tactium

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

FORTALEZA CE

Rua Dona Leopoldina, 1242
Centro CEP: 60110-000
+55 85 4005 0500

SÃO PAULO SP

Avenida Paulista, 2202, Cj 61
Bela Vista, CEP: 01.310-932
+55 11 94827 0749

Gold Microsoft Partner

Microsoft

Sumário

Elaborado por:	Equipe Infraestrutura
Revisado por:	Fernando Mendes
Data modificação:	03/10/2022
	Versão 1.8

1. Visão Geral

Este documento consiste na Política de Segurança da Informação – PSI da Softium informática Ltda, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos, definição de responsabilidades e prevenção de incidentes.

O documento visa orientar e estabelecer as diretrizes corporativas para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

A presente política é baseada nas recomendações propostas pela família de normas ABNT NBR ISO/IEC 27000, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

2. Objetivo

Estabelecer diretrizes que permitam aos colaboradores e parceiros seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Busca-se preservar a Softium e suas informações corporativas nos seguintes termos:

- Integridade: Garantir que a informação seja mantida em seu estado original, visando protegê-la, na posse ou transmissão, contra alterações indevidas, intencionais ou acidentais.

- Confidencialidade: Garantir que o acesso à informação seja obtido somente por pessoas devidamente autorizadas.

- Disponibilidade: Garantir que os usuários autorizados obtenham acesso à Informação e aos ativos correspondentes sempre que necessário.

3. Principios da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte. Dando ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Toda e qualquer informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence à Softium Informática Ltda. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. A Softium, por meio de monitoramento ativo, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações processadas.

4. Das responsabilidades

4.1. Colaboradores em geral

Entende-se por colaborador toda e qualquer pessoa física, contratada por meio da CLT ou prestadora de serviço, por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da empresa.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à Softium Informática Ltda ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

4.2. Colaboradores em regime de exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Polítiva de Segurança da Informação. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

4.3. Gestores de pessoas/processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Softium Informática Ltda.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos da Softium. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores e prestadores de serviços.

5. Acesso à rede corporativa

O ingresso à rede interna da Softium deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados, evitando que ativos não autorizados consigam acesso à rede. Todos os acessos à rede serão fornecidos pela equipe de infraestrutura, utilizando um login que contenha dois nomes próprios do usuário e uma senha segura. Assim, é preciso que sejam instauradas algumas regras:

5.1. Rede cabeada

A rede cabeada estará disponível apenas para máquinas e equipamentos de propriedade da Softium, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas dos colaboradores na empresa. Ativos não autorizados serão colocados em quarentena e devidamente removidos da rede cabeada.

5.2. Rede sem fio

A concessão de acesso à rede sem fio para acesso apenas à Internet se dará através de solicitação formal junto ao setor responsável. (ver possibilidade de formulário para tal solicitação)

5.3. Acesso à Internet

A Internet disponibilizada pelo Softium aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada pelo chefe e não prejudique o andamento dos trabalhos nos setores. A Softium utilizará de métricas para bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação.

5.4. Monitoramento de acesso

A Softium reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos. Haverá geração de relatórios de acesso à sites e downloads por usuário.

5.5. Downloads e uso de software de terceiros

Os colaboradores com acesso à Internet só poderão fazer o download de programas necessários às suas atividades e deverão providenciar a licença e o registro necessário desses programas, O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo setor responsável.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da Softium para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

5.6. Restrição de acesso às portas USB

Portas USB são um vetor chave para infringir a segurança da informação, podendo ser usadas para o roubo de informações confidenciais e propagação de malwares. Tal vulnerabilidade não é corrigível com firewalls, necessitando do comprometimento dos colaboradores para que seja mantida as boas práticas de segurança.

Portanto, para prevenir riscos e exposições à Softium, todas as portas de transferência de arquivos para dispositivos removíveis foram bloqueadas.

A liberação das portas USB pode ser solicitada caso o uso seja justificado e aprovado pelo líder do solicitante, mediante a autorização da diretoria. Caso contrário, nenhuma ação justifica a transferência de informações por meio de dispotivios removíveis dentro do ambiente.

5.7. Armazenamento de arquivos

Os arquivos inerentes à Softium, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

5.8. Descarte de mídias

O descarte de mídia deve ser mediado via processo de autorização, garantindo que nenhuma informação seja descartara erroneamente. Mídias somente devem ser descartadas caso a informação armazenada seja preservada em outro meio, além de garantir que os suportes em processo de descarte não possam ser lidos por membros fora da Softium.

