Política Corporativa

Segurança da Informação

SUMÁRIO

1. OBJETIVO

Estabelecer diretrizes que permitam aos colaboradores da Serede, fornecedores, partes relacionadas ou qualquer pessoa que faça uso, tenha acesso a informação ou sistema da empresa a seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades do 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.

Preservar as informações da Serede quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. CAMPO DE APLICAÇÃO

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da Serede, e se aplicam à informação em qualquer meio ou suporte. Esta política dá 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.

É também obrigação de cada Colaborador se manter atualizado em relação a PSI (Política de Segurança da Informação) e as normas relacionadas, buscando orientação do seu gestor ou da Gerência de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Serede pertence à instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

3. DEFINIÇÕES

- **Auditoria:** Processo de coleta e revisão de informações de acesso de pessoas a ambientes físicos e lógicos, a fim de garantir a identificação da ocorrência de falhas, fraudes ou incidentes e a adequação de procedimentos e permissões.

- **Autenticação:** Processo de confirmação da identificação, baseado em fatores biométricos (o que você é, ex.: impressão digital), na posse de dispositivos (o que você tem, ex.: cartão com código de barras) ou no conhecimento de alguma informação (o que você sabe, ex.: senha);

- **Autorização:** Pode ser entendido como uma ação que visa permitir ou negar acesso a algum sistema ou espaço físico;

- **Colaborador:** Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou em regime de exceção que exerça alguma atividade dentro ou fora da instituição.

- **Dispositivos móveis:** Entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Tecnologia de Informação e Comunicação, como: notebooks, smartphones e pendrives.

- **Custódia**: Lugar seguro onde se guarda alguém ou alguma coisa; ato de guardar; vigilância, guarda, proteção;

- **Custodiante:** Responsável pela custódia;

- **Custodiante de informações:** Área responsável pelo sistema, ou responsável pela guarda, evolução e manutenção de um ativo de informação.

- **Gestor da informação:** Área responsável pelo processo que coleta/processa e/ou gera dados de negócio e por esse motivo é responsável pela classificação da informação.

- **Informação:** todo componente (seja humano, tecnológico, software, entre outros) que armazena, processa ou transmite dados e informações, ou a própria informação;

- **Identificação:** Processo de reconhecimento da identidade de um indivíduo (ex.: apresentação da carteira de identidade na recepção; informação de nome de usuário no acesso a um sistema);

- **Segurança da Informação:** Conjunto de ações e controles com vista a garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

- **Microsoft Teams**: É uma plataforma unificada de comunicação e colaboração que combina Instant Messaging (mensagens instantâneas/chat), videoconferências, armazenamento de arquivos (incluindo colaboração em arquivos) e integração de aplicativos no local de trabalho. O serviço se integra ao pacote de produtividade Office 365 e apresenta

extensões que podem ser integradas a produtos que não são da Microsoft.

- **Home Office:** Regime de trabalho em que uma pessoa exerce sua função remotamente.

- **DMZ**: Abreviação de uma zona desmilitarizada, é uma rede de perímetro que permite que as organizações protejam suas redes internas.

- **AWS:** Amazon Web Services é uma plataforma de serviços de computação em nuvem, que formam uma plataforma de computação na nuvem oferecida pela Amazon.com.

3.1. REFERÊNCIAS

- [POL]0181.01 - Backup e Retenção de Dados

4. CONTEÚDO

4.1. Dos colaboradores em geral

4.1.1. Entende-se por colaborador toda e qualquer pessoa física, contratada 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 na Serede e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas;

4.1.2. O colaborador, ao aceitar o Código de Ética da empresa, estará dando aceite também a esta Política de Segurança da Informação e assumindo o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Serede;

4.1.3. É vedada ao colaborador a utilização de dispositivos móveis não autorizados pela empresa;

O acesso, armazenamento e distribuição de informações da empresa só devem ocorrer no estrito cumprimento das atividades profissionais atribuídas ao colaborador pela Serede e utilizando dispositivos autorizados pela empresa;

4.1.4. Colaboradores que estejam no programa Home Office deverão ler e aceitar eletronicamente o termo aditivo de trabalho Home Office.

A participação no Projeto Home Office acarreta aos colaboradores aceitação total e irrestrita

de todos os itens do regulamento.

