zema | FINANCEIRA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

VERSÃO 02

Data de Edição: dezembro/2020

Sumário

1. INTRODUÇÃO

1.1. Objetivos

A Política Corporativa de Segurança da Informação (PSI) é a incorporação lógica dos requisitos de negócio da empresa para segurança e controle. Objetiva estabelecer instruções e diretrizes para assegurar a integridade, confidencialidade e disponibilidade das informações e sistemas. Também esclarece as responsabilidades dos acionistas, colaboradores, terceiros, parceiros e fornecedores; bem como as diretrizes a serem consideradas para preservar e proteger as informações e recursos que processam e/ou transportam estas informações.

1.2. Escopo

Esta política abrange todas as informações, os sistema e recursos de Tecnologia da Informação **Zema Crédito, Financiamento e Investimento S/A**, designada neste documento como Empresa, suas filiais e subsidiárias; incluindo também seus colaboradores, estagiários, terceirizados, temporários e fornecedores em quaisquer das dependências da Empresa ou locais onde estes se façam presentes através da utilização, manuseio ou processamento das informações.

1.3. Responsabilidades

A Tecnologia da Informação (TI), seus recursos e informações são imprescindíveis para o negócio da Empresa. Também é inquestionável assegurar a proteção destes ativos através da gestão contínua de Segurança da Informação (SI).

Assim, a Diretoria de Operações é responsável pela Gestão de Segurança da Informação (SGSI – Sistema de Gestão de Segurança da Informação) bem como por

estabelecer, manter, publicar e divulgar as políticas de segurança, padrões e procedimentos. A operação, manutenção dos serviços de segurança, a investigação de intrusão em sistemas e outros incidentes de segurança da informação são de responsabilidade da área de Tecnologia da Informação (TI).

Também é responsabilidade da Auditoria Interna garantir o bom andamento do processo de gestão de SI, bem como a aderência de todas as áreas da Empresa a esta Política, através da publicação mensal de indicadores, realização de auditorias internas e/ou externas anualmente, em intervalos regulares e assegurando que riscos sejam mitigados em conjunto com a alta direção da Empresa.

As áreas de negócio da Empresa devem assegurar que contratos com clientes, fornecedores e parceiros de negócio possuam cláusulas de Segurança da Informação que assegurem a proteção das informações e recursos de TI. Um Termo de Confidencialidade deve ser assinado entre as partes antes do início de serviços e projetos que envolvam informações sensíveis, sendo responsabilidade da área contratante a garantia de que as cláusulas e termo de confidencialidade estão presentes durante e após a negociação.

Colaboradores da Empresa devem familiarizar-se, aderir e praticar as políticas contidas na PSI, bem como procedimentos e padrões relacionados à Segurança da Informação. As informações resultantes das atividades comerciais da Empresa, principalmente aquelas relacionadas a concessão de crédito que envolvam o tratamento de dados pessoais devem garantir adequação a Lei Geral de Proteção de Dados (13709/2018). Portanto, todos os colaboradores têm a obrigação de tratar estas informações como sigilosas, sob pena de sansões, punições, processos cíveis e criminais no rigor da lei.

A área responsável por Recursos Humanos é responsável por informar sobre os requisitos de Segurança da Informação aos possíveis candidatos a vagas de emprego da

Empresa mesmo antes de se concretizar a contratação, bem como apoiar e garantir os processos de educação e conscientização em Segurança da Informação durante o ciclo de vida do colaborador na Empresa.

Ações disciplinares resultantes da violação dos requisitos e diretrizes de Segurança da Informação serão tratadas pelo gestor do colaborador em conjunto com a área responsável por recursos humanos e caso necessário dependendo da gravidade devem ser levadas a apreciação e tratamento pelo Comitê de Ética da Empresa.

Visando a evolução do processo de gestão de Segurança da Informação e Privacidade de Dados Pessoais o Comitê de Gestão de Privacidade e Segurança da Informação deverá ser composto por gerentes de departamentos da Empresa, ou membros designados por estes. Deve reunir-se no mínimo bimestralmente ou em situações especiais através de convocação extraordinária. O Comitê deve avaliar e revisar o estado corrente da Gestão de Privacidade e Segurança da Informação na Empresa, aprovar novas ou modificar políticas de segurança, privacidade e deliberar sobre outras questões de alto-nível relacionadas às atividades de Gestão da Segurança da Informação.

A alta direção da Empresa deve supervisionar e garantir recursos para a eficácia do Comitê de Gestão de Privacidade e Segurança da Informação.

1.4. Carta da Presidência

Prezados Colaboradores,

O Grupo Zema ocupa uma posição destacada perante a sociedade por cultivar, desde o início de sua atuação, valores como Ser Simples, Transparência, Construir Pessoas, Trabalho e Coragem com Energia e Ética.

A reputação da nossa marca se constrói e se fortalece justamente graças à decisão diária de cada um dos nossos colaboradores de preservar os valores do Grupo, por meio de uma conduta profissional responsável no relacionamento com os colegas de trabalho, fornecedores, parceiros, clientes e sociedade.

Ao tornar público e acessível esta Política de Segurança da Informação, o Grupo Zema reafirma a importância desses valores para a perpetuação de seus negócios e demonstra o quanto é imprescindível o compromisso dos colaboradores em conhecer, seguir e praticar as responsabilidades e diretrizes para Segurança da Informação aqui previstas.

Este documento sintetiza o posicionamento do Grupo Zema quanto ao melhor caminho para se conservar um ambiente de trabalho seguro preservando a integridade, confidencialidade e disponibilidade das informações; oferecendo à sociedade um ambiente com as condições necessárias para a construção de relacionamentos saudáveis, à base de confiança, dignidade, lealdade, transparência e segurança.

Contamos com você.

Romero Zema

CEO Zema Crédito, Financiamento e Investimento S/A

2. RECURSOS HUMANOS

Assim que realizada a contratação, todos os colaboradores da Empresa devem receber cópia da PSI, ler e assinar o Termo de Responsabilidade e Confidencialidade, caracterizando a concordância com as diretrizes definidas nesta Política.

É responsabilidade da área de Recursos Humanos garantir este processo, bem como o arquivamento na pasta do colaborador de cópia do Termo de Responsabilidade e Confidencialidade assinado.

Todos os colaboradores em processo de término do contrato de trabalho devem ter os acessos revogados o mais rápido possível. É responsabilidade da área de Recursos Humanos garantir a execução fim-a-fim deste processo, onde é responsabilidade do gestor da área iniciar a exclusão através dos trâmites de acionamento e comunicação do desligamento; e da TI remover ou bloquear os acessos.

É responsabilidade da área de Recursos Humanos prover meios de divulgação desta política e de aculturação relacionada à Segurança da Informação para colaboradores já contratados e/ou em fase de contratação.

3. AUDITORIA, SANÇÕES E PUNIÇÕES

A Empresa reserva o direito para si de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações. Incluindo-se o uso particular (pessoal) através destes recursos, quando da existência de informações e/ou evidências de atos ilícitos ou conduta inadequada. Estes registros também podem ser utilizados para análises estatísticas visando a boa prestação de serviços e para verificação em casos relacionados a incidentes de segurança.

