POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e

Normas Administrativas

PSI	0001	-	5
SIGLA	NÚMERO/PARTE		REVISÃO

Data da Homologação:	22/03/2022

Referência: GTI – PSI-DDNA – ICRO	Versão: 1.4
Criado por: Diego Garcia	Data criação: 14/01/2022
Revisado por: Eduardo Lima	Data da revisão: 28/04/2022
Status: Aprovada	Número de páginas: 17
Em conformidade com ISO 27001 e ISO 27002	

Sumário

A Política de Segurança da Informação, referenciada por PSI, é o documento que orienta e estabelece as diretrizes corporativas da ICRO Solutions no que diz respeito a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser aplicada em larga escala e cumprida fielmente por todos os colaboradores, clientes, parceiros e fornecedores que tenha relação direta com a ICRO e o uso compartilhado de recursos ICRO.

O presente documento está baseado nas recomendações propostas pela ABNT NBR ***ISO/IEC 27002:2013***, 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

1. Definir as diretrizes necessárias que permitirão colaboradores, clientes, parceiros e fornecedores, seguirem um padrão de comportamento relacionado à segurança da informação, que sejam adequados às necessidades de negócio da ICRO Solutions bem como os aspectos de proteção legal da empresa e do indivíduo.

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

3. Garantir as informações da ICRO Solutions quanto à:

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

Aplicação da PSI

As diretrizes aqui estabelecidas precisam ser respeitadas e seguidas, incondicionalmente, por todos os colaboradores, clientes e prestadores de serviços (parceiros ou fornecedores) e se aplicam diretamente à informação bem como, qualquer meio através do qual esteja inserida a informação (ativos, processos, pessoas e itens de configuração).

Através destas diretrizes, damos ciência a cada colaborador, cliente ou prestador de serviços que os ambientes, sistemas, computadores, dispositivos móveis e redes da empresa, poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras, em especial, as **leis 12.965/2014 (Marco Civil da Internet) e 13.709/2018 (LGPD – Lei Geral de Proteção de Dados)**.

É também obrigação de cada colaborador, manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência

de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso ou descarte de informações no âmbito da ICRO Solutions.

A politica de segurança da informação tambem torna a ser a base para tomadas de decisões da TI com o negócio utilizando componentes como **Comitês**, **Políticas** e **Métricas** que permitem alinhamento, eficiência e Accountability da TI.

Alinhamento: Garante investimentos alinhados com o negócio. Garante que as iniciativas de TI estejam alinhadas com os padrões de arquitetura, controle e segurança presentes em nossos clientes.

Eficiência: Otimiza a alocação do orçamento de TI de acordo com as prioridades do Negócio. Racionaliza e otimiza o desenvolvimento e manutenção de soluções

Accountability: Melhora o desempenho do serviço e os retornos nos investimentos de TI, à medida em que as pessoas trabalham para alcançar os resultados pelos quais eles são responsáveis

Figura 1 – Estrutura de Governança de TI

Princípios da PSI

Toda informação produzida e/ou recebida pelos colaboradores e/ou prestadores de serviços, a partir da execução de atividades individuais ou em grupo no âmbito de atuação desta empresa ou como forma de entrega de produtos ou serviços para os clientes desta organização, pertence a ICRO Solutions. Qualquer exceção precisa ser explicitada e formalizada quando do contrato entre as partes.

Os ativos de tecnologia e comunicação, sistemas de informações, processos e POP's (Procedimento Operacional Padrão) são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que sejam:

- Previamente autorizados pela autoridade pertinente (chefes de departamento) e;
- Não prejudiquem o desempenho dos serviços e nem dos ativos ou IC's envolvidos na entrega destes serviços.

A ICRO Solutions poderá registrar todo o uso dos sistemas e serviços, com propósito de

garantir a disponibilidade, a integridade e a confidencialidade das informações utilizadas.

A estrutura normativa da Segurança da Informação é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- **Política:** constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- **Normas:** estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- **Procedimentos:** instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da Icro Solutions.