4.2. Dos Gestores de Pessoas e/ou Processos

4.2.1. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

4.2.2. 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.

4.2.3. Exigir dos colaboradores a assinatura do Código de Ética ou aceite eletrônico, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Serede.

4.2.4. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a PSI.

4.3. Da Área de Tecnologia da Informação

4.3.1. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

4.3.2. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

4.3.3. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI e pelas Normas de Segurança da Informação complementares.

4.3.4. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso apenas será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

4.3.5. Segregar as funções administrativa e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs das suas próprias ações.

4.3.6. Garantir segurança especial para sistemas com acesso publicado, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

4.3.7. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Serede.

4.3.8. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

4.3.9. O gerente da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

4.3.10. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário serão removidas antes de disponibilizar o ativo para outro usuário.

4.3.11. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

4.3.12. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de colaboradores serão de responsabilidade do próprio colaborador;
- Os usuários (logins) de terceiros serão de responsabilidade do gerente da área contratante.

4.3.13. Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

4.3.14. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

4.3.15. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

4.3.16. Realizar auditorias periódicas de configurações técnicas e análise de riscos.

4.3.17. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

4.3.18. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

4.3.19. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

4.3.20. Monitorar o ambiente de TI, gerando indicadores e históricos de:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos da Serede;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos utilizados na Serede;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

4.3.21. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esse sistema poderá ser usada para identificar usuários e respectivos acessos efetivados bem como material manipulado.

4.3.22. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior).

4.3.23. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

4.4. Da Área de Segurança da Informação

4.4.1. Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

4.4.2. Ser responsável por propor diretrizes de segurança que deverão ser seguidas pela área de desenvolvimento interno.

4.4.3. Ser responsável pela avaliação técnica, no que diz respeito à segurança, em todo processo de aquisição de software de terceiros.

4.4.4. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Serede.

4.4.5. Buscar alinhamento com as estruturas corporativas da instituição.

4.4.6. Apoiar a avaliação e adequação de controles específicos de segurança.

4.4.7. Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da Serede, mediante campanhas, treinamentos e outros meios de endomarketing.

4.5. Requisitos da Política de Segurança da Informação

4.5.1. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da Serede a fim de que a política seja cumprida dentro e fora da empresa.

4.5.2. Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada.

4.5.3. Deverá constar nos contratos da Serede o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

4.5.4. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.

4.5.5. Incidentes que afetem a segurança da informação deverão ser comunicados à Gerência de Segurança Corporativa.

4.5.6. Um plano de contingência e a continuidade dos principais sistemas e serviços deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de

confidencialidade, integridade e disponibilidade dos ativos de informação.

4.5.7. Deverão ser criados e instituídos controles apropriados ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela Serede ou por terceiros.

4.5.8. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

4.5.9. A Serede exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4.5.10. Esta PSI será implementada na Serede por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

4.5.11. O não cumprimento dos requisitos previstos nesta PSI e dos procedimentos de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

4.6. Compromisso e penalidades

4.6.1. Todas as garantias necessárias ao cumprimento da PSI serão estabelecidas formalmente com os colaboradores, fornecedores e parceiros comerciais da Serede, com o apoio dos instrumentos devidos. O nosso compromisso é essencial.

4.6.2. O descumprimento da PSI acarretará a aplicação das sanções previstas em lei, nos regulamentos internos ou nas disposições contratuais.

4.7. Correio eletrônico

4.7.1. O objetivo desta norma é informar aos colaboradores da Serede quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

4.7.2. O uso do correio eletrônico da Serede é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição.

4.7.3. Acrescenta-se que é proibido aos colaboradores o uso do correio eletrônico da Serede para:

4.7.3.1. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

4.7.3.2. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

4.7.3.3. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Serede ou suas unidades vulneráveis a ações civis ou criminais;

4.7.3.4. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

4.7.3.5. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

4.7.3.6. Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da Serede estiver sujeita a algum tipo de investigação;

4.7.3.7. Produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Serede;
- Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas; ou tenha conteúdo considerado impróprio, obsceno ou ilegal;

- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

4.7.4. As mensagens de correio eletrônico sempre deverão incluir assinatura com o formato definido pela gerência de Comunicação Interna:

- Nome do(a) Colaborador(a)
- Gerência ou departamento
- Diretoria
- Endereço completo
- Telefone (s)
- Correio eletrônico

4.8. Internet

4.8.1. Todas as regras atuais da Serede visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação;

4.8.2. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

4.8.3. A Serede, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo

gerente. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

4.8.4. Somente os colaboradores que estão devidamente autorizados a falar em nome da Serede para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista online, podcast, seja por documento físico, entre outros. Sempre que necessário, o colaborador deverá solicitar orientação ao seu gestor para que ele informe o procedimento correto.

