POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da SIMPLIFICACI para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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

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

Preservar as informações da SIMPLIFICACI 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.

APLICAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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.

Esta política dá ciência 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 esta Política de Segurança, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela SIMPLIFICACI, pertence à referida empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais.

A SIMPLIFICACI, por meio do Departamento de Infraestrutura, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

REQUISITOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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

Deverá constar em todos os contratos da SIMPLIFICACI 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 empresa.

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.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Departamento de Infraestrutura através do e-mail csirt@simplificaci.com.br.

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.

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.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a empresa 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 SIMPLIFICACI ou por terceiros.

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

O SIMPLIFICACI 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.

Esta PSI será implementada na SIMPLIFICACI 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.

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

DAS RESPONSABILIDADES ESPECÍFICAS

DOS COLABORADORES EM GERAL

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 a SIMPLIFICACI e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

DOS COLABORADORES TEMPORÁRIOS

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Departamento de Infraestrutura.

A concessão será 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.

DOS GESTORES

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

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI.

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 SIMPLIFICACI.

Antes de conceder acesso às informações da empresa, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

DA ÁREA DE TI (INFRAESTRUTURA)

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

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.

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.

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.

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

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.

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

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.

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

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 funcionários serão de responsabilidade do próprio funcionário.

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

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.

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.

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

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

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

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.

DA SEGURANÇA DA INFORMAÇÃO

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

Propor e apoiar iniciativas que visem à segurança dos ativos de informação do SIMPLIFICACI.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Diretor de Tecnologia da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio do SIMPLIFICACI, mediante campanhas, palestras, treinamentos e outros meios de marketing.

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

DO MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, a SIMPLIFICACI poderá:

• 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;

• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior);

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

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

CORREIO ELETRÔNICO

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

O uso do correio eletrônico do SIMPLIFICACI é para fins corporativos e relacionados às atividades do colaborador usuário dentro da empresa.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do SIMPLIFICACI:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da empresa;
- 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;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o SIMPLIFICACI ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

Produzir, transmitir ou divulgar mensagem que:

- contenha qualquer ato ou forneça orientação que conflite com os interesses do SIMPLIFICACI;
- contenha ameaças eletrônicas, como: spam, worms, vírus de computador;
- possua arquivos com código executável (.exe, .com, .bat, .pif, .js, .src,.cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- objetive obter acesso não autorizado a outro computador, servidor ou rede;
- objetive interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- objetive burlar qualquer sistema de segurança;
- objetive vigiar secretamente ou assediar outro usuário;
- objetive acessar informações confidenciais sem explícita autorização do proprietário;
- objetive acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- possua conteúdo considerado impróprio, obsceno ou ilegal;
- possua de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contendo perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- objetive fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir o papel de carta da empresa

ACESSOS A REDE CORPORATIVA E INTERNET

Todas as regras atuais do SIMPLIFICACI 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 empresa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

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

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

A SIMPLIFICACI, 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 empresa cooperará ativamente com as autoridades competentes.

Como é do interesse do SIMPLIFICACI 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.

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

Apenas os colaboradores autorizados pela empresa 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.

É proibida a divulgação e/ou o compartilhamento indevido de informações administrativas 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.

Os colaboradores com acesso à internet poderão fazer o download somente de programas relacionados diretamente às suas atividades no SIMPLIFICACI e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo Departamento de Infraestrutura.

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 removido pelo Departamento de Infraestrutura. Os colaboradores não

poderão em hipótese alguma utilizar os recursos do SIMPLIFICACI para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham suas atividades profissionais relacionadas a isso.

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.

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

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

O acesso a softwares peer-to-peer não será permitido. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos.

Não é permitido acesso a sites de proxy.

Gestão, controle de acessos e rastreabilidade

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

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

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

Todos os dispositivos de identificação utilizados no SIMPLIFICACI, 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.

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

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

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

O Departamento de Recursos Humanos do SIMPLIFICACI é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

O Departamento de Infraestrutura responde pela criação da identidade lógica dos colaboradores na empresa, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar

Os usuários deverão ter senha possuindo no mínimo 7 (sete) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

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.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Departamento de Infraestrutura da SIMPLIFICACI.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

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.

A periodicidade máxima para troca das senhas é 42 (quarenta e dois) dias, não podendo ser repetidas as 24 (vinte e quatro) últimas senhas. Os sistemas devem forçar a troca das senhas.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum colaborador 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 e outras situações similares.