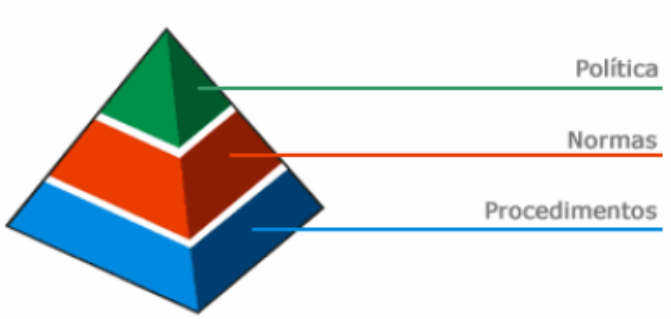

Figura 2 – Estrutura normativa de Segurança da Informação

Requisitos da PSI

Para garantir aderência e uniformidade quanto ao uso da informação, a PSI deverá ser comunicada a todos os colaboradores, clientes e parceiros ou fornecedores, de maneira explícita e direta, a fim de que esta política seja cumprida dentro e fora da ICRO Solutions.

Tanto a PSI quanto as normas de segurança da informação deverão ser revistas e atualizadas periodicamente sempre que algum fato relevante ou evento seja motivo de observação de adequação desta organização.

Em todos os contratos da ICRO Solutions (contratação de recursos humanos, venda de produtos e/ou serviços, bem como, contratos de apoio com parceiros ou fornecedores) deverá constar o **Anexo de Confidencialidade ou Cláusula de Confidencialidade**, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela organização.

Além disso, todos os recursos humanos e/ou parceiros e fornecedores, deverão ser comunicados previamente sobre sua responsabilidade em relação à segurança da informação, sendo então, no momento adequado, serem orientados sobre os procedimentos de segurança bem como o uso correto dos ativos a fim de reduzir possíveis riscos. Nesse momento, todos deverão assinar o **Termo de Responsabilidade** sobre uso dos ativos e serviços.

Todo incidente de segurança, conforme previsto no **Processo de Gerenciamento de Incidentes da ICRO Solutions**, deverá ser registrado, tratado e sinalizado, sumariamente, à Gerência de Tecnologia da Informação, que terá a responsabilidade de avaliar junto ao time, as

ações necessárias que precisarão ser implementadas nesta política, com a finalidade detectar, prevenir e remediar de maneira mais eficaz, as possíveis reincidências.

Deverão ser criados e constituídos controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a ICRO julgar importante para reduzir os riscos dos seus ativos de informação, como por exemplo, nas estações de trabalho, notebooks, acessos à internet, correio eletrônico, sistemas comerciais e financeiros desenvolvidos internamente ou externamente à organização.

Os ambientes de PRODUÇÃO devem ser segregados e rigidamente controlados garantindo o total isolamento em relação a outros ambientem como por exemplo: ambientes de desenvolvimento, teste e homologação. Nesse sentido ainda, para garantir maior controle, os ambientes de desenvolvimento, teste e homologação, precisam ser estruturados de acordo com sua finalidade e também segregados uns dos outros permitindo assim, sua individualizaçãode propósito.

A ICRO Solutions reserva-se ao direito de analisar dados e evidências, quando necessário, para obter provas a serem utilizadas nos processos investigatórios relacionados ao uso indevido, negligente ou imprudente dos recursos e serviços concedidos a seus colaboradores, clientes, parceiros ou fornecedores, em quaisquer situações confirmadas ou sob suspeita, para conduzir situações que estejam contra o que está previsto nesta política. Além disso, a ICRO também reserva-se ao direito de tomar as medidas legais cabíveis nestes casos.

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

O não cumprimento de quaisquer requisitos nesta PSI ou das Normas de Segurança da Informação, acarretará violação direta às regras internas desta organização e sujeitará o usuário, colaborador ou empresa jurídica às medidas administrativas legais existentes.

Responsabilidades Específicas

1. Dos colaboradores em geral

Entende-se por colaborador toda e qualquer pessoa física, contratada através do regime CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade delegada pela ICRO Solutions, dentro ou fora de suas dependências.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano causado a ICRO Solutions ou aos seus clientes, em decorrência da não obediência às diretrizes e normas aqui descritas.

2. Dos gestores de pessoas e/ou processos

Ter postura exemplar no que diz respeito 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 no tocante ao cumprimento da PSI da ICRO Solutions.