4.8.5. Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

4.8.6. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

4.8.7. Apenas os colaboradores da Gerência de Tecnologia da Informação estão autorizados a fazer download (baixa) de aplicativos/programas da internet. Estes programas devem ser diretamente ligados às atividades da Serede e deverão ser devidamente registrados e licenciados.

4.8.8. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

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

4.8.10. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gerentes.

4.8.11. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado para a Serede ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

4.8.12. Os colaboradores não poderão utilizar os recursos da Serede para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

4.9. Identificação

4.9.1. Os dispositivos de identificação e senhas protegem a identidade do Colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Serede e/ou terceiros.

4.9.2. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

4.9.3. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

4.9.4. Todos os dispositivos de identificação utilizados na Serede, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

4.9.5. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

4.9.6. Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

4.9.7. Se existir login de uso compartilhado por mais de um Colaborador, a responsabilidade perante a Serede e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gerente de uso compartilhado, ele deverá ser responsabilizado.

4.9.8. É proibido o compartilhamento de login para funções de administração de sistemas.

4.9.9. O Departamento de Recursos Humanos da Serede é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

4.9.10. A Gerência de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores na instituição.

4.9.11. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários,

empregados regulares, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

4.9.12. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %).

4.9.13. Todo sistema desenvolvido na empresa, seja com recursos próprios ou utilizando-se mão de obra terceirizada, deve se conectar ao sistema Identidade (ou o que vier a substitui-lo) para realização de autenticação de usuário e senha, de forma que sejam padronizadas em lugar único as políticas de senha dos sistemas.

4.9.14. Quando um sistema for adquirido de terceiro, deve-se, preferencialmente:

- Observar se o sistema a ser adquirido pode ser integrado ao sistema de identidade;
- Caso não seja possível, o sistema deve possuir a capacidade de exigir do usuário que a senha atenda aos requisitos desta PSI;
- Caso o item anterior não possa ser atendido, deve-se exigir em contrato a adequação da ferramenta a ser adquirida;
- Caso nenhuma das condições acima possam ser atendidas, o gerente e o diretor da área de TI e da área usuárias devem ser avisados e concederem autorização específica para contratação/aquisição do sistema. Esta autorização deverá ser armazenada para fins de auditoria juntamente com o contrato.

4.9.14.1. Na entrada em vigor desta PSI, no prazo de 6 meses, os sistemas adquiridos de terceiros e que não atendem a atual política, caso não possam ser substituídos, devem ser listados para que seja dada ciência aos gerentes e diretores envolvidos e para que seja solicitada uma autorização para a continuidade de uso destes sistemas. Esta autorização deve ser armazenada pela gerencia em TI em lugar seguro e apresentada sempre que necessário aos auditores, sejam internos ou externos.

4.9.15. Para todos os sistemas da empresa, a solicitação de criação ou alteração de perfil para um novo usuário deve ser realizada via ferramenta Atende Chamados, anexando ao chamado a aprovação do gerente do usuário a ser criado;

4.9.15.1. Para os sistemas onde haja perfis ou funções fortemente associadas às atividades de

uma área específica, deverá ser nomeado nesta área um gerente responsável por autorizar a criação ou alteração de perfil de um usuário nesta ferramenta. Essa autorização deverá ser anexada ao chamado no Service Desk para que ele possa ser executado. Por exemplo, para acesso ao módulo de contabilidade do sistema SAP, deve ser solicitada a autorização do gerente de contabilidade; para concessão de acesso à função de criação de pedido de compra, deve ser solicitada a autorização do gerente de suprimentos.

4.9.15.2. Para os sistemas que se encaixarem no item 6.9.15.1, o atendente do chamado deverá informar ao colaborador sobre a necessidade de aprovação do gerente do perfil/função.