Auditorias internas podem ser executadas sem aviso prévio, para a verificação do atendimento das considerações que compõe e suportam esta política.

No caso de descumprimento de quaisquer das considerações desta política e de não conformidade de auditorias internas, medidas disciplinares serão orientadas pelo Recursos

Humanos e Comitê de Ética, onde cada caso será avaliado face aos impactos e contexto aplicáveis.

Como medidas disciplinares poderão ser consideradas desde o simples feedback formal ao término do contrato de trabalho por justa causa.

4. DÚVIDAS, SUGESTÕES E EXCEÇÕES

A Diretoria de Operações é responsável pelo esclarecimento de dúvidas, recepção e tratativa de sugestões relativas a esta política. Dúvidas, sugestões e relatos de incidentes devem ser enviados para os endereços security@zemafinanceira.com, abuse@zemafinanceira.com ou comunicadas através do telefone 0800 095 6702 (Ouvidoria).

Exceções a esta política devem ser apresentadas a gerência imediata do colaborador, a qual deverá submetê-las à Diretoria de Operações, onde serão discutidas e avaliadas. Caso necessário, a exceção será submetida para apreciação do Comitê de Gestão de Privacidade e Segurança da Informação e/ou a alta direção da Empresa.

Todas as exceções devem ser devidamente registradas e documentadas de forma a propiciar a evolução futura desta política.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Para assegurar que a informação receba um nível adequado de proteção e de acordo com sua importância, a *Empresa* estabelece três categorias para responsabilidades associadas à informação e seu manuseio. Pelo menos uma das categorias aplica-se para cada colaborador, cliente, fornecedor e/ou parceiro enquanto durar a relação contratual ou trabalhista.

A saber: Proprietário, Custodiante e Usuário da informação.

Proprietário – O dono das informações, são os gerentes das unidades de negócio, membros das altas gerências ou aqueles que receberam delegação da *Empresa* para tratamento da informação através de sistemas da informação e/ou em meios não digitais. Sistemas são programas de computador que fornecem relatório e informações para suportar o processo decisório e de negócio da *Empresa*. Todos os sistemas de informação da *Empresa* TÊM que possuir um Proprietário (responsável) designado. Para cada tipo de informação, o Proprietário é responsável por designar a respectiva classificação, definir quais colaboradores terão acesso e o nível deste acesso; bem como aprovar requisições para os vários modos de utilização destas informações. Dados pessoais devem ser possuir especial atenção por parte do Proprietário, quanto a sua classificação e tratamento. O Proprietário dos dados é responsável por garantir que os requisitos da LGPD 13709/2018, incluindo-se consenso do Titular, registro do tratamento, exclusão, intercâmbio autorizado e segurança desde a concepção do processo de negócio, sejam atendidos.

Custodiante – São os indivíduos que têm a possessão física ou lógica das informações da *Empresa*. Os funcionários da área de Tecnologia da Informação, administradores de sistemas são primariamente designados como custodiantes. A *Empresa* é custodiante das informações de ou para concessão de crédito ao Cliente, incluindo-se os dados pessoais. Os custodiantes são responsáveis pela salvaguarda das informações, incluindo a implementação de controles para prevenir acesso e divulgação inadvertida; responsáveis pelas cópias de segurança (*backup*) para garantir que informações críticas não serão perdidas. O custodiante é responsável pela implementação, operação e manutenção das medidas de segurança requisitadas pelos Proprietários da informação. Quando o colaborador processa e mantém a informação na própria estação de trabalho ele automaticamente designa-se como custodiante e responsável pela mesma e, neste caso, é responsabilidade da área de TI garantir a existência e implementação de medidas de controle para segurança das informações nas estações de trabalho.

Usuários – Utilizam as informações no dia-a-dia de acordo com suas funções e classificação da informação. É obrigatória a utilização das informações e recursos de TI

somente para atividades relacionadas ao desempenho de sua função. Estes têm a responsabilidade de familiarizarem-se, aderir e praticar as políticas da PSI, bem como relatar possíveis incidentes relacionados a segurança através dos mecanismos existente e/ou para seu superior imediato.

5.1. Tipos de Classificação

As informações de propriedade ou sob responsabilidade da *Empresa* devem ser classificadas de acordo com o os tipos: CONFIDENCIAL, RESTRITO, USO INTERNO e PÚBLICA:

PÚBLICA – poderá ser tratada e divulgada internamente e externamente sem qualquer aprovação formal;

CONFIDENCIAL – somente poderá ser tratada e divulgada (pelas) para as entidades (usuários, clientes, fornecedores e outros) definidas como autorizadas a receberem a informação, por exemplo enquadram-se nesta classificação: informações relacionadas a novos planos de negócio e estratégias de crescimento da *Empresa*.

USO INTERNO – poderá ser tratada e divulgada somente na *Empresa* para áreas devidamente designadas e autorizadas, requerendo aprovação formal para ser divulgada externamente, por exemplo: modelo, processos e informações de operação da *Empresa*.

RESTRITO – informações formalmente autorizadas para tratamento por outras empresas e órgãos governamentais. Dados pessoais e informações caracterizadas como SENSÍVEL pela Lei Geral de Proteção de Dados (LGPD 13709/2018) deverão ser automaticamente tratadas como RESTRITO.

5.2. Classificação Padrão

Informação que não foi designada como CONFIDENCIAL, RESTRITO ou PÚBLICO TEM que ser tratada como USO INTERNO até que o Proprietário estabeleça a classificação.

Adicionalmente, informações pertencentes a “terceiros”, veiculadas na Empresa, TÊM que ser tratadas como USO INTERNO caso não exista nenhum contrato ou acordo escrito especificando o contrário.

5.3. Reclassificação

Informação designada como CONFIDENCIAL, assim permanecerá até que o Proprietário ou outro usuário designado pelo Proprietário altere a classificação. A única exceção é quando a informação possui um rótulo ou especificação de data ou realização de um evento para automaticamente tornar-se PÚBLICA.

5.4. Divulgação, Transferência

Acordos de Não Divulgação e Sigilo da Informação (NDA) deverão ser estabelecidos formalmente entre a Empresa, seus colaboradores, fornecedores e outras empresas. É proibida a divulgação e transferência de informação CONFIDENCIAL para entidades externas, salvo se previamente e formalmente autorizada pelo Proprietário e existência de NDA assinado entre as partes.

O Proprietário de informação CONFIDENCIAL e RESTRITO tem que assegurar a existência deste Acordo antes da divulgação da informação para qualquer entidade externa, bem como os controles para salvaguarda destas informações.

O Proprietário da informação é responsável pela atenção e observância as medidas de segurança da informação para transferência de dados CONFIDENCIAL e RESTRITO para com as entidades externas. Cláusulas contratuais de responsabilidade solidária devem ser observadas e incluídas em relações onde a Empresa é controladora da informação e fará a transferência e compartilhamento com empresas que estarão na condição de operadores da informação. Atenção as cláusulas contratuais para LGPD 13709/2018.