Exigir dos colaboradores e prestadores de serviço a assinatura do Termo de Responsabilidade e do Acordo de Confidencialidade, assumindo então o dever de seguir as normas estabelecidas bem como, se comprometer a manter o sigilo e confidencialidade necessários, mesmo após o seu desligamento do quadro funcional ou de prestação de serviços, sobre todos os ativos de informação da ICRO Solutions.

Adaptar as normas, processos e procedimentos internos específicos de suas áreas, ao que se prevê nesta PSI.

3. Dos Custodiantes da Informação

3.1. Da área de tecnologia da informação

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Acordar os níveis de serviço adequados e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos, ferramentas e sistemas disponibilizados aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança especificados nessa política;
- Os administradores e profissionais de suporte do ambiente tecnológico da ICRO podem, pela característica de seus privilégios, acessar arquivos e dados de outros usuários. No entanto, isso somente será permitido, quando for estritamente necessário para a execução de atividades operacionais sob sua responsabilidade, como por exemplo, ao realizar manutenção nos computadores, execução de cópias de segurança, realização de auditorias ou testes no ambiente;
- Define-se ainda, em relação ao item anterior, que acessar arquivos ou dados não significa empoderamento do administrador ou profissional de suporte, no que diz respeito a tomar conhecimento do conteúdo daquele arquivo ou dado. Ou seja, é proibido ao administrador ou profissional de suporte, abrir os arquivos e/ou dados para tomar ciência de seu conteúdo;
- Criar a segregação de funções administrativas e operacionais a fim de restringir ao mínimo necessário, os poderes de cada indivíduo;
- Gerar e manter trilhas de auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas através de meios eletrônicos, implantar controles de integridade para torná-las juridicamente válidas como evidências;
- Administrar, proteger e testar cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a ICRO;
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;
- 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;

- 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;
- 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;
- 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;
- 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;
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
  - ✓ uso da capacidade instalada da rede e dos equipamentos;
  - ✓ 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);
  - ✓ incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante).

3.2 Aprovações e revisões

Os documentos integrantes da estrutura Normativa da Segurança da Informação da deverão ser aprovados e revisados conforme os seguintes critérios:

- **Política**
  - **Nível de Aprovação**: DPO
  - **Periodicidade de Revisão:** Anual
- **Normas**
  - **Nível de Aprovação:** Comitê Gestor de Segurança da Informação
  - **Periodicidade de Revisão:** Anual
- **Procedimentos**
  - **Nível de Aprovação:** Coordenador de operações de TI
  - **Periodicidade de Revisão:** Anual

3.3 Atividades, Responsabilidades e Autoridades

Atividades	Responsabilidades	Autoridades
Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da Icro.	Todos os Funcionários e Terceiros	Todos os gestores
Buscar orientação do superior hierárquico imediato ou do especialista em Segurança da Informação Corporativo em caso de dúvidas relacionadas ao tema.	Todos os Funcionários e Terceiros	Todos os gestores
Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento.	Todos os Funcionários e Terceiros	Todos os gestores
Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela Icro.	Todos os Funcionários e Terceiros	Todos os gestores
Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Icro.	Todos os Funcionários e Terceiros	Todos os gestores
Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual.	Todos os Funcionários e Terceiros	Todos os gestores
Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.	Todos os Funcionários e Terceiros	Todos os gestores
Atualizar a Política de Segurança da Informação.	Analista de suporte* com aporte do CGSI	DPO
Identificar e atribuir responsabilidades com relação à Segurança da Informação.	Analista de suporte*	Coordenador de Operações de TI
Avaliar e monitorar o nível de Segurança da Informação.	Analista de suporte*	Coordenador de Operações de TI
Monitorar alterações que possam afetar a segurança da informação.	Analista de suporte*	Coordenador de Operações de TI
Identificar e documentar as violações e suas consequentes ações disciplinares, juntamente com os gerente.	Analista de suporte*	Coordenador de Operações de TI
Propor soluções e alternativas para elevar o nível de segurança da informação da Icro.	Analista de suporte* com aporte do CGSI	Coordenador de Operações de TI
Auditar o cumprimento das regras definidas nas políticas de segurança da informação.	Analista de suporte*	Coordenador de Operações de TI
Restringir o acesso e assegurar a proteção de todos os ativos físicos que contenham informações confidenciais.	Analista de suporte*	Coordenador de Operações de TI
Restringir o acesso e assegurar a proteção dos ativos constantes nos servidores da Icro Solutions.	Analista de suporte*	Coordenador de Operações de TI
Aprovar a Política de Segurança da Informação e suas revisões.	Analista de suporte* com aporte do CGSI	DPO
Aprovar a nomeação dos “proprietários” da informação.	CGSI	DPO
Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação.	Coordenador de Operações de TI	DPO