4.9.15.3. Todo acesso concedido ao sistema SAP que não estiver em uso por mais de 60 dias deverá ser bloqueado pela TI. Caso o usuário necessite novamente do acesso, deverá fazer nova solicitação via Service Desk, conforme item 6.9.15.

4.9.16. Para a criação de usuários na ferramenta SAP, além de atender o item 6.9.15 e 6.9.15.1, deverá também ser anexada a autorização do gerente de TI ou na sua ausência, do coordenador de TI.

4.9.16.1. Caso o usuário para o qual se deseja conceder acesso ao SAP seja de empresa terceirizada, o gerente do contrato ou gerente responsável pelas atividades da empresa terceirizada na Serede deverá abrir um chamado na ferramenta Service Desk. No chamado deverá conter além das informações do usuário a ser criado, as funções que serão atribuídas a ele e a justificativa para que o acesso seja concedido. Esta autorização não substitui a necessidade de autorização também do gerente de TI ou na sua ausência, do coordenador de TI.

4.9.16.2. O prazo máximo de concessão de acesso a usuários terceiros no SAP é de 90 dias, podendo ser prorrogada quantas vezes forem necessárias mediante a abertura de solicitação na ferramenta de Service Desk, seguindo a regra estabelecida no item 6.9.16.1.

4.9.17. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

4.9.18. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.) e devem ser evitadas informações pessoais, como próprio nome, e combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

4.9.19. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

4.9.20. A periodicidade máxima para troca das senhas dos sistemas é de 45 (quarenta e cinco) dias, não podendo ser repetidas as 6 (seis) últimas senhas. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

4.9.21. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

4.9.22. Caso o Colaborador esqueça sua senha, ele deverá abrir um chamado via Service Desk solicitando a alteração da senha.

4.9.23. Caso o colaborador entre de férias, ou seja, afastado, ele poderá transferir permissões de acesso para outro colaborador, através de abertura de chamado. Em nenhuma hipótese deverá ser permitido o compartilhamento de usuário/senha.

4.9.24. No caso de afastamento por férias ou outros motivos, o Gerente ou Diretor deverá, através de abertura de chamado, nomear outro Gerente ou Diretor para substituí-lo nas devidas aprovações, informando o período de afastamento. Esta delegação deverá seguir os critérios definidos na Política de Aprovações e Delegações de Alçadas (PADA), assim devem ser observadas as delegações pertinentes ao cargo originário a outro de mesmo nível ou superior, nunca inferior. A permissão será revogada automaticamente pelo sistema após o período do afastamento.

4.9.25. No caso de afastamento por férias ou outros motivos, o acesso ao SAP será automaticamente bloqueado. O acesso será liberado de forma automática após o término do período de afastamento.

4.9.26. Todo chamado que estiver ocioso por 72 horas será movimentado automaticamente para a situação (status) EM ATENDIMENTO.

4.10. Computadores e Recursos Tecnológicos

4.10.1. Os equipamentos disponíveis aos colaboradores são de propriedade da Serede, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

4.10.2. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Serede, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Tecnologia da Informação.

4.10.3. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

4.10.4. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no Service Desk.

4.10.5. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

4.10.6. Arquivos pessoais e/ou não pertinentes ao negócio da Serede (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para o equipamento localmente e nos drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

4.10.7. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

4.10.8. Os colaboradores da Serede e/ou detentores de contas privilegiadas não devem executar

nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Sistemas e Soluções.

4.10.9. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

4.10.9.1. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

4.10.9.2. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Serede ou por terceiros devidamente contratados para o serviço.

4.10.9.3. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

4.10.9.4. O Colaborador deverá manter a configuração do equipamento disponibilizado pela Serede, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelos procedimentos específicos da instituição, assumindo a responsabilidade como custodiante de informações.

4.10.9.5. Deverão ser protegidos por senha (bloqueados) todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

4.10.9.6. Todos os recursos tecnológicos adquiridos pela Serede devem ter imediatamente suas senhas padrões (default) alteradas.

4.10.9.7. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

4.10.10. Acrescenta-se algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Serede:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para 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;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

4.10.11. A Serede tem o Microsoft Teams como ferramenta oficial para Instant Messaging (mensagens instantâneas), videoconferência e tramitação de arquivos, dentre outras funcionalidades. Dessa forma, todos os colaboradores da área administrativa deverão utilizar como padrão a ferramenta Teams para estas atividades.