5.5. Rótulos

5.5.1. Confidencial

Todo documento em papel ou eletrônico designado como CONFIDENCIAL deve possuir a palavra CONFIDENCIAL escrita em cada página exibida do documento,

preferencialmente no cabeçalho e/ou rodapé das páginas. Versões eletrônicas de documentos CONFIDENCIAIS devem apresentar o rótulo CONFIDENCIAL na primeira tela apresentada ao usuário, sempre que possível. Mídias magnéticas ou ópticas (discos magnéticos, fitas, DVDs, etc.) contendo informação CONFIDENCIAL devem possuir uma etiqueta com o rótulo CONFIDENCIAL.

5.5.2. Uso Interno

Todo documento em papel ou eletrônico designado como USO INTERNO deve possuir as palavras USO INTERNO escritas em cada página exibida do documento, preferencialmente no cabeçalho e rodapé das páginas. Versões eletrônicas de documentos de USO INTERNO devem apresentar o rótulo na primeira tela apresentada ao usuário, sempre que possível. Mídias magnéticas ou ópticas (discos magnéticos, fitas, DVDs, etc.) contendo informação de USO INTERNO têm que possuir uma etiqueta com o rótulo USO INTERNO.

Arquivos contendo registros de eventos de segurança (logs) por definição devem ser tratados e considerados como USO INTERNO. Estes arquivos são importantes para a correção de erros, auditorias internas, causas forenses, tratamento de incidentes de segurança e esforços relacionados.

5.5.3. Restrito

Todo documento em papel ou meio eletrônico designado como RESTRITO deve possuir a palavra RESTRITO escrita em cada página exibida do documento, preferencialmente no cabeçalho e rodapé das páginas. Versões eletrônicas de documentos RESTRITO devem apresentar o rótulo na primeira tela apresentada ao usuário, sempre que possível.

5.5.4. Público

Todo documento em papel ou meio eletrônico designado como PÚBLICO deve possuir a palavra PÚBLICO escrita em cada página exibida do documento, preferencialmente no cabeçalho e rodapé das páginas. Versões eletrônicas de documentos

PÚBLICO devem apresentar o rótulo na primeira tela apresentada ao usuário, sempre que possível.

5.5.5. Ausência de Rótulo

Informações em mídia eletrônica ou não, que não apresentarem os rótulos PÚBLICO, CONFIDENCIAL ou RESTRITO serão automaticamente considerados como USO INTERNO.

5.6. Divulgação Inadvertida

Usuários que trabalham com informações CONFIDENCIAL, RESTRITO e de USO INTERNO têm que estar sempre atentos para evitarem a divulgação inconsciente ou inadvertida para entidades não autorizadas a tratar a informação. O armazenamento das informações CONFIDENCIAL e RESTRITO, em locais seguros, bem como a utilização de proteção de tela, “logoff” automático, ou ações similares são necessárias quando usuários não autorizados estão presentes.

5.7. Uso Compartilhado

A comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e a Empresa, bem como entre entes privados e a Empresa requer cláusula contratual de proteção de dados pessoais e mecanismos de segurança para o tratamento destas informações em meio digital ou não. É responsabilidade da Diretoria de Operações recomendar e implementar os mecanismos de segurança para o tratamento. É responsabilidade da área Comercial e Jurídica a garantia de existência de cláusulas e mecanismos contratuais para proteção da Empresa.

5.8. Armazenamento

Quando não estiver em uso, a informação CONFIDENCIAL, RESTRITO e de USO INTERNO em papel ou arquivo eletrônico deverá estar armazenada em locais seguros ou que evitem a exposição, tais como: cofres apropriados, gavetas, armários com mecanismos

de tranca, diretórios da rede com níveis de permissão apropriados. Informação CONFIDENCIAL em arquivos eletrônicos localizada em computadores portáteis, ou mídias magnéticas portáteis devem estar codificada através dos métodos de criptografia aprovados pela área de Tecnologia da Informação.

É responsabilidade da área de Tecnologia da Informação definir os logs críticos e essenciais para o processo de tratamento de incidentes bem como a custódia dos mesmos. Os arquivos contendo registros de eventos de segurança devem ser armazenados de forma centralizada por pelo menos um (1) ano. Durante este período devem ser armazenados com segurança para não serem modificados e nem acessados por pessoas e serviços de TI não autorizados, considerando-se controles rígidos de acesso físico e lógico, bem como proteção contra perdas de informação

5.9. Destruição

Quando informações CONFIDENCIAL, RESTRITO, PÚBLICO e de USO INTERNO não são mais necessárias e seus requisitos legais e jurídicos já expiraram, deverão ser destruídas através de mecanismos que não permitam a reconstrução da informação, tais como “fragmentação” e incineração. As mídias magnéticas contendo as informações CONFIDENCIAL e RESTRITO devem ser formatadas fisicamente, pois a remoção simples (deletar) permite a recuperação da informação. Se a mídia não for reaproveitada a sua destruição faz-se mandatória.

A área de Tecnologia da Informação é responsável por manter um processo de descarte de informações e mídias que garanta o registro das operações de descarte.

6. GOVERNANÇA DE TECNOLOGIA

Todas as áreas da *Empresa* devem inteirar-se sobre melhores práticas de gestão de TI (ITIL, COBIT, SGSI, etc.) e suportar a área de Tecnologia da Informação com recursos e informações necessários ao bom desempenho dos processos de gestão.

É responsabilidade da área de Tecnologia da Informação estruturar, manter e divulgar processos e procedimentos de gestão de desempenho, capacidade, segurança da informação, requisição de serviços, operação de TI, gestão de mudanças, incidentes e problemas. Devendo apresentar indicadores de acompanhamento mensalmente e planos de correção de rumo no caso de desvios.

É responsabilidade da Diretoria de Operações realizar a gestão de riscos de ambiente e de processos relacionados à Segurança da Informação, visando mitigar a ocorrência de incidentes de disponibilidade e capacidade dos serviços de TI para serviços internos ou terceirizados.

A área de TI deve garantir que recursos de hardware e software, para suportar serviços críticos, tenham características básicas de contingência e redundância tais como:

- ✓ Fontes redundantes de energia, interfaces de rede múltiplas e conectadas em portas de rede alternativas;
- ✓ Processo de cópia de segurança (backup) estruturado, implantado e monitorado;
- ✓ Processo de gestão de falhas e desempenho estruturado, implantado e monitorado.

Bem como documentação da topologia e inventário de serviços críticos estruturada, implantada, monitorada, atualizada e divulgada para áreas da *Empresa* que requisitem estas informações como parte de sua operação.

Equipamentos, que armazenam e processam informações da *Empresa*, devem estar acondicionados em ambiente com controle de acesso físico, energia estabilizada e

condições de climatização adequadas aos requisitos técnicos de cada equipamento. Estes ambientes devem ser devidamente gerenciados e eventos que extrapolem condições mínimas ou requisitos de operação devem ser tratados como incidentes de disponibilidade, registrados e acompanhados.

Todas as alterações de configuração na infraestrutura de TI, segurança da informação e sistemas críticos da *Empresa* devem ser registradas e aprovadas através de processo específico para Gestão de Mudanças.

O processo de gestão de mudança deve assegurar no mínimo que os riscos operacionais foram identificados, que o processo de retomada/recuperação em caso de problemas existe e está validado pelos responsáveis pela gestão de mudança.

