POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

CALCULIST

A Política de Segurança da Informação, também referida como PSI, é o documento chave que estabelece as diretrizes corporativas adotadas pela **CALCULIST** para a proteção dos ativos de informação. Essa política é essencial para orientar todas as atividades relacionadas à segurança da informação e para a prevenção de responsabilidade legal envolvendo o uso e a gestão desses ativos. Portanto, seu cumprimento é mandatório em todas as áreas operacionais e administrativas da empresa.

Esta PSI é aplicável a todos os colaboradores da **CALCULIST**, sem exceções. Todos os funcionários, independentemente do nível hierárquico ou função, são responsáveis por aderir e promover as práticas de segurança aqui estabelecidas.
Fundamentada nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, esta política também está alinhada com as leis vigentes no Brasil. A adoção desses padrões e legislações assegura que a **CALCULIST** esteja na vanguarda da proteção de informações confidenciais e da integridade dos dados corporativos.

1. OBJETIVOS

1.1. Estabelecer diretrizes que permitam aos colaboradores e clientes da **CALCULIST** seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

1.2. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

1.3. Preservar as informações da **CALCULIST** quanto à:

1.3.1. 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.

1.3.2. Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

1.3.3. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. APLICAÇÕES DA PSI

2.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

2.2. Esta PSI 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.

2.3. É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou **do setor de TI - Tecnologia da Informação** sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3. PRINCÍPIOS DA PSI

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

3.2. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

3.3. A **CALCULIST**, por meio **do setor de TI - Tecnologia da Informação**, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. REQUISITOS DA PSI

4.1. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da **CALCULIST** a fim de que a Política seja cumprida dentro e fora da empresa.

4.2. Poderá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

4.3. Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança da Informação.

4.4. Deverá constar em todos os contratos da **CALCULIST** 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 **CALCULIST**.

4.5. 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. Eles devem assinar um termo de responsabilidade.

4.6. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao **TI - Tecnologia da Informação** Interno e ele, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

4.7. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

4.8. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

4.9. Deverão ser criados e instituídos controles apropriados, trilhas de auditoria 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 **CALCULIST** ou por terceiros.

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

4.11. A **CALCULIST** 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.

4.12. Esta PSI será implementada na **CALCULIST** 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.

4.13. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da **CALCULIST** e sujeitará o usuário às medidas administrativas e legais cabíveis.

5. DAS RESPONSABILIDADES ESPECÍFICAS

5.1. Dos colaboradores em geral:

5.1.1. 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 **CALCULIST**.

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

5.2. Dos colaboradores em regime de exceção (temporários):

5.2.1. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

5.2.2. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao

regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

5.3. Dos gestores de pessoas e/ou processos:

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

5.3.2. 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 da **CALCULIST**.

5.3.3. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da **CALCULIST**.

5.3.4. Antes de conceder acesso às informações da **CALCULIST** e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

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

6. DOS CUSTODIANTES DA INFORMAÇÃO

6.1. Da área de tecnologia da informação:

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

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

6.1.3. 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.

6.1.4. 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 só 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.

6.1.5. Segregar as funções administrativas 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 e trilhas de auditoria das suas próprias ações.

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

6.1.7. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

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

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

6.1.10. O gestor 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.

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

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

6.1.13. 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:

6.1.13.1. os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

6.1.13.2. os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

6.1.13.3. 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.

6.1.13.4. 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.

6.1.13.5. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo exigindo o seu cumprimento dentro da **CALCULIST**.

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

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

6.1.13.8. 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.

6.1.13.9. 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.

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

6.1.13.10.1. uso da capacidade instalada da rede e dos equipamentos;

6.1.13.10.2. tempo de resposta no acesso à internet e aos sistemas críticos da **CALCULIST**;

6.1.13.10.3. períodos de indisponibilidade no acesso à internet e aos sistemas críticos da **CALCULIST**;

6.1.13.10.4. incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

6.1.13.10.5. 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).

6.2.Da área de segurança da informação:

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

6.2.2. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da **CALCULIST**.

6.2.3. Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

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

6.2.5. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

6.2.6. Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

6.2.7. Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

6.2.8. Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a **CALCULIST**.

6.2.9. Buscar alinhamento com as diretrizes corporativas da **CALCULIST**.

6.3.Do comitê de segurança da informação ("CSI"):

6.3.1. Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano.

6.3.2. Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário

deliberar sobre algum incidente grave ou definição relevante para a **CALCULIST**.

