Política de Segurança da Informação

Soluções Estratégicas e Inteligência Corporativa

Interact SOLUTIONS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
INTERACT SOLUTIONS

MN 022 – Versão 02

Infraestrutura

Lajeado - RS, junho de 2020

SUMÁRIO

1 INTRODUÇÃO

A Interact, empresa brasileira de pesquisa e desenvolvimento de softwares, atua no mercado de Tecnologia da Informação desde 1999, ocupando uma reconhecida posição de liderança no Brasil e em expansão na América Latina e Europa no mercado de sistemas e soluções para a gestão corporativa, reconhecendo a importância de proteger as informações e os ativos de Tecnologia da Informação - TI com relação aos riscos e às ameaças que apresentam nesta área.

A área de Infraestrutura, ciente da relevância deste assunto, elaborou este manual com o objetivo de estabelecer diretrizes, princípios e responsabilidades, além de orientar na execução das ações relacionadas ao tratamento das informações e ao uso adequado de ativos e/ou informações pelos colaboradores, terceiros e fornecedores do Grupo Interact.

1.1 Objetivo

Este documento institui um padrão para o tratamento adequado de ativos e/ou informações estabelecendo diretrizes que permitam aos usuários da Interact Solutions seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo, visando alinhar suas ações aos três pilares da segurança da informação:

- **Confidencialidade**: garantir que os ativos e informações tratadas sejam de conhecimento e uso exclusivo de pessoas especificamente autorizadas;
- **Integridade**: garantir que os ativos e informações sejam mantidos íntegros, sem modificações indevidas, acidentais ou propositais;
- **Disponibilidade**: garantir que os ativos e informações estejam disponíveis a todas as pessoas autorizadas a tratá-los e utilizá-los.

1.2 Definições

Colaboradores – entende-se como colaborador qualquer pessoa física contratada como CLT, jovem aprendiz, estágio ou intercâmbio que exerça atividades vinculadas ao Grupo Interact.

Terceiros – prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Mídias – CDs, DVDs, pendrives, HD externos, discos rígidos, fitas LTO ou qualquer outro tipo de dispositivo que possa armazenar informações digitais.

Comunicadores instantâneos – Skype, Clickmeeting, Rocketchat, Whatsapp ou qualquer outro *software* similar.

Servidores – um servidor é um *software* ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores. Esses serviços podem ser de naturezas distintas, como por exemplo, arquivos e correio eletrônico.

Área de Infraestrutura – responsável por planejar, coordenar, executar, monitorar e avaliar projetos e atividades relacionados a investimento, desenvolvimento, manutenção e segurança em tecnologia da informação.

VLAN - Uma rede local virtual logicamente independente. Várias VLANs podem coexistir em um mesmo computador (*switch*), de forma a dividir uma rede local (física) em mais de uma rede (virtual).

DMZ – é a área de rede que permanece entre a rede interna de uma organização e uma rede externa, normalmente detém os equipamentos que hospedam serviços e realizam uma comunicação bilateral entre a LAN (*Local Area Network*) e WAN (*Wide Area Network*).

VPN – *Virtual Private Network*, é de uma rede virtual e remota com objetivo de interligar um dispositivo remoto a rede local da Interact.

Compliance – busca a adequação, fortalecimento e funcionamento dos sistemas de controles internos, visando a mitigação de riscos legais, operacionais, reputacionais e disseminação da cultura de controles para assegurar o cumprimento da legislação e das políticas internas e externas existentes.

Compliance Officer – profissional responsável por verificar que todos estão praticando o Compliance na Interact.

Compliance Office - é o grupo interdisciplinar, formado pelo Compliance Officer (profissional responsável por fomentar o cumprimento dos regulamentos internos e externos) e Diretores.

Vulnerabilidades – qualquer fragilidade dos sistemas computacionais e redes de computadores que permita a exploração maliciosa e acessos indesejáveis ou não autorizados.

Ativos – todo e qualquer recurso tecnológico físico ou virtual que compõe a infraestrutura de TI.

