente.

4.3.5 Caso a TI identifique risco de segurança da informação, ela pode questionar a solicitação de acesso e propor sugestão de alteração.

4.3.6 A Segurança da Informação poderá auditar em qualquer tempo os acessos às informações e seu devido uso, aplicar sanções cabíveis de Nível 1, orientar e realizar correção necessárias para estar compliance as normas da política de segurança da informação vigente. Caso ocorra alguma infração as gerências dos envolvidos devem ser informadas via e-mail.

4.3.7 Sempre que houver a necessidade de transferir um usuário ou usuário terceiro para outro departamento ou função e houver necessidade de revisão dos acessos existentes, o antigo gestor deve registrar chamado para bloquear os acessos concedidos anteriormente.

4.3.8 Os dados de propriedade do Grupo 7COMm, ou não, devem ser

armazenados exclusivamente em seus servidores e plataforma corporativa em nuvem e nos servidores de arquivo. Dados impressos devem estar devidamente arquivados em locais seguros.

4.3.9 O acesso aos arquivos e diretórios é realizado através de compartilhamento na rede respeitando as normas de gestão de acesso por perfil através das contas de rede, entretanto é responsabilidade dos gestores de área a abertura de chamado junto a TI para solicitação, revisão e revogação de acessos.

4.3.10 É proibido o uso de mídias externas tais como: Pendrives, HDs Externos e CDs para cópias particulares dos dados de trabalho.

4.3.11 O sigilo das informações é responsabilidade de todos os destinatários, sendo proibida a utilização não autorizada de informações do Grupo 7COMm.

4.3.12 A confidencialidade e privacidade das informações deve ser prioritária conforme orientado na política de sigilo e privacidade referenciada no item 4.5 deste documento.

4.4 Gestão de Ativos

Esta política visa estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação do Grupo 7COMm, por seus usuários autorizados.

Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade do Grupo 7COMm:

4.4.1 O Grupo 7COMm fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais.

Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade do Grupo 7COMm, sendo expressamente proibida a utilização para fins particulares;

4.4.2 A alteração e/ou a manutenção de qualquer equipamento de propriedade do Grupo 7COMm é uma atribuição específica do departamento de infraestrutura interna do Grupo 7COMm que, a seu exclusivo critério, poderá delegar formalmente a outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;

4.4.3 Os equipamentos do Grupo 7COMm devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado.

4.4.4 Computadores de mesa (desktops) ou móveis (notebooks) devem ser bloqueados no final do expediente ou sempre que o usuário se ausentar.

4.4.5 Para a liberação ou empréstimo de ativos do Grupo 7COMm é necessário a assinatura do Contrato de Comodato de Equipamento - Notebook e Periféricos e/ou Termo de Recebimento e Responsabilidade – Notebook e Periféricos, sendo que esta ocorrerá somente após a assinaturas dos documentos.

4.4.6 Ao final da prestação de serviços e/ou vínculo contratual, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com o Grupo 7COMm.

4.4.7 A seu critério exclusivo o Grupo 7COMm poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, que deverão passar por avaliação técnica pelo departamento de tecnologia da informação garantindo que o mesmo esteja dentro dos padrões mínimos de segurança.

4.4.8 Não é permitido conectar à rede do Grupo 7COMm dispositivos de rede, Wi-fi ou telefonia sem a autorização do setor de tecnologia da informação. Esses equipamentos por medida de segurança possuem uma instalação padronizada e o descumprimento desta norma é considerado grave.

4.4.9 O Grupo 7COMm poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser cumpridas as diretrizes conforme norma geral de armazenamentos de dados.

4.4.10 Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pelo Grupo 7COMm.

4.4.11 O Grupo 7COMm poderá, a seu critério exclusivo, fornecer certificados digitais para usuários que executam atividades profissionais específicas, sendo cada receptor responsável pelo uso devido e aceitável devendo ser observadas as diretrizes da norma de identificação digital.

4.4.12 Uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser

feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse do Grupo 7COMm ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

4.4.13 Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais do Grupo 7COMm, o usuário responsável deverá informar imediatamente o ocorrido ao departamento de tecnologia da informação.