6.3.3. O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

6.3.4. Cabe ao CSI:

6.3.4.1. propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;

6.3.4.2. propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;

6.3.4.3. avaliar os incidentes de segurança e propor ações corretivas;

6.3.4.4. definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

6.4. Do monitoramento e da auditoria do ambiente:

6.4.1. Para garantir as regras mencionadas nesta PSI a **CALCULIST**:

6.4.1.1. 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 esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

6.4.1.2. tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;

6.4.1.3. realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

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

6.5.Do correio eletrônico:

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

6.5.2. O uso do correio eletrônico da **CALCULIST** é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a **CALCULIST** e também não cause impacto no tráfego da rede.

6.5.3. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da **CALCULIST**:

6.5.4. enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da **CALCULIST**;

6.5.5. 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;

6.5.6. enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a **CALCULIST** ou vulneráveis a ações civis ou criminais;

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

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

6.5.9. apagar mensagens pertinentes de correio eletrônico quando a **CALCULIST** estiver sujeita a algum tipo de investigação.

6.5.10. produzir, transmitir ou divulgar mensagem que:

6.5.10.1. - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da **CALCULIST**;

6.5.10.2. - Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

6.5.10.3. - 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;

6.5.10.4. - Vise obter acesso não autorizado a outro computador, servidor ou rede;

6.5.10.5. - Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

6.5.10.6. - Vise burlar qualquer sistema de segurança;

6.5.10.7. - Vise vigiar secretamente ou assediar outro usuário;

6.5.10.8. - Vise acessar informações confidenciais sem explícita autorização do proprietário;

6.5.10.9. - Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

6.5.10.10. - Inclua imagens criptografadas ou de qualquer forma mascaradas;

6.5.10.11. - Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)

6.5.10.12. - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

6.5.10.13. - Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

6.5.10.14. - Tenha fins políticos locais ou do país (propaganda política);

6.5.10.15. - Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;

6.5.10.16. - Tenha conteúdo considerado impróprio, obsceno ou ilegal.

6.6.Da internet:

6.6.1. Todas as regras atuais da **CALCULIST** 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 **CALCULIST** com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

6.6.2. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a **CALCULIST**, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

6.6.3. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da **CALCULIST**, 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.

6.6.4. A **CALCULIST**, 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 gestor. 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.

6.6.5. A internet disponibilizada pela **CALCULIST** aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

6.6.6. Como é do interesse da **CALCULIST** que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

6.6.7. Somente os colaboradores que estão devidamente autorizados a falar em nome da **CALCULIST** para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

6.6.8. Apenas os colaboradores autorizados pela **CALCULIST** poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à

norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

6.6.9. 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.

6.6.10. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na **CALCULIST** e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.

6.6.11. 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. Qualquer software não autorizado baixado será excluído pela Gerência de Sistemas.

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

6.6.13. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

6.6.14. 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 gestores.

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

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

6.6.17. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Gerencia de Sistemas.

6.6.18. Não é permitido acesso a sites de proxy.

6.7.Identificação:

6.7.1. 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 **CALCULIST** e/ou terceiros.

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

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

6.7.4. Todos os dispositivos de identificação utilizados na **CALCULIST**, 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.

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

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

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

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

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

6.7.10. A Gerência de Sistemas responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

6.7.11. 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.

6.7.12. 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.

6.7.13. 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.

6.7.14. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

6.8.Computadores e Recursos Tecnológicos:

6.8.1. Os equipamentos disponíveis aos colaboradores são de propriedade da **CALCULIST**, 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.

6.8.2. 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 Gerência de Sistemas da **CALCULIST**, ou de quem este determinar.

6.8.3. 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.

6.8.4. 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.

6.8.5. Arquivos pessoais e/ou não pertinentes ao negócio da **CALCULIST** (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os 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.

6.8.6. 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.

6.8.7. Os colaboradores da **CALCULIST** 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.

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

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

6.8.10. 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 Gerência de Sistemas da **CALCULIST** ou por terceiros devidamente contratados para o serviço.

6.8.11. Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

6.8.12. O colaborador deverá manter a configuração do equipamento disponibilizado pela **CALCULIST**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

6.8.13. Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

6.8.14. Todos os recursos tecnológicos adquiridos pela **CALCULIST** devem ter imediatamente suas senhas padrões (default) alteradas.

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

6.8.16. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da **CALCULIST**.

6.8.17. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

6.8.18. Burlar quaisquer sistemas de segurança.

6.8.19. Acessar informações confidenciais sem explícita autorização do proprietário.

6.8.20. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

6.8.21. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

6.8.22. 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;

6.8.23. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

6.8.24. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

6.9. Uso De Dispositivos Móveis

6.9.1. **Política de Uso de Celulares:** A **CALCULIST**, reconhecendo a importância dos dispositivos móveis para a eficiência operacional e comunicação interna, remete ao documento específico intitulado "Política de Uso de Celulares" para regulamentar a utilização destes equipamentos. Esta política se aplica a todos os colaboradores da **CALCULIST**, estabelecendo diretrizes claras e obrigatórias para o uso responsável e seguro de dispositivos móveis corporativos e pessoais dentro do ambiente de trabalho.