Não é permitido o descarte em lixo comum de documentos e aparelhos confidenciais nem o descarte sem autorização prévia do setor de infraestrutura, que é responsável por documentar e auxiliar todo o processo.

5.8.1 Métodos de descarte:

a) em caso de papel, recomenda-se que seja fragmentado ao ponto de toda as informações contidas ficarem ilegíveis. Esse processo é possível de ser realizado tanto manualmente como com o suporte de ferramentas.

b) em caso de discos rígidos e SSD, é necessária uma formatação total do aparelho, impossibilitando que dados deletados sejam recuperados. Caso os dispositivos não funcionem corretamente é possível ser feita a sua destruição.

c) CDS e DVDS devem ser fragmentados com o auxílio de tesouras antes de irem para o lixo.

d) Mídias arquivadas no computador devem ser excluídas da pasta de armazenamento e logo em seguida removidas da lixeira, impossibilitando que o arquivo seja restaurado.

5.9. Política de Senhas

A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;

5.9.1 Ciclo de vida

a) A senha inicial só será fornecida ao próprio colaborador ou diretamente ao seu gestor. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador

b) É proibido o compartilhamento de login para funções de administração de sistemas;

c) As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);

d) As senhas deverão seguir os seguintes pré-requisitos:

Tamanho mínimo de oito caracteres;
Existência de pelo meno três desses caracteres:
Letras maiúsculas,
Letras maiúsculas,
Números e caracteres especiais;
Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, etc).

e) O acesso deverá ser imediatamente cancelado nas seguintes situações:
Desligamento do colaborador
Mudança de função do colaborador
Quando, ou qualquer razão, definida previamente pelo gestor

5.10. Email

O E-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

5.11. Estações de trabalho

a) É de responsabilidade do colaborador do equipamento zelar pelo mesmo, mantendo-o em boas condições;

b) É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, entrar em contato com setor responsável;

c) As estações de trabalho só estarão acessíveis aos colaboradores através de suas contas de usuário de domínio.

d) É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe do INFRA;

e) É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe de INFRA;

f) As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do colaborador;

g) Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;

h) Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;

i) É proibido o uso de estações de trabalho para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

j) O setor de INFRA não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição

k) As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

5.12. Equipamentos particulares e dispositivos móveis

Todas as regras do tópico “Estações de Trabalho” se enquadram nesta seção, adicionando os seguintes pontos:

Fica autorizado o uso de notebooks e dispositivos móveis (Smartphones, Tablets) para acesso à rede interna da Softium mediante autorização do chefe imediato. O setor de INFRA deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido.

Os equipamentos particulares devem ser utilizados somente após a validação do setor de INFRA, garantindo que o antivírus e o firewall estejam oferencendo a devida proteção ao colaborador.

6. Backup

Os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento. As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter.

7. DataCenter

7.1. Estrutura Física do Data Center

Os Servidores que armazenam os sistemas utilizados pela Softium Informática, ficam em área protegida e de acesso restrito. Todos os equipamentos críticos para o funcionamento das atividades computaticonais da empresa ficam mantidos no Data Center. A entrada no DataCenter tem acesso devidamente controloda e monitorado, as permissões de acesso físico são definidas pela diretoria e equipe de segurança.

O acesso às dependências do DataCenter com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de Segurança e mediante supervisão.

O acesso ao Datacenter sem as devidas identificações só poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Caso haja necessidade do acesso não emergencial, o requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a mesma deve ser autorizada pelo Subcomitê Gestor de Segurança da Informação.

7.2. Estrutura Lógica do Data Center

Na política de segurança da Informação da Softium Informática, define-se que o setor de INFRA, deve ser o único a ter permissão para ler/editar as informações, obedecendo as atribuições de sua área de atuação.

O objetivo da segurança lógica no Data Center é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados. Somente os colaboradores devidamente autorizados podem ter acesso aos dados armazenados. Os logs dos ativos de rede devem ser monitorados constantemente a fim de evitar acessos indevidos.

8. Gestão de Logs

Ativos autorizados pela Softium obedecem à vigência da política de logs, sendo monitoradas informações como data e hora de login e logout dos usuários, acessos negados, origem da conexão e arquivos acessados.

Os logs são armazenados de forma centralizada por até 90 dias, ocasionalmente sendo utilizados para análise e verificação de atividades suspeitas, mantendo um período adequado para cumprir o processo de gerenciamento de auditorias.

As análises de logs devem ocorrer a cada 60 dias ou a cada vez que uma anomalia for detectada, sendo obrigatório documentar todo o processo para consultas futuras.