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

Prevenção contra vírus, arquivos e softwares maliciosos

Os equipamentos disponíveis aos colaboradores são dotados de ferramentas de controle e proteção de antivírus e firewall afim de aprimorar a segurança nos equipamentos. Além disso tais dispositivos são conectados a serviços de atualizações de segurança dos sistemas operacionais visando manter os sistemas seguros e estáveis.

Conscientização em Segurança da Informação

A SimplificaCI promove eventos e workshops internos para conscientização da Política de Segurança da informação e suas atualizações. Adicionalmente são realizados treinamentos sobre segurança cibernética para que os usuários de dispositivos da empresa, estejam orientados sobre fraudes e ameaças que exploram as vulnerabilidades humanas e tecnológicas.

EQUIPAMENTOS E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da SIMPLIFICACI, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa.

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 de Infraestrutura.

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.

Os colaboradores da SIMPLIFICACI 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 do Departamento de Infraestrutura.

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

• 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 do Departamento de Infraestrutura da SIMPLIFICACI ou por terceiros devidamente contratados para o serviço.

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

• O colaborador deverá manter a configuração do equipamento disponibilizado pela SIMPLIFICACI, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e

pelas normas específicas da empresa, assumindo a responsabilidade como custodiante de informações.

• Deverão ser protegidos por senha (bloqueados), todos os terminais de computador quando não estiverem sendo utilizados.

• Todos os recursos tecnológicos adquiridos pela SIMPLIFICACI devem ter imediatamente suas senhas padrões alteradas.

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

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do SIMPLIFICACI.

• 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 delituosa de acordo com a legislação nacional.

DISPOSITIVOS MÓVEIS

O SIMPLIFICACI deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da empresa, ou aprovado e permitido pelo Departamento de Infraestrutura, como: notebooks, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

O SIMPLIFICACI, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume 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 no SIMPLIFICACI, mesmo depois de terminado o vínculo contratual mantido com a empresa.

O suporte técnico aos dispositivos móveis de propriedade do SIMPLIFICACI e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela empresa.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Departamento de Infraestrutura.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico do Departamento de Infraestrutura da SIMPLIFICACI.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo SIMPLIFICACI, notificar imediatamente seu gestor direto e a Gerência de Sistemas.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao SIMPLIFICACI e/ou a terceiros.

MANUTENÇÃO E CÓPIAS DE SEGURANÇA

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, períodos em que não há nenhum ou pouco acesso de usuários causando baixo ou nenhum impacto de desempenho.

As mídias de backup devem ser devidamente identificadas de preferência com etiquetas, dando uma conotação mais organizada e profissional.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da SIMPLIFICACI, 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.

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

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 90 ou 180 dias, de acordo com a criticidade do backup.

SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da SIMPLIFICACI, assim como o uso de eventuais ramais virtuais instalados nos computadores é responsabilidade do departamento de Infraestrutura, de acordo com as definições da Diretoria da SIMPLIFICACI. Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

AMBIENTES EM NUVEM E DATACENTERS EXTERNOS

Todos os acessos a ambientes externos para publicações, manutenções e implantações são realizados através de túneis criptografados.

Todos os ambientes em nuvens públicas são gerenciados centralizadamente visando impedir, detectar e responder a ameaças com maior visibilidade e controle sobre a segurança dos recursos disponibilizados aos usuários dos sistemas da SimplificaCI.

É utilizado WAF (firewall de aplicativo Web) para proteger os aplicativos Web contra ataques comuns baseados na Web, como injeção de SQL, ataques de scripts entre sites e sequestros de sessão.

Nós realizamos teste de penetração automatizados regularmente nos aplicativos, visando aprimoramento contínuo da segurança.

Adotamos uma arquitetura de segurança em camadas que fornecem um ambiente de runtime isolado implantado em uma Rede Virtual ocultando os back-ends de API do acesso à Internet geral.

Utilizamos criptografia em trânsito como mecanismo de proteção de dados quando eles são transmitidos entre redes utilizando HTTPS ao transferir dados dentro ou fora do Armazenamento.

GESTÃO DE CONTINUIDADE DOS NEGÓCIOS

A GCN (Gestão de Continuidade de Negócios) é constituída de uma série de procedimentos e medidas que terão, por objetivo, minimizar as perdas decorrentes de um desastre, ou seja, de eventos de grandes proporções em termos de impacto, não sustentado pela organização.

Um dos objetivos da GCN é a continuidade operacional dos processos da organização que foram identificados como críticos. Isso se dá por meio da implantação de uma série de estratégias e ferramentas realizadas de acordo com as prioridades identificadas durante a elaboração do plano.

PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.