Todas as alterações de configuração na rede e sistemas críticos da *Empresa* requerem obrigatoriamente a realização de cópia de segurança das configurações antes e após a realização das mudanças. A equipe responsável pelas alterações também é responsável pela realização, classificação e armazenamento das cópias de segurança.

Mudanças emergenciais devem ser registradas, aprovadas e validadas após a sua execução em prazo mínimo possível.

7. RECURSOS DE TECNOLOGIA

7.1. Uso de Software

O uso de software é regulamentado por legislação específica e qualquer ato que a contrarie pode ser punido com os rigores da lei. É PROIBIDA a instalação de software não licenciado.

Existem softwares de livre distribuição (*freeware*, *open source*) e outros cuja aquisição e registro de licença são obrigatórios. Para os que requerem licença é necessário que a *Empresa* possua as devidas autorizações de uso para que estes possam ser instalados e

utilizados nas estações de trabalho, notebooks, equipamentos de rede e servidores da *Empresa*. É responsabilidade da área de Tecnologia da Informação manter inventário de hardware, software e controle de licenças atualizados.

Cuidado adicional deve ser prestado quanto a software de livre distribuição (*freeware, open source*), pois há grande probabilidade deste software carregar e inserir ameaças no ambiente de Tecnologia da *Empresa*. Assim, estes não podem ser utilizados em equipamentos da *Empresa* sem a devida homologação e aprovação pela área de TI em conjunto com a área de Segurança. Um processo de aprovação formal deve ser gerenciado pela área de TI com os devidos registros de liberação e restrição.

É responsabilidade da área de TI manter uma linha base com registro de software necessários ao desempenho das funções dos usuários.

Sempre que houver dúvida sobre a legalidade de uso de algum software a equipe de Tecnologia da Informação, responsável pelo inventário e administração de software, deve ser consultada a fim de fornecer os esclarecimentos pertinentes.

É vedada ao colaborador, a instalação e/ ou remoção de softwares nos equipamentos da *Empresa*, salvo através de autorização formal da equipe de Tecnologia da Informação.

A *Empresa* é proprietária de todos os direitos sobre patentes, direitos autorais, invenções ou outras propriedades intelectuais originadas e desenvolvidas por seus funcionários individualmente ou em grupo constituído por outros fornecedores de serviço externos, durante a vigência dos respectivos contratos de trabalho e prestação de serviço.

Todos os programas e documentos criados ou providos pelos funcionários em benefício da *Empresa* são considerados propriedade da mesma.

A *Empresa* é a custodiante legal das informações contidas em sistemas de informação sobre seu controle e/ou administração. A *Empresa* reserva-se o direito de acesso, uso e

poder de decisão sobre estas informações respeitando-se os requisitos vigentes nas leis federais, estaduais e municipais.

Sistemas que tratam informações sensíveis ao negócio e ou aqueles utilizados para prover acesso remoto ao ambiente devem prover mecanismos de geração de *logs* de acesso e trilha de auditoria visando a rastreabilidade de eventos.

7.2. Uso de Hardware

A Empresa considera como estações de trabalho quaisquer equipamentos de sua propriedade associados aos domínios e grupos de trabalho disponibilizados pela área de Tecnologia da Informação. Assim, desktops, laptops, notebooks, tablets e smartphones são considerados estações de trabalho. É responsabilidade da área de Tecnologia da Informação manter inventário atualizado de hardware e software.

Como equipamentos de rede a Empresa considera quaisquer equipamentos de sua propriedade associados ao transporte e segurança das informações entre as redes da Empresa, Internet, clientes, parceiros e fornecedores. Como exemplo de equipamentos de rede destacam-se: switches, roteadores, firewalls e equipamentos detectores de intrusos (IPS).

Todos os servidores e estações de trabalho devem ser obrigatoriamente associados aos domínios de controle definidos pela área de Tecnologia da Informação. É vedada a utilização de estações de trabalho que não estejam associadas a algum domínio de responsabilidade da Empresa; salvo em condições previamente aprovadas pela área de TI.

Os colaboradores/terceiros não devem utilizar computadores e periféricos pessoais, tais como discos externos, roteadores wireless, pendrive e impressoras, bem como software pessoal nas redes da Empresa, salvo com autorização prévia da equipe de Segurança da Informação.

Todos os servidores, estações de trabalho e equipamentos de rede do Empresa devem obrigatoriamente apresentar aviso de advertência (banner) no processo de logon/login para reiterar a propriedade da Empresa e uso somente por pessoas autorizadas.

Os servidores e equipamentos de rede críticos têm que estar em local fisicamente protegido, que possua condições de temperatura e umidade adequadas ao bom funcionamento destes. É responsabilidade da área de Tecnologia da Informação garantir estas condições. Para sites remotos, onde não exista infraestrutura física adequada é necessário considerar o uso de cofres e racks com controle de acesso.

Manutenções e intervenções realizadas por terceiros nos equipamentos de rede e servidores requerem acompanhamento obrigatório por pessoal especializado da Empresa e processo de Gestão de Mudança formalizado.

O transporte de equipamentos que em sua característica não possuem mobilidade natural (servidores, desktops, switches, roteadores) só poderá ser realizado através de liberação formal da área de Tecnologia da Informação, através de acondicionamento adequado, devido registro da autorização e do transporte.

É vedada a instalação de hardware sem prévia aprovação da área de Tecnologia da Informação e /ou projeto previamente aprovado.

A utilização de hardware por clientes, fornecedores e terceiros nas redes de propriedade da Empresa deverá ser habilitada somente após inspeção e verificação das condições de segurança do hardware. A área de Segurança da Informação é responsável por gerenciar este processo.

7.3. Acesso Remoto

O acesso remoto à(s) rede(s) da Empresa, ou seja, o acesso a partir de outra empresa deve ser realizado somente através de projeto elaborado e implementado pela área de Tecnologia da Informação ou através dos meios de VPN (Rede Privativa Virtual) já implantados e disponíveis contratualmente.

O acesso remoto para terceiros só pode ser feito por intermédio de projeto específico da área de Tecnologia da Informação, considerando que terão acesso controlado e apenas aos recursos e serviços de TI necessários para o exercício da atividade contratada.

O acesso remoto para colaboradores só pode ser realizado através de protocolos seguros e por meio de plataformas homologadas e validadas pela área de TI. É responsabilidade da área de TI disponibilizar, gerenciar e monitorar os acessos remotos.

Sempre que o colaborador estiver trabalhando remotamente deverá observar, com atenção redobrada, todos os cuidados descritos nesta política. Exemplos de ambientes remotos incluem, mas não se restringem a aeroportos, hotéis e redes sem fio de outras empresas.

Os equipamentos conectados à rede corporativa da Empresa não podem ser diretamente conectados a outras redes ou diretamente à Internet. Estas conexões devem ser feitas através de serviços seguros proporcionados por segurança de perímetro, redes privadas virtuais (VPN), proteção contra malware e outros, validados e homologados pela área de TI. Conexões de exceção devem ser aprovadas, configuradas e monitoradas pela área de SI.

7.4. Internet, E-Mail, Redes Sociais

a. Internet

A Internet é estrutura fundamental ao desempenho das atividades do negócio da Empresa e por ser uma rede com abrangência mundial, permite a conexão de entidades com todos os tipos de propósito. Em virtude disso, cuidados no seu uso devem ser considerados.