4.11. Backup/Restore

4.11.1. Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente 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.

4.11.2. Existem duas rotinas distintas de backup full: A primeira é diária e é feita através do banco de dados e salva os registros alterados no dia. A segunda é feita através da plataforma nativa da AWS (AWS Backup) as quais são realizadas da seguinte forma: Diariamente, semanalmente e mensalmente.

4.11.3. A rotina diária do banco de dados emite alerta através de um bot para o grupo de trabalho e em caso de falha, o job deverá ser executado manualmente.

4.11.4. As rotinas de backup da AWS poderão ser verificadas por logs de execução e em caso de falha, o backup deverá ser refeito manualmente. Caso seja verificado que haverá impacto nos sistemas em produção, o gerente de Tecnologia da Informação deverá ser informado.

4.11.5. Os testes de restauração serão executados em janela fora do expediente e em ambiente diferente do ambiente de produção.

4.11.6. As solicitações de restauração (restore) de backup podem ser solicitadas pelos responsáveis pelos sistemas, de acordo com a criticidade do backup, via abertura de chamado específico

para este fim.

4.12. Classificação das Informações

Até que seja devidamente classificada, toda informação da Serede deve ser considerada de uso interno. Para efeitos de classificação da informação, a Serede pode adotar as seguintes categorias:

- **Pública:** Será considerada como informação pública aquela definida por força de lei, ou devidamente autorizada à divulgação externa. No geral trata-se de uma informação disponível ao público ou que seja acessível por meio de consulta pública, preservando a sua integridade.
- **Uso interno:** Representa baixo nível de confidencialidade e risco. Informações de uso interno são aquelas de uso exclusivo por colaboradores, terceiros e parceiros autorizados, mas que em caso de vazamento das informações assim classificadas, poderá causar danos ou impactos institucionais. No geral, são informações que devem ser protegidas contra alteração ou exposição não autorizada. Essa categoria é atribuída a informações do tipo e-mails, correspondências, comunicados e outros documentos internos.
- **Confidencial:** O rótulo atribuído a informações que, devido a sua natureza, devem ser limitadas a pessoas específicas e previamente autorizadas. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer prejuízos financeiros, de imagem, às pessoas ou ao próprio negócio da Serede. No geral, são informações relacionadas a novos projetos estratégicos, orçamento da Serede, novos clientes, dados pessoais e dados pessoais sensíveis.

4.13. Diretrizes da Classificação de Dados

4.13.1. Diretrizes

Toda informação deve ser classificada, seja ela em meio físico ou digital, pelo gestor da informação;

- As informações devem estar protegidas de acordo com os padrões, políticas e diretrizes de Segurança da informação, referenciados no documento;
- Somente o gestor da informação pode reclassificar as informações;
- Toda classificação da informação deve estar identificada e de fácil visualização, seja em formato físico ou digital;

- A classificação da informação não pode ter o objetivo de atribuir sigilo a informações que sejam públicas por força de lei, ou já tenham sido classificadas como “Pública”
- Informações internas e confidenciais, sejam elas físicas ou digitais só podem ser transmitidas ou transportadas por meios ou tecnologias homologadas pela Serede;
- Informações classificadas como internas ou confidenciais não podem ser discutidas ou exibidas em local público (corredores internos, elevadores, restaurantes, etc.);
- Informações que não tenham sido rotuladas devem ser consideradas como de uso interno, não sendo permitida sua publicação ou divulgação, salvo em virtude de Lei.
- O acesso às informações internas e confidenciais deve estar limitado para o estritamente necessário ao desempenho das atividades e funções dos usuários;
- Informações em formato físico classificadas como confidenciais, devem ter descrito em seu envelope ou embalagem, o (s) destinatário (s) que possui (em) autorização de acesso;
- Cópias ou reproduções, totais ou parciais, herdam a mesma classificação da informação original e sua reprodução deve ser realizada em local e condições adequados.
- Informações confidenciais não devem ser impressas, exceto em casos autorizados explicitamente pelo Gestor da Informação.
- Informações confidenciais devem possuir controle de acesso que exija a identificação e autenticação do usuário;
- Toda informação classificada como interna ou confidencial deve estar resguardada por contingência;
- Caso a informação seja utilizada em meio eletrônico, esta deve estar protegida por todos os padrões de segurança e ser devidamente rotulada, contendo um aviso (disclaimer) seguindo o nível de criticidade:
    - **Pública:** o conteúdo desta mensagem é público, e pode ser de conhecimento de qualquer pessoa;
    - **Interna**: Informações de uso interno que não podem ser divulgadas para pessoas que não façam parte da Serede ou não tenham sido autorizadas pela organização;
    - **Confidencial**: Informações de uso confidencial que não podem ser divulgadas para pessoas que não tenham sido autorizadas pela organização.