9. Gestão de Patches

9.1. Objetivo

Busca-se preservar a Softium e suas informações corporativas por meio da gestão de patches, garantindo o funcionamento seguro dos softwares ativos na empresa por meio de atualizações periódicas. Dessa forma, a política de patches tem por objetivo a definição de normas e procedimentos específicos para nortear o processo de atualizações e correções em ativos.

Por questões administrativas e de segurança, somente a equipe de infraestrutura deve ter acesso aos processos de gerenciamento de patches. Dados que resultem de análise de logs, scans de vulnerabilidades ou qualquer outro meio que detecte uma falha de segurança em um ativo deve manter-se restrito à equipe autorizada da Softium.

9.2. Implementação de patches

O escopo elaborado pela Softium engloba todos os desktops e servidores de propriedade da empresa, além de outros dispositivos conectados à rede de internet, como câmeras, roteadores e switches. Os principais alvos das atualizações são sistemas operacionais.

Os patches de atualização são gerenciados de modo a permitir o controle sobre o que deve ou não ser alterado, garantindo que apenas atualizações de caráter definitivo sejam implementadas no sistema, evitando bugs e prevenindo riscos de indisponibilidade dos ativos.

São utilizados softwares próprios para versar o processo de implementação, como o WSUS e o WDS, garantindo que tudo ocorra de forma automatizada e com as devidas evidências. Além disso, em casos de maior severidade, a equipe de infraestrutura vai acompanhar e monitorar todo o processo de atualização.

9.3. Periodicidade

Os patches de atualização são implementados de acordo com a urgência de cada cenário. Dessa forma, para garantir uma melhor disponibilidade dos serviços, foi definido um escopo de tempo baseado na natureza de cada atualização:

a) Atualizações críticas de segurança

Atualizações críticas devem ser implementadas o mais breve possível, zelando pela integridade dos ativos. A implementação do patch de correção deve ocorrer 5 dias após o seu lançamento, garantindo que erros ou falhas no processo de atualização já tenham sido identificados e corrigidos.

b) Atualizações altas ou médias de segurança

Atualizações altas ou médias devem ser implementadas em até 60 dias após o lançamento e somente caso sejam necessárias ao desenvolvimento das atividades dentro da Softium.

c) Atualizações de desempenho e novas funções

Atualizações que não apresentam um caráter relacionado à segurança podem ser implementadas em até 120 dias após o lançamento.

Assim, para garantir o funcionamento ideal dos ativos, os processos de implementação de patches estão previstos para ocorrerem uma vez a cada mês (salvo as atualizações críticas).

10. Tratamento de Incidentes

O Tratamento de incidentes de segurança dentro da corporação visa zelar pela segurança das informações e comunicações da Softium, prevenindo e tratando incidentes de rede, em cumprimento à Política de Segurança da Informação.

A gestão de incidentes de segurança, que consiste em receber, filtrar, classificar e responder às solicitações e alertas bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de vulnerabilidades.

Toda e quaisquer falhas, anomalias, ameaça ou vulnerabilidades observadas devem ser notificadas de forma imediata ao setor responsável através de chamado de suporte no Tactium e envio de e-mail para: infra@softium.com.br.

Cabe à equipe de segurança obter informações acerca dos incidentes ocorridos que descrevam: sua natureza, as causas, a data do ocorrido, bem como a frequência e os sintomas apresentados.

Após o levantamento dos dados do incidente o mesmo deverá ser tratado e documentado, visando manter histórico dos incidentes ocorridos. A equipe de segurança irá trabalhar em conjunto com a direção para deliberar as medidas a serem adoradas quanto aos riscos dos incidentes identificados.

11. Conscientização sobre segurança e privacidade

A Softium disponibiliza um treinamento de segurança da informação, visando conscientizar os colaboradores a adotarem boas práticas. A atividade deve ser realizada por meio de apresentações, vídeos, debates e reuniões entre os colaboradores e o time de infra.

O treinamento deve ocorrer anualmente, preferencialmente divido em duas partes, retratando temas recorrentes sobre segurança que possam impactar diretamente a integridade dos serviços e do ambiente Softium.

O planejamento das atividades deve levar em consideração fatores estratégicos para a criação, como a quantidade e disponibilidade dos colaboradores, segmento de atuação e a notoriedade dos assuntos abordados, dando prioridade a fatos que sejam recorrentes à instituição.

12. Violações da política e suas penalidades

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

a) Advertência verbal

O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação da Softium e será recomendado à leitura desta Norma.

b) Advertência formal

A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida. A segunda notificação será encaminhada para a chefia imediata do infrator