A Empresa reserva-se o direito de bloquear acesso a sites de conteúdo ilícito, sexo, atividades hacker e outros, sem aviso prévio e de forma automática.

A navegação na Internet propicia o acesso a qualquer tipo de conteúdo. Desde páginas idôneas, úteis e produtivas até as páginas de conteúdo impróprio. Desta forma é proibida a navegação em sites de conteúdo adulto e sites ilícitos, porque estes podem promover as atividades de hackers e improdutividade funcional. A Empresa promove o controle automático de navegação a sites não considerados apropriados ao desempenho das funções do colaborador.

A Empresa armazena os registros de navegação na Internet e poderá monitorá-los para avaliar atividades ilícitas, possíveis fraudes, comportamentos impróprios ao exercício da função definida em contrato de trabalho, bem como gerar estatísticas de uso e desempenho visando aprimorar seus serviços internos e externos.

Toda informação recebida a partir da Internet deve ser trabalhada com cautela. Colaboradores não estão autorizados a compartilhar e/ou salvar informações da Empresa em sites que provêm serviço de guarda de documentos (*file sharing*), salvo se autorizado formalmente pela a área de SI.

Sempre que possível a Empresa deverá utilizar-se de protocolos seguros criptográficos (HTTPS, IPSec) para transmissão de informações críticas e sensíveis via Internet. Cabe aos gestores avaliar a criticidade das informações e solicitar os recursos necessários para a área de TI.

b. E-mail

Colaboradores da Empresa que possuem contas de e-mail associadas ao desempenho de suas funções, devem utilizá-la somente para fins específicos desta função.

Contas de e-mail de uso pessoal não podem ser utilizadas para envio e recebimento de informações da Empresa.

A Empresa armazena os registros de uso de e-mail corporativo e poderá monitorá-los para avaliar atividades ilícitas, possíveis fraudes, comportamentos impróprios ao exercício da função definida em contrato de trabalho; bem como gerar estatísticas de uso e desempenho visando aprimorar seus serviços internos e externos.

Cuidados especiais devem ser prestados aos e-mails recebidos de origem desconhecida. A grande maioria são vetores que carregam vírus, armadilhas e outros códigos maliciosos. Nenhum anexo destes e-mails deve ser visualizado, baixado ou executado.

Ao redigir e-mails os colaboradores devem anexar somente os arquivos necessários. Tendo ciência que cada mensagem enviada, principalmente com anexos, consome consideráveis recursos da rede e do(s) servidor(es), além disso, consome o precioso tempo de quem a recebeu.

A comunicação via e-mail pode ser monitorada em casos de investigação relacionada a incidentes de segurança e fraudes, incluindo-se os e-mails pessoais acessados no e através do ambiente corporativo da Empresa.

E-mails não solicitados não devem ser respondidos, pois na maioria das vezes e-mails são enviados a uma infinidade de destinatários válidos ou não. O ato de responder o e-mail confirma ao agressor a validade do endereço de e-mail de destino, logo este e-mail poderá ser inserido em um cadastro que poderá ser comercializado para a prática do SPAM.

Não é permitido o uso do sistema de e-mail, cujos domínios pertencem a Empresa, ou aqueles administrados pela mesma, para o repasse de correntes, mensagens com conteúdo ilegal, racista, pornografia, religioso, preconceituoso, pejorativo ou ameaçador; bem como qualquer outro conteúdo inadequado ao ambiente corporativo e ou que possa trazer instabilidade de relacionamento pessoal e queda desempenho nos recursos de Tecnologia da Informação.

c. Redes Sociais

Funcionários devem ter especial atenção e assegurar que NÃO representam a Empresa em grupos de discussão na Internet, fóruns públicos e redes sociais; salvo com autorização expressa da Diretoria de Operações ou função expressamente atribuída através do cargo em vigência.

É vedada aos colaboradores a publicação de informações em qualquer rede social, salvo por área devidamente autorizada pela Empresa. Mesmo as áreas autorizadas devem ter especial atenção ao conteúdo, bem como a classificação da informação a qual para ser divulgada deverá previamente ser classificada como PÚBLICO (rótulo). Um processo de revisão e aprovação da comunicação deve ser devidamente registrado pelas áreas autorizadas.

A Empresa coíbe automaticamente o acesso a redes sociais, através de sua infraestrutura de TI, para colaboradores que NÃO tenham em sua função de trabalho as necessidades de acesso a redes sociais.

8. CONTROLE DE ACESSO LÓGICO E FÍSICO

Acesso às informações e sistemas da Empresa deve ser autorizado de acordo com as atividades atribuídas ao cargo ou função exercida pelo colaborador, cliente, fornecedor e terceiros. Os privilégios de acesso atribuídos para os mesmos devem ser revistos periodicamente pelos gerentes responsáveis.

Todo colaborador, cliente, fornecedor e terceiros deve possuir uma única identificação de usuário (User IDs, ou logon) e senha(s) (password) relacionada às suas atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço. Os privilégios e direitos de acesso devem ser atribuídos de acordo com as atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço. Colaborador, cliente, fornecedor e terceiros são responsáveis pelo uso e segurança de sua senha.

É proibido o empréstimo e compartilhamento de identificação de usuários e senhas associadas a qualquer tipo acesso às informações, sistemas e equipamentos da Empresa.

A construção de qualquer senha deve considerar o uso e composição entre caracteres alfabéticos, maiúsculos, minúsculos e números. Toda senha deve ter no mínimo 8 (oito) caracteres.

O colaborador/terceiro não poderá repetir nenhuma das últimas treze senhas já previamente utilizadas.

É responsabilidade da área de TI garantir configurações no(s) domínio(s) de controle para assegurar a construção de senhas fortes, aplicação de histórico e expiração automática das senhas.

Os colaboradores, clientes, fornecedores e terceiros devem escolher senhas fáceis de serem memorizadas, porém ao mesmo tempo difíceis de serem descobertas ou quebradas. Técnicas para esta escolha incluem:

- Combinar palavras de fácil memorização através de caracteres alfanuméricos, por exemplo: Carro01&branco, Ceu02+limpo;
- Combinar as primeiras letras das palavras que compõe o trecho de uma música ou frase;
- Combinar sinais de pontuação e números com uma palavra conhecida, por exemplo: Tempo1123x.

As senhas devem ser obrigatoriamente alteradas a cada 90 (noventa) dias. É responsabilidade da área de Tecnologia da Informação garantir as configurações necessárias nos sistemas para que as senhas expirem automaticamente. Informações de expiração da senha devem ser apresentadas no mínimo 5 (cinco) dias antes da expiração no processo de identificação (logon) do usuário.

Quando o colaborador/terceiro suspeitar de utilização indevida de sua(s) senha(s) deverá alterá-la(s) imediatamente e tratar a situação como um incidente de segurança reportando ao seu superior imediato o qual deverá comunicar a área de SI.

As senhas não devem ser armazenadas em forma compreensível (leitura) em código fonte, scripts, macros e papel para evitar a divulgação inadvertida e uso indevido destas.