Uso do Correio Eletrônico

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

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

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da ICRO Solutions para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da organização;
- 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 a ICRO Solutions 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;
- Apagar mensagens pertinentes de correio eletrônico ou serviço de mensageria quando a ICRO Solutions estiver sujeita a algum tipo de investigação;
- Produzir, transmitir ou divulgar mensagem que:
  - ✓ contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da ICRO Solutions;
  - ✓ 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 e com intuito de causar dano;
  - ✓ 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;
  - ✓ contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
  - ✓ 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.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- Cargo do colaborador;
- Nome da empresa;
- Telefones de contato do colaborador;
- Endereço de correio eletrônico do colaborador;
- Redes sociais da empresa.

Uso da Internet

Todas as regras atuais da ICRO Solutions visam basicamente o desenvolvimento de um comportamento 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.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a ICRO Solutions, 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 ICRO Solutions, 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.

Ao monitorar a rede interna, pretende-se 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.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos na unidade.

Como é do interesse da ICRO 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.

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

Apenas os colaboradores autorizados pela organização 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 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 a surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na ICRO e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Gerência de Tecnologia da Informação.

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 Tecnologia da Informação.

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

Como regra geral, materiais de cunho sexual não poderão ser acessados, 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 ICRO Solutions 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 ICRO Solutions 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 (uTorrent, BitTorrent e afins) não serão permitidos bem como os serviços de streaming (Netflix, Amazon Prime e afins).

Os serviços de comunicação instantânea serão permitidos desde que, sejam os homologados pela ICRO Solutions (Microsoft Teams).

O acesso às redes sociais (Facebook, Instagram e afins) não serão permitidos salvo, para aqueles usuários autorizados e que tenham relação direta com o uso dessas plataformas para realizar suas atividades no interesse da ICRO Solutions.

Não é permitido acesso a sites de proxy externo ou transparentes, somente aqueles que sejam implementados diretamente pela ICRO com a finalidade de regular e filtrar o acesso a conteúdo da internet.

Uso das Credenciais de Identificação

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 ICRO Solutions 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).**

Esta norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada e seguida, indiscutivelmente, por todos os colaboradores.

Todos os dispositivos de identificação utilizados na ICRO Solutions, 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 organização e a legislação (cível e criminal). Todo e qualquer dispositivo de

identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Não será permitido o uso compartilhado de login e senha por mais de um colaborador. Cada colaborador precisa ter um acesso físico ou lógico individualizado que permita sua correta identificação no uso dos recursos.

Também não é permitido compartilhamento de login e senha para as funções de administração tecnológica do ambiente (infraestrutura e sistemas).

A área de Recursos Humanos ou outro departamento administrativo da ICRO Solutions será responsável pelo controle dos documentos físicos de identidade dos colaboradores bem como, o provisionamento de crachás de identificação contendo obrigatoriamente:

- Nome completo do colaborador;
- Número de matrícula do colaborador;
- Cargo ou função do colaborador.

A área de Tecnologia da Informação será responsável pela criação da identidade lógica dos colaboradores (login e senha) bem como, enquadramentos necessários para liberação do uso dos recursos da ICRO Solutions.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, 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:

- Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).
- Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo).

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.

As senhas não devem em hipótese alguma:

- Serem anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, post-it eletrônicos, etc.), compreensíveis por linguagem humana (não criptografados);
- Serem anotadas ou armazenadas em papéis, cadernos, post-it ou quaisquer outros locais onde os mesmos fiquem expostos ou com fácil acesso;
- Não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento;
- Não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário deverá ser bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de Tecnologia de Informação através dos meios disponibilizados para tal.

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. Para esses casos, também é essencial que o usuário notifique a Gerência de Tecnologia da Informação para as devidas tratativas conforme previsto nesta PSI.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou

comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade). A periodicidade máxima para troca das senhas é 60 (sessenta) dias, não podendo ser repetidas as 3 (três) últimas senhas.

Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas também a cada 60 dias. Os sistemas devem permitir forçar a troca das senhas dentro desse prazo máximo. Caso não permitam, deverão ser criados lembretes de alteração para serem executados.

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 ou o responsável por esse trâmite dentro da ICRO Solutions, deverá imediatamente comunicar tal fato à Gerência 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.

Uso dos Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores e/ou prestadores de serviço são de propriedade da ICRO Solutions, salvo casos previstos, 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.

O uso de equipamentos pessoais (BYOD – Bring your own device) será permitido desde que, as seguintes medidas sejam adotadas pelo colaborador e/ou prestador de serviços:

- Formatação do equipamento com instalação de sistema operacional homologado e licenciado;
- Imediata inclusão do dispositivo no ambiente de domínio da ICRO Solutions, estando assim, em conformidade com todas as políticas e regras de uso aplicadas aos dispositivos;
- Imediata instalação de aplicativos homologados e licenciados ao usuário, para execução de suas atividades no interesse da organização, garantindo assim a conformidade regulatória e os requisitos para execução de seu papel;
- Imediata instalação dos aplicativos destinados ao inventário de hardware e software bem como os de cunho protecional (antivírus, antimalware e afins);
- Quando do desligamento do colaborador ou prestador de serviços, seu dispositivo pessoal deverá passar por uma rotina de backup permitindo a salvaguarda dos dados e informações que pertencem a ICRO Solutions. O backup deverá ser apresentado para o responsável pela guarda e uso daquelas informações;
- Na sequência o dispositivo deverá passar por toda baixa de licenciamento de software e após isso, a formatação da estação de trabalho.

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 Tecnologia da Informação.

As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Tecnologia da Informação, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Somente poderão ser instalados nos dispositivos corporativos, softwares homologados pela ICRO e para os casos dos softwares licenciados, com licença disponibilizada para uso.

Não será permitido o uso de nenhum tipo de sistema, software ou aplicativo em condição denominada “beta” ou “em fase de testes” nos dispositivos.

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 oficial pelo fabricante ou fornecedor.

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 a Gerência de Tecnologia da Informação mediante registro de chamado.

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.

Arquivos pessoais e/ou não pertinentes ao negócio da ICRO Solutions (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 serão excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

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.

Os colaboradores da ICRO Solutions 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 Tecnologia da Informação.

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

- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- 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 Tecnologia da Informação;
- Os dispositivos como pen drives, CDs e DVDs poderão ser utilizados desde que existam rotinas de verificação destes dispositivos para identificação de ameaças como vírus, worms, trojans e afins;
- O colaborador deverá manter a configuração do equipamento disponibilizado pela ICRO, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da organização, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados), todos os terminais de computador;
- Todos os recursos tecnológicos adquiridos pela ICRO Solutions, devem ter imediatamente suas senhas padrões (default) 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 da ICRO Solutions:

- 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.

Uso dos Dispositivos Móveis

Com o objetivo de facilitar a mobilidade e o fluxo de informação entre os colaboradores, a ICRO Solutions permite que os mesmos utilizem equipamentos portáteis. Para tal, trataremos “dispositivo móvel” como qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Tecnologia da Informação, tais como: notebooks, smartphones, tablets 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.

Na qualidade de proprietária dos equipamentos fornecidos ou ainda do ponto de vista das características condicionadas aos dispositivos BYOD, onde os mesmos encontram-se dentro da norma prevista nesta política, a ICRO Solutions reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

Diante disso, o colaborador ou prestador de serviços, 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 na ICRO Solutions, mesmo depois de terminado o vínculo contratual mantido com a organização.

É responsabilidade de cada colaborador realizar periodicamente cópia de segurança dos dados de seu dispositivo móvel.

O suporte técnico aos dispositivos móveis de propriedade da ICRO Solutions e aos seus usuários deverá seguir o mesmo fluxo de suporte das estações de trabalho, sendo de responsabilidade da área técnica.

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

A instalação de aplicativos corporativos homologados é autorizada por padrão.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

Não é permitida a instalação de aplicativos terceiros que não forem homologados pela Gerência de Tecnologia da Informação.

Não é permitida a instalação de softwares ou aplicativos corporativos da ICRO Solutions em smartphones ou tablets pessoais.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela ICRO Solutions, notificar imediatamente seu gestor direto e a Gerência de Tecnologia da Informação. 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 a ICRO Solutions ou terceiros.