Infomações internas – CPF's, RG, endereço, telefones, valores contratuais, currículos

Softwares piratas – softwares sem licenciamento ou inadequado para ambientes corporativos (licenças para uso doméstico, universitário ou desenvolvimento).

Lei Geral de Proteção de Dados Pessoais (lei nº 13.709/2018) – LGPD - em vigor a partir de agosto de 2020 a lei abrange uma série de princípios, direitos e deveres visando regular o tratamento de dados pessoais e exige o desenvolvimento e adequação da cultura da segurança e proteção de dados.

2 DIRETRIZES

2.1 Acesso à rede física e sem fio

- A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade do Interact, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores;

- A Internet sem fio deverá ser segmentada, garantindo o isolamento das redes internas, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas; poderão ter outras redes com acesso apenas à internet para disponibilizar aos visitantes e usuários que não podem ter acesso aos dados internos;

- Não serão permitidas as alterações das configurações de rede, introdução de equipamentos como *switchs*, *hubs* ou roteadores, bem como o roteamento através de celulares, *notebooks* ou virtualizadores sem o devido conhecimento da área de Infraestrutura;

- Os colaboradores não poderão usar os recursos da Interact para deliberada ou inadvertidamente propagar qualquer tipo vírus, *worms*, cavalos de troia, *spam*, *keyloggers* ou programas de controle remoto de outros computadores;

- Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede

interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando a área de Infraestrutura deverá estar devidamente ciente e autorizar o procedimento;

- Os acessos externos à rede local da Interact só serão permitidos através de VPN's nominais e intransferíveis, o destino permitido nessa VPN será o acesso a estação de trabalho do próprio colaborador;

- A utilização dos dispositivos móveis pessoais, como celulares e *tablets*, não estarão sujeitos aos mesmos controles aplicados aos computadores e outros dispositivos de propriedade da Interact, porém, não isentará os colaboradores de seguirem as mesmas diretrizes descritas nesse PSI;

2.2 Acesso à Internet

- Os acessos à internet através dos equipamentos e serviços da Interact devem ser utilizados com finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais;

- A Interact reserva o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos e evitar possíveis indisponibilidades ou quedas na qualidade da prestação do serviço, garantindo a integridade da rede, sistemas e dados internos, observando a LGPD;

- Os colaboradores não poderão em hipótese alguma utilizar os recursos do Interact para fazer o *download* ou distribuição de *software* ou dados "pirateados";

- É permitido ao colaborador a utilização do acesso à internet para realizar o *download* de arquivos que sejam necessários à execução das suas atividades, desde que em conformidade com a lei, a moral e os bons costumes bem como os termos de licença de uso, os registros dos programas e os direitos autorais.

Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de *proxies* anônimos e estratégias de *bypass* de *firewall*;

- É proibida a divulgação e compartilhamento de informações em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia ou similar, sem o devido enquadramento e conhecimento ao PSI e Compliance Officer;

- Não é permitida a utilização de *software* de *peer-to-peer* (P2P), tais como Torrent, Kazaa, Emule e afins.

- Qualquer comunicação realizada durante o cumprimento da sua função laboral deve ser através de canal oficial, com identificação corporativa criada pela área de Infraestrutura nos padrões definidos pela Interact;

2.3 Estações de trabalho

- Todo o colaborador deve assinar o termo de comodato de equipamento antes de iniciar as suas atividades na Interact;

- É de responsabilidade do colaborador zelar pelas boas condições de uso do equipamento, realizando a limpeza básica e utilizando-o de forma consciente;

- Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;

- É vedada a abertura de computadores para qualquer tipo de atividade pelos colaboradores;

- As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas, salvo quando forem equipamentos de uso compartilhados, como salas de reuniões, estações para acessos remotos e VPN’s e estações de testes;

- É proibida a instalação de *softwares* ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela área de Infraestrutura;

- É proibida a utilização de quaisquer *softwares* que não estejam listados no DC 196 - Softwares Padrão;

- Os documentos e arquivos críticos, que necessitam de *backup*, não devem ser armazenados localmente, eles devem ser armazenados no mapeamento do servidor de arquivos correspondente ao setor do colaborador;