Todas as estações de trabalho do Empresa devem utilizar proteção de tela (screensaver) previamente homologada pela área de Tecnologia da Informação e com ação automática de execução da proteção a partir de 10 (dez) minutos de inatividade das mesmas. É responsabilidade da área de Tecnologia da Informação configurar políticas nos diversos domínios para assegurar a utilização de proteção de tela. É vedada a qualquer usuário a remoção das configurações de proteção de tela da estação de trabalho.

O acesso às dependências físicas da Empresa deve ser controlado e gerenciado através de procedimento construído e mantido de acordo com a criticidade do ambiente. Mecanismos de dissuasão, controle, monitoramento de ambiente tais como vídeo vigilância, catracas, guardas e uso de crachá devem ser implementados e monitorados.

9. MALWARE

Malware (código maléfico), junção das palavras "***mal****icious*" e "*soft****ware***" é um software projetado para infiltrar e danificar um sistema de computador sem o consentimento do proprietário do sistema. A expressão constitui um termo geral utilizado pelos profissionais da área de Tecnologia da Informação para designar uma série de ameaças hostis, intrusivas e perigosas inseridas em algum código de computador.

O termo "vírus de computador" é o mais abrangente e utilizado para incluir todos os tipos de malware. Porém, existem também os chamados vermes, cavalos de Tróia, *spyware, keystroke loggers, ransomware* e etc.

Toda estação de trabalho e servidor deve possuir software antivírus instalado e atualizado automaticamente. É responsabilidade da área de Tecnologia da Informação assegurar o processo de controle de *malware* na *Empresa*.

É responsabilidade do colaborador comunicar a área de Tecnologia da Informação comportamentos associados a *malware* em suas estações de trabalho.

O uso de dispositivos do tipo “mídia removível” (*pendrives*) deve ser previamente autorizado formalmente e controles de segurança da informação devem ser empregados pela área de TI coibindo o uso não autorizado.

10. CRIPTOGRAFIA

Criptografia é a ciência ou arte de escrever mensagens em forma cifrada (codificada). É usada, dentre outras finalidades para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos; proteger o sigilo de comunicações pessoais e comerciais.

As comunicações e transferências de informações entre a Empresa, clientes, instituições financeiras, parceiros e fornecedores estratégicos devem ser realizadas através de redes privadas (VPN) utilizando-se de esquemas criptográficos previamente avaliados e aprovados pela área de Tecnologia da Informação.

As bases de dados contendo senhas devem estar criptografadas e o com respectivo controle adequado das chaves de criptografia. A responsabilidade pela gestão das ferramentas de criptografia, chaves e códigos fonte é da área de Tecnologia da Informação.

11. CÓPIAS DE SEGURANÇA E CONTINGÊNCIA

Todas as informações críticas de negócio da *Empresa* têm que possuir cópia de segurança (*backup*) realizada de acordo com planejamento associado a criticidade da informação para o negócio.

É responsabilidade da área de Tecnologia da Informação providenciar os recursos físicos e lógicos para armazenamento e restauração das cópias de segurança. Também deve assegurar que cópias estejam presentes em locais físicos diferentes do local de origem da informação e devidamente acondicionadas.

É responsabilidade do Proprietário da informação definir os requisitos mínimos de salvaguarda da informação, tais como tempo de retenção e periodicidade da cópia.

As cópias de segurança devem ser verificadas sistemicamente para assegurar o processo de restauração. É responsabilidade da área de Tecnologia da Informação prover os recursos necessários e realizar a restauração das cópias de segurança regularmente.

O processo de restauração das informações críticas armazenadas em cópias de segurança é responsabilidade exclusiva da área de Tecnologia da Informação. A restauração da informação deverá ser solicitada formalmente a esta área pelo Proprietário da informação.

Informações críticas ao negócio da *Empresa* presentes em estações de trabalho e equipamentos móveis, tais como *laptops*, celulares e *tablets* também devem estar presentes em diretórios de rede para que o processo de cópia de segurança seja assegurado. É responsabilidade dos colaboradores garantir que estas informações estejam em diretórios de rede.

O processo de desenvolvimento e aquisição de novos sistemas deve considerar as melhores práticas de segurança da informação. Estas práticas devem ser atualizadas, discutidas e disseminadas na *Empresa*. É responsabilidade da área de Tecnologia da Informação garantir a disseminação e aplicação de melhores práticas para desenvolvimento seguro.

Sem acordo, ou direitos autorais previamente expressos de outra forma, qualquer programa, sistema e/ou documentação gerada ou provida por colaboradores, consultores ou contratados, em benefício da *Empresa*, será de propriedade da mesma. Os gestores são responsáveis por assegurar esta propriedade através de assinatura de NDAs, cláusulas contratuais e outros instrumentos que tratem desta garantia.

Aquisição e implantação de novos sistemas devem considerar a verificação de requisitos mínimos de segurança da informação. A definição destes requisitos é responsabilidade da área de SI, a verificação do emprego e uso adequado destes requisitos é da área de TI.

A Política de Corporativa Segurança da Informação deve fazer parte como anexo de qualquer contrato envolvendo a aquisição e uso de novos sistemas. O fornecedor proponente deverá atender as condições estabelecidas neste documento para garantir a integridade, disponibilidade e confidencialidade das informações.

É mandatória a comprovação de melhores práticas de desenvolvimento seguro, realização de análise de vulnerabilidades e mapa de riscos de Segurança da Informação, para as soluções e sistemas a serem adquiridos ou desenvolvidos externamente. Os sistemas devem apresentar recursos para controle de acesso lógico segregado e robusto, bem como capacidade para a execução e verificação de trilhas de auditoria. É responsabilidade da área de Tecnologia da Informação classificar os fornecedores e apresentar a Diretoria de Operações matriz de decisão técnica com aspectos, requisitos de SI e classificação de risco para o mesmo.

13. GESTÃO DE RISCOS DE SI E CONTINUIDADE

A área Tecnologia da Informação é responsável pela gestão de incidentes de Segurança da Informação, gerenciar e manter seus registros, bem como aplicar melhores práticas para contenção e resolução de causa raiz.

É responsabilidade da área Riscos gerenciar os riscos relacionados à Segurança da Informação, comunicar possíveis alterações no cenário e impactos imediatos, bem como apresentá-los trimestralmente a Diretoria de Operações e manter registros das decisões aplicadas. A realização de análise de vulnerabilidades e testes de invasão periódicos deve ser prática de responsabilidade da área SI, informada e acompanhada pela área de Auditoria Interna.

É responsabilidade da área de Tecnologia da Informação manter e gerenciar um programa de gestão de vulnerabilidades de acordo com as melhores práticas de mercado e alinhado a gestão de risco de SI da *Empresa*.

É responsabilidade da área de TI avaliar, manter e disponibilizar contingência de recursos críticos para a continuidade do negócio bem como aqueles necessários a continuidade da gestão de SI na ocorrência de eventos adversos. Servidores, equipamentos de rede e segurança críticos ao negócio devem ser adquiridos e implementados com capacidades próprias de contingência tais como fontes redundantes, placas de rede alternativas, memória com correção de erros, processadores duplos, placas controladoras e sistemas em alta disponibilidade. No caso da contratação de serviços de infraestrutura de TI em nuvem os mesmos requisitos são aplicáveis. A arquitetura de processamento para serviços críticos deve ser analisada e validada quanto aos requisitos de contingência e continuidade.