4.5 Privacidade e Confidencialidade das Informações

4.5.1 Todos os colaboradores que tenham acesso a informações do Grupo 7COMm ou sob guarda da empresa - estratégias, pessoais, sensíveis ou não - não poderão utilizá-las para fins pessoais ou divulgá-las a pessoas não autorizadas. As restrições incluem a utilização de dados em palestras, apresentações, publicações ou qualquer outra divulgação ao público externo sem aprovação prévia da diretoria da empresa.

4.5.2 Para garantir a integridade e confiabilidade dos dados, o Grupo 7COMm conta com o uso de tecnologias de virtualização integrada a armazenamento em nuvem mantendo seu ambiente seguro em casos de desastres.

4.5.3 O Grupo 7COMm realiza o tratamento de dados pessoais com finalidades específicas e de acordo com as bases legais previstas na LGPD.

4.5.4 Dados pessoais são informações relacionadas a um indivíduo vivo que é ou pode ser identificado a partir dos dados ou dos dados em conjunto com outras informações que estão ou provavelmente estarão em posse do Grupo 7COMm. Todos os destinatários desta Política que realizem o tratamento de dados devem estar cientes e seguir as diretrizes da Política de Privacidade do Grupo 7COMm, zelando pela confidencialidade e privacidade de dados conforme legislação vigente.

4.6 Backup e Restore

4.6.1 Para garantir a integridade e confiabilidade dos dados, o Grupo 7COMm conta com o uso de tecnologias de virtualização integrada a armazenamento em nuvem mantendo seu ambiente seguro em casos de desastres.

4.6.2 O setor de tecnologia da informação realiza periodicamente teste de restore a fim de garantir a disponibilidade em casos de desastre. Os detalhes técnicos estão detalhados na norma de gestão de backup que complementa esta política.

4.6.3 Restores poderão ser solicitados via chamado e terão seu SLA seguido conforme política de gestão de serviços.

4.6.4 A Política de Backup não contempla a cópia de segurança de informações armazenadas em estações de trabalho (Desktop/Notebook), portanto é necessário que os usuários armazenem informações apenas nos servidores ou em recursos ofertados pelo Grupo 7COMm.

4.7 Acesso Remoto

O Grupo 7COMm fornece aos usuários e usuários terceiros que prestam serviços à distância acesso VPN, para garantir conexão segura à sua rede corporativa.

4.7.1 Somente equipamentos validados e configurados pela equipe de TI, podem ter acesso a VPN.

4.7.2 Somente a equipe de Infraestrutura interno do Grupo 7COMm é autorizada a realizar acessos remotos em desktops, notebooks, dispositivos e servidores para fins de manutenção e monitoramento. Caso ocorra alguma necessidade, o gestor do colaborador deve abrir um chamado estando sujeito aos prazos de SLA de atendimento.

4.7.3 O acesso remoto de usuário e usuário terceiro a ativos/serviços de informação ou recursos computacionais do Grupo 7COMm somente poderá ser concedido após a efetivação do acordo de confidencialidade entre as partes e deve ser monitorado pela Infraestrutura interna do Grupo 7COMm. A concessão do acesso deverá ser limitada ao tempo necessário estimado a atividade do terceiro ou prestador de serviço. Serão concedidos acessos de privilégios mínimos para a execução das atividades.

4.7.4 O usuário terceiro, bem como a empresa onde ele trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credenciais de acesso remoto.

4.7.5 Durante o monitoramento do acesso remoto a seus ativos/serviços de informação ou recursos computacionais, o Grupo 7COMm se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, gravar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

4.8 Controle de Acesso Físico

O acesso ao ambiente controlado deverá ser realizado por meio de credencial única, pessoal, identificável e não poderá ser cedida a outra pessoa;

Este tópico visa formalizar as diretrizes de acesso físico ao Data Center do Grupo 7COMm. O controle de acesso às demais dependências, será feito de acordo com a especificidade de cada área a ser visitada, onde serão observados os critérios estabelecidos pelos responsáveis das mesmas.