- Em computadores e/ou dispositivos pessoais ou de terceiros a área de Infraestrutura não será responsável pela manutenção, instalação e configuração de *software* ou *hardware* e *backups*;

- Toda atividade executada pelo colaborador que viole a legislação em vigor, a moral e os bons costumes é de sua inteira responsabilidade**;**

2.4 Servidores

- Os servidores só poderão ser acessados através de chaves de acessos privados;

- Todo acesso ao servidor é controlado por políticas de *firewall* que especificam a origem, o destino e o protocolo;

- São hospedados em uma VLAN DMZ onde não deve haver tráfego paralelo entre colaboradores e servidores, apenas vertical, através do *firewall;*

- Os servidores da Interact devem ser devidamente monitorados e ter políticas de *backup* com o intuito de manter a mais alta disponibilidade e integridade dos serviços hospedados;

- Os servidores devem ser mantidos atualizados, nas últimas versões estáveis dos *patchs*, *hotfix* e versões de aplicativos e sistemas operacionais;

2.5 Datacenter

- Os servidores ficam alocados no datacenter da Interact, o acesso físico aos mesmos só será permitido com aval e presença de um colaborador da área de Infraestrutura;
- A sala do datacenter fica trancada, a chave para acesso fica em posse da área de Infraestrutura;
- O controle de temperatura e umidade bem como a manutenção do sistema de refrigeração da sala deve ser monitorado constantemente;
- Todos os equipamentos devem estar ligados a *no-breaks*;
- A sala do datacenter deve possuir extintores específicos para equipamentos eletrônicos;

2.6 Backup

- Implementar e manutenir métricas para monitoramento e validação da rotina de *backup*;
- *Backups* devem ser armazenados em uma estrutura remota, fora das dependências da Interact;
- A área de Infraestrutura deve realizar testes periódicos, por processo de amostragem, nas amostras de *backup*;
- *Backups* não podem ser transportados ou armazenados por colaborador que não seja da Infraestrutura para evitar que o acesso aos dados, através do *backup*, burle o controle e a gestão dos acessos implementados nos servidores;

2.7 Licenciamento de Software

- A Interact proíbe a utilização de qualquer software não licenciamento nas suas dependências pelos seus colaboradores;

- A utilização de qualquer software, seja ele: *desktop*, *portable*, SaaS ou aplicativos para dispositivos móveis está condicionada à liberação da Infraestrutura;

- Em equipamentos pessoais, mesmo os softwares licenciados devem passar pela inspeção da área de Infraestrutura, tendo em vista que o licenciamento em ambiente corporativo pode ser diferente do licenciamento de ambiente doméstico;

2.8 Política Mesa Limpa/Tela Limpa

- Os computadores de trabalho devem permanecer bloqueados (logoff) nos períodos de ausência do colaborador;

- Ao utilizar um recurso de uso comum, como sala de reuniões ou estações de testes, é de responsabilidade do colaborador remover as informações, sessões ou credenciais que foram utilizadas no mesmo;

- Informações impressas devem ser armazenadas corretamente ao se ausentar do seu posto de trabalho;

- As estações de trabalho devem ser desligadas ao término do expediente, diminuindo o período de exposição à ataques e invasões e promovendo uma utilização sustentável da energia elétrica;

- Todo descarte de mídias deverá ser realizado exclusivamente pela área de Infraestrutura, antes de descartadas as mídias serão destruídas de acordo com o seu tipo e finalidade;

2.9 Gestão de acessos

- Os acessos são pessoais e intransferíveis, é de responsabilidade do colaborador o zelo pelas credenciais;
- Qualquer violação, proposital ou não, deve ser imediatamente comunicada a área de Infraestrutura, para que novas senhas ou chaves de segurança sejam disponibilizadas;
- As credenciais de acesso e as permissões vinculadas as mesmas serão cadastradas via processo automatizado “Admissão de Colaboradores” ou “Solicitação de Liberação de Acessos”;
- A exclusão das credenciais de acesso e suas permissões será realizada mediante processo automatizado “Rescisão de Colaboradores”;
- Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens;
- Os acessos do colaborador serão bloqueados durante os períodos de férias e licenças mediante processo automatizado “Processo de Férias” e “Solicitação de Ausência”;
- Toda alteração de acesso deve ser realizada via ticket ou processo automatizado com aprovação do superior imediato ou responsável do requerente;
- Deve ser realizado o monitoramento e histórico dos acessos realizados pelos usuários;