A continuidade do negócio é responsabilidade da Diretoria de Operações envolvendo a análise de riscos e definição de estratégias para mitigar os riscos. Uma política e/ou

procedimento específico para a gestão de continuidade e calcado em melhores práticas deve ser definido, implementado e testado regularmente pela *Empresa*. Evidências dos testes deve ser mantida para assegurar requisitos de conformidade com órgão regulador.

14. SEGURANÇA CIBERNÉTICA

Serviços críticos e essências aos negócios da *Empresa* devem ser protegidos contra ataques cibernéticos de interrupção de serviços tais como DDoS (Ataques de Interrupção de Serviços Distribuídos), ransomware, envenenamento de DNS, divulgação de dados pessoais e outros. É responsabilidade da área de TI em conjunto com a área de Risco determinar as possíveis ameaças, definir e adotar medidas de proteção tais como a contratação de links seguros, serviços de gestão de conteúdo e etc.

A conformidade com requisitos legais e contratuais é responsabilidade de todos os colaboradores da *Empresa*. Os gestores devem identificar e observar a legislação aplicável à *Empresa*, garantindo a adequação contratual e observância das diretrizes de Segurança da Informação desta Política.

15. CONFORMIDADE

A conformidade com requisitos legais e contratuais é responsabilidade de todos os colaboradores da *Empresa*. Os gestores devem identificar e observar a legislação aplicável à *Empresa*, garantindo a adequação contratual e observância das diretrizes de Segurança da Informação desta Política.

Em especial os requisitos da Lei Geral de Proteção de Dados (LGPD 13709/2018) devem ser observados por todos os colaboradores visando preservar a privacidade do Titular

dos Dados pessoais. Informações de Identificação Pessoal ou Dados Pessoais" incluem qualquer informação que possa ser associada ou rastreada a qualquer indivíduo, incluindo o nome, endereço, número de telefone, endereço de e-mail, informações de cartão de crédito, número de CPF, RG, sexo, preferências religiosas, partidárias ou outras informações factuais específicas semelhantes, independentemente da mídia na qual tais informações são armazenadas (por exemplo, em papel ou eletronicamente) e incluem as informações que são geradas, coletadas, armazenadas ou obtidas como parte do exercício da função do empregado no Contrato de Trabalho e negócios da empresa, incluindo dados transacionais e outros referentes aos clientes. O funcionário cumprirá todas as leis e regulamentos aplicáveis de privacidade (LGPD 13709/2018) e outras leis relacionadas à proteção, coleta, uso e distribuição de Informações Pessoais Identificáveis. Em nenhum caso, o funcionário poderá vender ou transferir informações pessoalmente identificáveis a terceiros, ou fornecer acesso a elas sem a autorização formal e prévia. A confidencialidade e sigilo de Dados Pessoais devem ser observados, preservados e garantidos por todos os colaboradores da *Empresa*. A área de TI é responsável por propiciar mecanismos de proteção condizentes com a criticidade da informação e requerer estes aspectos de provedores de serviços e sistemas. Suspeitas de violação de Dados Pessoais devem ser comunicadas ao superior imediato e/ou através de contato com a ouvidoria (0800 095 6702) e/ou envio de e-mail para privacy@zemafinanceira.com.

Relações contratuais com diretrizes de Segurança da Informação inferiores às contidas nesta Política devem ser evitadas e caso não haja opção, devem ser analisadas quanto ao risco e aprovadas formalmente pela Diretoria de Operações. É responsabilidade da área de Controle de Riscos Corporativos garantir este processo.

Os gestores da organização devem observar e garantir direitos de propriedade intelectual de terceiros e da própria *Empresa*.

Enquanto durar a relação contratual as patentes, invenções, direitos autorais, ou outras propriedades intelectuais tais como: estudos, projetos, relatórios e demais dados

desenvolvidos pelo colaborador são de direito exclusivo da *Empresa* que poderá registrá-los nos órgãos competentes e utilizá-los ou cedê-los sem qualquer restrição ou custo adicional.

A contratação de serviços de terceiros para tratamento de informações da *Empresa* que caracterizem processamento e armazenamento em nuvem, deve considerar os requisitos de adequação a legislação e regulação vigentes, em especial aos requisitos da Resolução 4658 BACEN (Banco Central do Brasil). É responsabilidade da área de Tecnologia da Informação manter e gerenciar procedimento contendo os requisitos. É responsabilidade da área de Controle de Riscos Corporativos avaliar os riscos previamente a contratação.

A análise crítica e independente do processo de gestão de Segurança da Informação deve ser realizada pelo menos uma vez ao ano através da contratação de auditoria especializada. A área de Auditoria Interna é responsável pela garantia de isenção neste processo devendo acompanhar e zelar pela execução das correções de acordo com o risco para o negócio. A alta direção da *Empresa* é responsável por garantir recursos orçamentários, técnicos e humanos para a área de Auditoria Interna.

16. REFERÊNCIAS

Código de Ética e Conduta

Procedimento de Gestão de Continuidade de Negócios

Normas ABNT NBR ISSO/IEC 27001:2013 e 27002:2013

Lei Geral de Proteção de Dados 13709/2018

Resolução 4658 BACEN

17. GLOSSÁRIO

Acesso remoto – Acesso no qual o usuário utiliza-se de algum mecanismo, rede ou ligação telefônica, para obter acesso a um sistema fisicamente localizado em outro local. Exemplos incluem um acesso via VPN, através de linha discada, banda larga.

Access Point (AP) - Ponto de acesso sem fio, dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Anonimização - utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Antivírus - Programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

Atacante - Pessoa responsável pela realização de um ataque. Veja também Ataque.

Ataque - Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques quaisquer tentativas de negação de serviço.

Backdoor - Código malicioso instalado em um computador, geralmente sem o consentimento do usuário. O *backdoor* provê uma porta dos fundos por onde um hacker pode obter acesso oportunamente.

Backup - Processo que objetiva manter as informações a salvo de problemas nos meios de armazenamento, é feita uma cópia de segurança que pode ser restaurada caso haja necessidade.

Banco de dados - conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Banner - É uma forma comum na internet, em que as empresas utilizam para divulgar informações de seus sistemas para seus colaboradores através de um “anuncio” na tela.

Cavalo de Tróia - Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar

funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Código malicioso - Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms, bots*, cavalos de Tróia, *rootkits*, etc.

Consentimento - Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Criptografia - Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

Cracker - Os crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. Em alguns casos, o termo “Pirata Virtual” é usado como sinônimo para cracker.

Dado pessoal - informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DDoS - *Distributed Denial of Service*. Tipo de ataque cibernético onde os recursos são exauridos em sua capacidade de forma a se impedir o acesso ou uso final pelo cliente.

Desktop - Veja Estação de trabalho.

Dispositivo Móvel - Designado popularmente em inglês por handheld é um computador de bolso habitualmente equipado com um pequeno monitor e um teclado em miniatura (entrada de informação). No caso dos PDAs, a saída de informação e a entrada combinam-se em um monitor tipo *touch screen*. Os dispositivos móveis mais comuns são: Smartphones, PDA, Console portátil, tablets, notebooks e televisão portátil.