As seguintes diretrizes para ambientes de acesso controlado devem ser cumpridas:

4.8.1 O acesso ao Data Center é permitido somente a equipe de Infraestrutura de TI, Segurança da Informação ou outras pessoas supervisionadas.

4.8.2 Em auditorias internas ou externas, os auditores devem entrar no Data Center sempre acompanhados por pelo menos um membro da equipe do Grupo 7COMm.

4.8.3 Em caso de serviços de terceiros a serem realizados dentro do Data Center é necessário o acompanhamento e aprovação da área de TI e Segurança da Informação.

4.8.4 Todo acesso ao Data Center deve ser registrado em sistema próprio de controle de acesso e será permitido através do uso de cartão de aproximação.

4.8.5 Os registros de acesso ao Data Center devem ser armazenados em local seguro e devem ser mantidos em histórico por pelo menos 1 (um) ano.

4.8.6 Em ambientes de acesso controlado é proibida a utilização de câmeras

fotográficas, sejam elas acopladas ao smartphone ou não, salvo em situações inerentes à rotina de trabalho e/ou sob autorização da TI.

4.9 Quanto ao Uso Aceitável da Internet Corporativa

Este visa formalizar as diretrizes gerais de utilização da Internet, E-mail, Redes Sociais e ferramentas de mensagens instantâneas nas dependências do Grupo 7COMm.

4.9.1 A Internet deve ser utilizada pelos usuários e usuários terceiro, para as atividades relacionadas ao trabalho e disponibilizada conforme necessidade correspondente ao perfil funcional de cada usuário, com o objetivo de atender as necessidades das respectivas áreas;

4.9.2 Nos casos em que se fizer necessário o acesso para outros fins, a internet poderá ser disponibilizada com a devida autorização do gestor imediato, sendo este acesso controlado e monitorado;

4.9.3 O acesso à internet de pessoas sem vínculo o Grupo 7COMm, poderá ser disponibilizado em ambiente tecnológico separado (rede de visitantes), controlado e monitorado, quer seja em meio móvel (wi-fi) ou fixo;

4.9.4 A concessão de acesso à rede de visitantes deve estar associada à conscientização das regras internas de uso da rede.

4.9.5 O Grupo 7COMm busca priorizar a conformidade com as leis vigentes, para garantir o cumprimento o Grupo 7COMm adota algumas medidas de monitoramento e bloqueio agindo preventivamente melhorando a segurança alinhando seus objetivos de negócio;

Os seguintes itens são passíveis de monitoramento, bloqueio e penalidade se realizados com os ativos do Grupo 7COMm:

1. Navegação excessiva em sites que não sejam estratégicos aos negócios do Grupo 7COMm
2. Navegação em sites que permitam ou estimulem downloads e ou distribuição de sites piratas,
3. Navegação em sites impróprios.
4. Navegação em sites que promovam jogos de azar.
5. Divulgação ou propagação de difamação, preconceito ou atitude fraudulenta.

4.9.6 O acesso a redes sociais (ex.: facebook, linkedin, etc.) ou a sites que

possuem áudio e/ou vídeo (ex: rádios, TV's online, youtube, etc.) são controlados e disponibilizado apenas para áreas que precisam utilizar esses recursos nas suas atividades de trabalho. As solicitações de liberação desses sites devem ser realizadas através de abertura de chamado, o qual deve ser autorizado pelo gestor imediato e arquivado para fins de auditoria;

4.9.7 Softwares com as características peer-to-peer (P2P), tais como Emule, Kazaa, Morpheus, Torrent e afins, não são permitidos, assim devem ser restringidos pela área técnica de Segurança da Informação e os acessos dos usuários monitorados, com objetivo de garantir segurança e a correta utilização da internet;

4.9.8 É proibido fornecer ou divulgar na internet (sites de inscrições, grupos de discussão, redes sociais, entre outros) informações do Grupo 7COMm que sejam classificadas como interna, reservada ou confidencial.