2.10 Correio Eletrônico e comunicadores instantâneos

- Todas as contas de correio eletrônico e comunicadores instantâneos terão uma titularidade determinando o responsável sobre a sua utilização;

- A utilização do correio eletrônico da Interact está vinculada a utilização da assinatura de e-mail padronizada pela área de Infraestrutura, nenhum e-mail deve ser enviado sem a identificação formal da Interact;

- Não é permitido o envio simultâneo de e-mails para mais de 20 destinatários;

- Não é permitido o envio de e-mails com mais de 20mb;

- É permitido o envio de e-mails com anexos com extensões de arquivo: de pacotes office e editores de texto (BrOffice, LibreOffice, Microsoft Office, Wordpad, Notepad e similares), documentos PDF e compactadores de arquivos (7Zip, Winrar, Winzip, TAR, Gzip e similares);

- Não é permitido o envio de e-mail com trechos de código, SQL ou scripts;

3 OBRIGAÇÕES

3.1 Colaboradores

- Conhecer e cumprir as normas e orientações estabelecidas neste documento, bem como no MN–013 Manual do Colaborador e MN-006 Código de Ética, Conduta e Compliance da Interact;
- Responder por atos que violem as diretrizes deste PSI;
- Reportar qualquer violação a esta política, suas normas e diretrizes à área de Infraestrutura, seus superiores ou Canal de Denúncias da Interact;
- Buscar a área de Infraestrutura ou Compliance Officer para qualquer esclarecimento referente as diretrizes e orientações estabelecidas neste PSI;
- Proteger os ativos e informações contra acesso, divulgação, modificação ou destruição não autorizados pela Interact;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Interact;
- Não se passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;

3.2 Área de Infraestrutura

- Definir as regras para implementação de *software* e *hardware* na Interact;
- Homologar os equipamentos pessoais (*smartphones* e *notebooks*) para uso na rede da Interact;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede, *desktops*, *notebooks* e dispositivos

móveis), tendo como referência a Política de Segurança da Informação – PSI e o ***Anexo 5.1*** deste documento;

- Propor melhorias nas metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades, etc.;
- Identificar vulnerabilidades e realizar as ações necessárias para mitigá-las;
- Analisar criticamente incidentes de segurança em conjunto com o Compliance Officer da Interact;
- Administrar, proteger e testar as cópias de segurança (*backup*) dos programas e dados relacionados aos processos críticos e relevantes para a Interact;
- Elaborar cenários de incidentes para realização periódica de testes de continuidade;
- Estabelecer planos de contingência;
- Buscar alinhamento com das diretrizes do PSI com os objetivos da organização;

3.3 Compliance Officer

- Adotar medidas corretivas e disciplinares, garantir a imparcialidade e demonstrar o compromisso com todo o processo investigativo de denúncias;

4 REFERENCIAS

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;

Legislação federal Lei n.º 12.965/2014 – Marco Civil da Internet;

Legislação federal Lei nº 12.551/2011 – Home Office;

Legislação federal Lei nº 12.527/2011 – Legislação sobre acesso à informação;

Legislação federal Lei nº 9.609/1998 – Legislação sobre software;

Legislação federal Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

5 ANEXOS

5.1 Matriz de Monitoramento

Navegação/Internet

Conteúdo monitorado: origem, destino e data/hora
Periodicidade: 180 dias

E-mails

Conteúdo monitorado: origem, destino, assunto, mensagem, data/hora e anexos
Periodicidade: 90 dias

Rocketchat

Conteúdo monitorado: origem, destino, mensagem, data/hora e anexos
Periodicidade: indeterminado para mensagens e 45 dias para anexos

Segurança predial

Conteúdo monitorado: imagem e digitais
Periodicidade: indeterminado

Telefone

Conteúdo monitorado: origem, destino e data/hora
Periodicidade: indeterminado