DNS - *Domain Name System* – Serviço de Internet que transforma a URL em um endereço localizável. Responsável por descodificar os nomes dos domínios dos sites que as pessoas digitam nos navegadores web em números IP.

E-mail - Veja Endereço eletrônico

Endereço eletrônico - É um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação

Endereço IP - Este endereço é um número único para cada computador conectado à Internet, composto por uma sequência de 4 números que variam de 0 até 255, separados por ".". Por exemplo: 192.168.34.25.

Engenharia social - Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Estação de trabalho - Nome genérico dado a computadores, situados, em termos de potência de cálculo, entre o computador pessoal e o computador de grande porte.

Feedback - O significado de feedback é utilizado em teorias da Administração de Empresas, quando é dado um parecer sobre uma pessoa ou grupo de pessoas na realização de um trabalho com o intuito de avaliar o seu desempenho. É uma ação que revela os pontos positivos e negativos do trabalho executado tendo em vista a melhoria do mesmo.

Firewall - Dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores.

Freeware - Software de livre distribuição, não é necessário que sejam adquiridas licenças para que tal tipo de software seja usado.

FTP - File Transfer Protocol, é um protocolo de transferência de arquivos muito utilizado na Internet. Este protocolo não tem mecanismos de segurança em sua implementação.

Hacker - Indivíduo com elevados conhecimentos de computação e segurança que os utiliza com propósitos de identificar e publicar falhas relacionadas à segurança em aplicativos, sistemas e equipamentos.

Hardware - Parte física do computador, equipamento de rede e outros.

Invasão – Ataque que resulte no acesso, manipulação ou destruição de informações em um computador.

Invasor - Pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão.

IP - Veja Endereço IP.

Laptop - Veja Estação de trabalho.

Log - Registro de atividades gerado por programas de computador. No caso de logs relativos a incidentes de segurança, eles normalmente são gerados por firewalls ou por IDSs.

Malware - Do Inglês *malicious* software (software malicioso). Veja Código malicioso.

Mídia Removível - É qualquer meio de armazenamento que pode facilmente ser conectado e desconectado de computadores, exemplos incluem disquetes, CD's, DVD`s, ZipDrives, PenDrives, fitas magnéticas e outros.

Mídia Magnética ou ópticas - é uma mídia de armazenamento não-volátil que consiste em uma fita plástica coberta de material magnetizável. A fita pode ser utilizada para registro de informações analógicas ou digitais, incluindo áudio, vídeo e dados de computador.

Notebook - Veja Estação de trabalho.

Operador - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Password - Veja Senha.

PCN – Plano de Continuidade de Negócio – Conjunto de medidas e recursos para a empresa continuar operando o negócio no caso de eventos adversos (desastres).

Phishing - Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Ransomware – Tipo de vírus que criptografa as informações do computador e exige resgate para recuperação das mesmas pago em moeda virtual.

Rede sem fio – (*Wireless*) Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

Rootkits – Conjunto de código malicioso que substitui o código original e executa ações programadas pelo agressor, escondendo-se da detecção padrão executada através de comandos do sistema operacional.

Scam - Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan - Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja Scanner.

Scanner - Programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Screensaver - Imagem animada que é ativada quando nenhuma atividade no computador do usuário for detectada por um determinado tempo.

Senha - Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

Servidor - Sistema de computação que fornece serviços a uma rede de computadores. Esses serviços podem ser de natureza diversa, por exemplo, arquivos e correio eletrônico

Software - Um programa de computador é composto por uma seqüência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual. Em um programa correto e funcional, essa sequência segue padrões específicos que resultam em um comportamento desejado

Spam - Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do *Inglês Unsolicited Commercial* E-mail).

Spammer - Pessoa que envia spam.

Spyware - Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Titular - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento - toda operação realizada com as informações, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Touch screen – Sensível e responsivo ao toque.

Trojan Horse - Veja Cavalo de Tróia.

UCE - Do inglês *Unsolicited Commercial* E-mail. Termo usado para se referir aos e-mails comerciais não solicitados.

URL - Do Inglês *Universal Resource Locator*. URL – é a especificação de endereços de páginas web, como por exemplo: www.zemafinanceira.com.br

Uso compartilhado de dados - comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Verme - Um tipo especial de vírus que não depende de estímulo para ser ativado, geralmente usa a rede para novas infecções.

Vírus - Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

VPN - *Virtual Private Network* é uma rede que provê uma conexão remota de forma segura. Muito utilizada por usuários que estão fora das dependências da empresa e para a interconexão de várias unidades de uma empresa.

Vulnerabilidade - Falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Wi-Fi - Do Inglês *Wireless Fidelity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless - Veja Rede sem fio.

Worms - Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

18. HISTÓRICO DE REVISÕES

nº versão	Solicitante	Data Revisão	Aprovação
01	Controle de Riscos Corporativos	12/02/2019	Diretoria Executiva
02	Controle de Riscos Corporativos	03/12/2020	Diretoria Executiva

19. APROVAÇÃO

_____

Juliano Antônio de Oliveira
Diretor Presidente

_____

José Joaquim de Oliveira Junior
Diretor Adm. / Financeiro

_____

Maria Virgínia Gomes Moreira
Diretora de Operações

Autenticação da assinatura

Documento: f3a807b7-81b9-4803-b4df-c01748316b2f

Envelope: 27c021b1-2941-492f-b709-94663945080e

DOCUMENTO:

Nome do arquivo:	política_de_segurança_informação.pdf
Número de páginas:	

EMISSOR:

Nome do emissor:	Carlos Eduardo
Razão Social:	ELETROZEMA
CNPJ:	26.404.731/0001-96
Data e hora de envio (UTC):	03/12/2020 19:47:59

1º ASSINANTE:

Nome completo:	Juliano Antonio de Oliveira
CPF:	93996993668
Número do celular:	5534988710673
E-mail:	juliano@zema.com
Tipo de assinatura:	Própria
Dispositivo da assinatura:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Geolocalização da assinatura:	-19.5835754640998,-46.9564051120721
Assinado em (UTC):	08/12/2020 20:35:17
Método de autenticação:	SMS + E-mail + CPF

2º ASSINANTE:

Nome completo:	José Joaquim de Oliveira Junior
CPF:	34833941848
Número do celular:	5534991565667
E-mail:	junior.oliveira@zemafinanceira.com
Tipo de assinatura:	Própria
Dispositivo da assinatura:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Geolocalização da assinatura:	-18.512178,-44.5550308
Assinado em (UTC):	07/12/2020 20:52:04
Método de autenticação:	SMS + E-mail + CPF

3º ASSINANTE:

Nome completo:	Maria Virgínia Gomes Moreira

CPF:	45636036604
Número do celular:	5531999941000
E-mail:	virginia.moreira@zemafinanceira.com
Tipo de assinatura:	Própria
Dispositivo da assinatura:	Mozilla/5.0 (iPhone; CPU iPhone OS 14_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.1 Mobile/15E148 Safari/604.1
Geolocalização da assinatura:	Geolocalização não compartilhada pelo usuário
Assinado em (UTC):	03/12/2020 19:55:15
Método de autenticação:	SMS + E-mail + CPF

43 páginas