4.9.9 Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet de dentro da empresa poderá ser auditada sem aviso prévio. O Grupo 7COMm reserva o direito de monitorar e realizar auditorias constantes de acesso a sites visitados pelos usuários e usuários terceiros dentro das conformidades legais.

4.9.10 Os destinatários desta PSI responderão por quaisquer atos ou infrações causadas por imprudência ou imperícia que possam comprometer a segurança da informação por meio do uso da internet.

4.10 Uso Do E-mail Corporativo

O Grupo 7COMm fornece o serviço de e-mail exclusivamente para o desempenho de suas atividades profissionais para usuários e usuários terceiros autorizados;

4.10.1 Não é permitido para fins de trabalho, o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pelo Grupo 7COMm;

4.10.2 Não é permitido utilizar-se do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do Grupo 7COMm;

4.10.3 Não é permitido enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo do Grupo 7COMm, excetuando-se quando expressamente autorizado;

4.10.4 Durante o monitoramento o Grupo 7COMm se resguarda o direito de, sem qualquer notificação ou aviso, monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de e-mail sem aviso prévio;

4.11 Mensageria

4.11.1 O Grupo 7COMm disponibiliza o Microsoft Teams para toda a sua organização e adota esta aplicação como padrão. É expressamente proibido utilizar outro serviço de mensageria que não o padrão do Grupo 7COMm para comunicação ou compartilhamento de dados. Exceto quando por solicitação expressa de um cliente;

4.12 Desenvolvimento Seguro

Estas diretrizes tem o objetivo de garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação, estabelecendo as diretrizes e requisitos para desenvolvimento e manutenção dos sistemas de informação, fornecendo normativas para desenvolvimento seguro de software no âmbito Grupo 7COMm.

Quanto ao armazenamento de dados não se deve utilizar meio de armazenamento que não possua acesso para leitura e escrita restrito por senha, além disso, deve-se preferencialmente, armazená-los criptografados.

4.12.1 Quanto ao acesso ao banco de dados:

1. Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões de root.
2. Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões para execução de comandos em Data Definition Language (DDL).
3. Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões além das estritamente necessárias ao seu funcionamento.
4. As regras acima podem ser alteradas de acordo com as necessidades de cada cliente e devem ser devidamente justificadas.

4.12.2 Quanto ao uso de senhas:

1. Não se deve permitir a elaboração de senhas que não sigam os padrões estabelecidos nas normas de gestão de acesso do Grupo 7COMm.
2. Não se deve utilizar o armazenamento de senhas em código-fonte.
3. Os ambientes de homologação e produção não poderão ter as mesmas senhas que os ambientes de desenvolvimento e testes.

4.12.3 Quanto à autorização e autenticação de usuários

1. Não se deve armazenar senhas em texto plano sem utilizar um algoritmo de hash seguro e salt.
2. Deve-se utilizar autenticação via AD ou LDAP sempre que possível.

4.12.4 Autenticação em Sistemas Web:

1. Sendo o HTTP um protocolo stateless, que utiliza cookies para manter sessões de usuário, faz-se necessário garantir tanto a segurança da troca de credenciais quanto a segurança das demais páginas acessadas pelos usuários dos sistemas web. O protocolo HTTPS visa contribuir para que essa segurança seja garantida.
2. Dessa forma deve-se utilizar HTTPS em todas as telas dos sistemas.

4.12.5 Ataques e Defesa:

1. Deve-se prevenir ataques de injeção de SQL (SQL Injection).
2. Não se deve criar SQLs concatenando parâmetros textuais de origem não-segura, como parâmetros preenchidos pelo usuário ou mesmo armazenados no banco de dados.
3. Deve-se restringir as permissões de acesso ao banco de dados para o usuário da aplicação.
4. Deve-se, sempre que possível, passar parâmetros em comandos SQL (DML ou DDL) utilizando prepared statements. Consultas que não podem ser parametrizadas devem receber tratamento especial, como escapes ou codificação em hexadecimal.
5. Deve-se prevenir ataques de injeção de HTML e Javascript.
6. Deve-se prevenir ataques do tipo cross-site scripting (XSS).
7. Deve-se prevenir ataques de quebra de autenticação e gerenciamento de sessão (Broken Authentication and Session Management).
8. Deve-se submeter os sistemas da área de Produtos a ferramentas de testes de invasão.