Uso dos Arquivos Compartilhados e File Server

Os ambientes denominados File Server (compartilhamento de arquivos) deverão ser administrados de maneira efetiva e com aplicação de práticas de liberação de acesso.

Deverão ser criadas pastas departamentais como repositório oficial dos arquivos de cada departamento. As seguintes regras deverão ser implementadas para essas pastas:

- As pastas deverão ser diferenciadas de acordo com a classificação da informação a ser armazenada naquela pasta;
- O acesso à essas pastas serão gerenciadas mediante a criação de grupos de acesso específicos;
- Os grupos de acesso deverão apresentar atributos com permissões de leitura, edição ou controle total;
- Os usuários precisarão ser inclusos nos grupos aos quais sua permissão esteja claramente definida.

Deverão ser criadas pastas individuais como repositório oficial dos arquivos de cada colaborador. As seguintes regras deverão ser implementadas para essas pastas:

- O acesso a essa pasta será concedido exclusivamente ao colaborador para armazenar seus arquivos corporativos;
- A liberação de acesso às pastas ou arquivos dentro da estrutura individual de cada colaborador, será feita mediante compartilhamento direto com outros usuários;

- Será de responsabilidade do colaborador, atribuir o tipo de permissão que desejar aos arquivos e pastas que estiver compartilhando;
- Ainda com relação às permissões, o colaborador “owner” ou proprietário do arquivo, será responsável por quaisquer cenários decorrentes desse compartilhamento, como por exemplo, alterações que tenham sido feitas em documentos por outros usuários com os quais o mesmo compartilhou aquele arquivo ou pasta.

Acesso remoto

Será permitido aos colaboradores e prestadores de serviço da ICRO Solutions, utilizar remotamente os recursos e serviços de TI disponibilizados para as atividades diárias. Para tanto, algumas regras deverão ser observadas:

- Os colaboradores que necessitarem de acesso remoto ao ambiente, deverão registrar chamado solicitando a liberação;
- Caberá ao gestor do solicitante e a Gerência de Tecnologia da Informação, nessa ordem respectivamente, aprovar ou não a liberação do acesso remoto;
- Uma vez aprovado o acesso remoto, este deverá ser feito através de cliente VPN homologado para tal finalidade pela ICRO Solutions;
- Para gerenciar os colaboradores que terão esse tipo de acesso, deverá ser criado um grupo de acesso para inclusão destes.

Os times de Operações e Projetos que precisarem acessar remotamente o ambiente de clientes para implementação de projetos ou suporte a serviços contratados, deverão instalar e realizar o acesso através de clients de VPN específicos que cada cliente possuir ou definir, respeitando as PSI de cada cliente.

Os times de Operações e Projetos que precisarem dentro de VPN, acessar dispositivos como notebooks, estações de trabalho, servidores, etc., deverão realizar os acessos conforme estipulado na PSI de cada cliente, salvo os casos onde, não existir PSI no cliente ou quando orientação do cliente for diferente desta.

É permitido o uso de aplicativos como Team Viewer ou Anydesk para acessar estações de trabalho, servidores e demais dispositivos, desde que, sejam tomadas precauções para garantir a proteção de acesso à informações sensíveis no lado do cliente.

Backup

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.

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.

Os repositórios de backup deverão ser providos diretamente em ambiente Cloud, facilitando assim a disponibilidade dos dados a partir de qualquer local.

Eventualmente deverão ser realizados testes de integridade com os arquivos de backup tendo como objetivo garantir a pronta recuperação do ambiente caso necessário. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, paraque assim, não sobreponha os arquivos válidos.

O acesso ao repositório Cloud onde estão armazenados os backups, precisam ser concedidos somente a pessoal técnico autorizado.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle de execução dessas rotinas, o qual deverá ser preenchido pelos colaboradores responsáveis e pela Gerência de Tecnologia da Informação. Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha deresponsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivosde força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

Conclusões

Todas as normas, politicas e procedimentos da Icro Solutions são consideradas material intelectual da empresa e devem ser acessados apenas por pessoas com as devidas autorizações. Demais duvidas referentes ao material contido neste documento devem ser tratadas através do canal de e-mail dpo@icrosolutions.com.