6.9.2. **Abrangência e Conformidade:** As diretrizes detalhadas nesta política específica abrangem a utilização de celulares, tablets, e demais dispositivos portáteis, tanto de propriedade da empresa quanto pessoais dos colaboradores, e são obrigatórias para todos aqueles que acessam a rede corporativa ou manipulam dados corporativos através desses dispositivos.

6.10. **Segurança e Responsabilidade:** A Política de Uso de Celulares visa proteger as informações corporativas e pessoais em conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras legislações pertinentes, assegurando que a utilização de tais dispositivos esteja em alinhamento com as normas de segurança da informação estabelecidas pela empresa.

6.11. **Termos de Uso:** Todo colaborador que utilize dispositivos móveis, conforme estabelecido na política específica, deverá assinar os respectivos Termos

de Uso que detalham as obrigações, responsabilidades e condutas esperadas, garantindo a adesão às práticas de segurança e proteção de dados.

6.12. **Monitoramento e Conformidade:** A aderência à Política de Uso de Celulares será monitorada constantemente, e qualquer desvio das práticas estabelecidas poderá acarretar sanções, conforme detalhado na política. É esperado que todos os colaboradores cooperem plenamente com as diretrizes para garantir a segurança e a integridade dos ativos de informação da empresa.

6.13. **Atualizações da Política:** A Política de Uso de Celulares será revisada periodicamente para garantir sua atualização e conformidade com as mudanças na legislação e nas práticas de mercado, mantendo sua eficácia e relevância.

6.14. **Integração com Outras Políticas:** Enquanto este documento trata especificamente do uso de dispositivos móveis, ele integra-se com outras políticas de segurança da informação e práticas de governança de TI estabelecidas pela **CALCULIST** e suas subsidiárias.

6.15. Datacenter:

6.15.1. O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

6.15.2. Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

6.15.3. Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

6.15.4. O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas.

6.15.5. A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

6.15.6. Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

6.15.7. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade.

6.15.8. O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

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

6.15.10. Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse do coordenador de infraestrutura.

6.15.10.1. O Datacenter deverá ser mantido limpo e organizado.

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

6.15.10.3. A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

6.15.11. No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

6.16.Backup:

6.16.1. Todos os backups devem ser automatizados por sistemas de agendamento automatizado 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.

6.16.2. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

6.16.3. Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da **CALCULIST**, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

6.16.4. Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

6.16.5. Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

7. DISPOSIÇÕES FINAIS

7.1. Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da **CALCULIST**. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

8. GESTÃO DE INCIDENTES DE SEGURANÇA

8.1. **Registro de Incidentes**: Todos os incidentes de segurança devem ser prontamente registrados no portal da Iguana IT por parte dos colaboradores ou detectados pelos sistemas automáticos de monitoramento.

8.2. **Análise Inicial**: Após o registro, o time de especialistas em segurança da informação deverá verificar o relato do incidente em um prazo máximo de uma hora, podendo, se necessário, solicitar informações adicionais para melhor compreensão do ocorrido.

8.3. **Classificação de Prioridade**: Com base nas informações coletadas, o incidente será classificado conforme seu nível de prioridade, determinando a urgência e os recursos alocados para sua resolução.

8.4. **Investigação e Resolução**: Inicia-se a fase de investigação para identificar a causa raiz e implementar as soluções adequadas para resolver o incidente, seguindo as melhores práticas e padrões de segurança vigentes.

8.5. **Testes de Verificação**: Após a implementação das soluções, serão realizados testes para assegurar que o incidente foi completamente resolvido e que não existem falhas remanescentes ou novas vulnerabilidades criadas.

8.6. **Documentação e Revisão**: Finalmente, todas as informações pertinentes ao incidente, incluindo sua natureza, a resposta dada e os resultados dos testes de verificação, serão meticulosamente documentadas e arquivadas no portal da Iguana IT. Esta documentação estará disponível para consultas futuras e para a realização de auditorias periódicas, visando a melhoria contínua dos processos de segurança.

8.7. **Disposições Éticas**: Ressalta-se que qualquer incidente de segurança é considerado uma violação ética, contrária aos princípios e bons costumes regidos pela **CALCULIST**, devendo ser tratado com a máxima seriedade e seguindo os protocolos estabelecidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.