4.12.6 Quanto aos testes

1. Deve-se realizar testes de segurança em cada versão do software que modifique sua estrutura (telas de login, serviços não autenticados, novos formulários com interação com o usuário, etc.) quando aplicável a ser definido pelo responsável técnico da aplicação.
2. Deve-se garantir, através de testes automatizados, que os serviços e dados sigilosos estejam protegidos e disponíveis apenas para os usuários detentores das informações.
3. Deve-se elaborar uma política de testes, automatizados ou não, visando a garantia de não vulnerabilidade aos principais ataques conhecidos em sistemas.
4. Deve-se definir cenários de testes voltados à garantia dos requisitos não funcionais do software, preferencialmente realizado por uma equipe de testes diferente da equipe de desenvolvimento do software, com intuito de se evitar vícios.

Deve-se definir cenários de testes, principalmente nos aspectos de segurança, para os casos de atualizações na arquitetura do sistema (servidores de aplicação, banco de dados, versões de browser, versões de sistema operacional, etc.).

4.12.7 Acesso ao repositório de fontes e regras de negócio

1. Para cada projeto há uma área específica em nossos repositórios sendo que os acessos tanto aos fontes como às regras de negócio são permissionadas apenas aos colaboradores que de alguma forma tenha envolvimento com o projeto.
2. Os acessos são controlados via usuário e senha definidos no *Active Directory* corporativo sob a responsabilidade da área de segurança e infraestrutura.
3. Os acessos os repositórios são permitidos, por solicitação formal do líder do time responsável, quando um usuário inicia no projeto.
4. Os acessos são retirados imediatamente quando o usuário é desligado da empresa, entra em licença, saí do projeto ou é realocado.
5. Ao término do projeto todos os acessos são retirados;
6. Além das manutenções cotidianas, há uma avaliação trimestral junto os líderes e é verificado se os usuários ainda devem continuar com os acessos existentes, caso negativo os acessos são retirados.

Politica de Segurança da Informacao-versão 1 1-20220509 pdf

Código do documento 06aefdd8-bd48-4f61-8ba1-b72dd48b36cb

Assinaturas

ESTEFANIE MARI TAKASE
estefanie@7comm.com.br
Assinou como parte

Eventos do documento

16 May 2022, 17:26:25
Documento 06aefdd8-bd48-4f61-8ba1-b72dd48b36cb **criado** por SHAYRA PRISCILA LIMA CAVALCANTE MONTONI (e23f67b1-c445-4f8f-89bd-0bc1c662ba87). Email:shayra.montoni@7comm.com.br. - DATE_ATOM: 2022-05-16T17:26:25-03:00

16 May 2022, 17:28:12
Assinaturas **iniciadas** por SHAYRA PRISCILA LIMA CAVALCANTE MONTONI (e23f67b1-c445-4f8f-89bd-0bc1c662ba87). Email: shayra.montoni@7comm.com.br. - DATE_ATOM: 2022-05-16T17:28:12-03:00

17 May 2022, 15:44:13
ESTEFANIE MARI TAKASE **Assinou como parte** (55c77f38-ec49-4b4e-9492-4cb79138e5b0) - Email: estefanie@7comm.com.br - IP: 200.161.143.173 (200-161-143-173.dsl.telesp.net.br porta: 48822) - Geolocalização: -23.6239887 -46.7196924 - Documento de identificação informado: 127.752.628-13 - DATE_ATOM: 2022-05-17T15:44:13-03:00

Hash do documento original
(SHA256):c206519a220e952fa7d675cc281d037ee5dd50dd52430551cd7b368b65f998c2
(SHA512):4748ce9ae7363718b85739325781f3bd43df6eb1a5ea444b656be9b3695e762b9f889aa1b2393b31cbc8d29ea9dd56c376bd9b7ac65cf0dad3bad2da4a416573

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign

People and tech to transform