4.13.2. PAPÉIS E RESPONSABILIDADES

4.13.2.1. Gestor da Informação

- Definir a classificação das informações sob sua responsabilidade com base nas categorias de classificação constantes nessa política;
- Controlar as informações geradas em sua área de negócio e atuação;
- A cada seis meses, deverá revisar a classificação das informações sob sua guarda;
- Garantir que as informações tratadas em sua gerência estejam devidamente classificadas;
- Assegurar que as diretivas definidas nesta política estão sendo aplicadas conforme a classificação indicada;
- Assegurar o devido armazenamento físico e lógico, e a preservação da informação;

4.13.2.2. Área de Segurança da Informação

- Auxiliar na definição dos padrões, tecnologias, critérios e técnicas para a segurança das informações de acordo com o nível de classificação da informação agindo em caráter consultivo;
- Monitorar eventos que possam representar riscos cibernéticos à aplicação dessa política, com base nas tecnologias definidas, utilizando-se de todos os meios viáveis para tal;

4.13.2.3. Equipe de Privacidade de Dados

- Definir os direcionadores de classificação de dados pessoais;
- Garantir e realizar a governança do registro de operações de tratamento de dados pessoais da Companhia;
- Realizar a governança dos riscos relacionados à privacidade de dados pessoais;

4.13.2.4. Usuário da Informação

- Tratar as informações da Serede de acordo com o estabelecido nesta política;
- Reportar quaisquer desvios identificados relacionados nesta política à Equipe de Segurança da Informação.

4.14. Regras para a execução do Processo de Contratação de Serviços Externos

Previamente a contratação de serviços externos que interajam com dados e informações, a Serede deverá enviar ao fornecedor a Política de Segurança da Informação que consiste em:

- Políticas de Segurança que prevê a utilização de controles para garantir sigilo, integridade e confidencialidade das informações e ativos tecnológicos, de forma ampla;
- Padrões de Segurança da Informação, que determinam os métodos de implementações de controles definidos nas políticas de segurança;
- Padrões de Segurança Digital, que determinam os métodos de implementações de controles definidos nas políticas de segurança voltado a tecnologias digitais, nuvens e interconexões de ativos. O aceite desta documentação é obrigatório para todos os contratos que envolvam tecnologia e tem o objetivo de informar ao fornecedor quais são os pontos de atendimento obrigatório, no que tange as melhores práticas cobradas por segurança da informação.

4.15. Compartilhamento de Dados

Os dados só deverão ser compartilhados a partir das ferramentas oficiais da empresa (Teams, OneDrive, e-mail corporativo).

4.16. Criptografia e Confidencialidade

Toda solução adquirida pela Serede deve utilizar mecanismos criptográficos para garantir o sigilo, integridade e confidencialidade no armazenamento (data at rest) e transmissão de informações (data in transit).

- A solução deve possuir mecanismos de validação de entrada de forma positiva e sanitização de todas as saídas de dados (de usuários e/ou interfaces com outros sistemas) quanto ao formato dos dados e valores/caracteres esperados.
- A solução não deve armazenar informações sensíveis (ex: senhas, chaves criptográficas, credenciais de acesso, dados de conexão, etc) de forma fixa no ativo.
- Toda solução deve ser desenvolvida de forma componentizada, permitindo a distribuição física dos componentes (ex.: front-end, aplicativo e banco de dados) por diferentes áreas da rede da organização (ex.: DMZ, rede interna).
- Nos casos em que seja obrigatória a garantia de privacidade dos dados, esta deve permitir

que uma política de privacidade seja publicada e exibida aos usuários.

- Estar aderente aos requisitos vigentes de legislação, regulatório e outros.
- A solução não deve armazenar informações sensíveis de forma a proteger o sigilo do cliente, sempre que possível.

5. ANEXOS

Não se aplica.