



Política de Segurança e privacidade da informação

**SEUS DADOS
ESTÃO PROTEGIDOS**

SUMÁRIO

- Termos e definições	pag. 3
- O que é informação?	pag. 4
- O que é segurança e privacidade da informação?	pag. 4
- Objetivo da Política de Segurança e Privacidade da Informação da CONTREI	pag. 4
- Vantagens da Política de SISTEMA DE GESTÃO INTEGRADO aos colaboradores e clientes da CONTREI	pag. 5
- Quem é responsável pela Política de Segurança e Privacidade?	pag. 6
- Comitê gestor de SISTEMA DE GESTÃO INTEGRADO - SGI	pag. 6
- Como acessar a Política de Segurança e Privacidade da Informação?	pag. 6
- Análise, avaliação e tratamento de riscos	pag. 7
- Organização da segurança e privacidade da informação	pag. 8
- Gerenciamento de ativos	pag. 9
- Classificação da informação	pag. 10
- Segurança Física e do Ambiente	pag. 11
- Gerenciamento das Operações e Comunicações	pag. 12
- Controle de acesso	pag. 14
- Gerenciamento de Incidentes de Segurança e Melhorias	pag. 15

Sistema de Gestão da Privacidade da Informação – o SGI

TERMOS E DEFINIÇÕES

- **SGI** - considera segurança da informação e a proteção da privacidade da CONTREI
- **Encarregado de Dados:** pessoa indicada pela CONTREI para ser responsável pelo SGI e atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- **Comitê de Segurança e Privacidade da Informação – CSPI:** Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da CONTREI, que tem por finalidade tratar questões ligadas ao SGI.
- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- **Gestor da Informação:** Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.
- **Usuário da informação:** Empregados com vínculo empregatício de qualquer área da CONTREI ou terceiros alocados na prestação de serviços a CONTREI, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação da CONTREI para o desempenho de suas atividades profissionais.
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.



Iniciando...

O QUE É INFORMAÇÃO?

Informação é a resultante do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema que a recebe. O valor da informação varia conforme o indivíduo, as necessidades e o contexto em que é produzida e compartilhada. Uma informação pode ser altamente relevante para um indivíduo e a mesma informação pode não ter significado algum para outro indivíduo. Informação enquanto conceito carrega uma diversidade de significados, do uso cotidiano ao técnico. Genericamente, o conceito de informação está intimamente ligado às noções de restrição, comunicação, controle, dados, forma, instrução, conhecimento, significado, estímulo, padrão, percepção e representação de conhecimento. O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.

O QUE É SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO?

A segurança e privacidade da informação garante a proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

São propriedades básicas do SGI: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

A segurança e privacidade da informação não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção de informações e dados. De um modo geral, um SGI eficaz também garante à direção e a outras partes interessadas que os ativos da organização estejam seguros e protegidos contra danos, agindo como um facilitador dos negócios.

ENTÃO, O QUE É E QUAL O OBJETIVO DA POLÍTICA DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO DA CONTREI?

O objetivo do SGI é garantir a gestão sistemática e efetiva dos aspectos relacionados à segurança e privacidade da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos à instituição. A CONTREI atende integralmente à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Alta Direção, gestores e colaboradores são comprometidos com uma gestão efetiva de Segurança e privacidade da Informação na CONTREI. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas são realizadas para garantir sua contínua pertinência e adequação às necessidades da CONTREI.

CONFIRA AS VANTAGENS DA POLÍTICA DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO AOS COLABORADORES E CLIENTES DA CONTREI

Protegemos seus dados através de diversas práticas e tecnologias, como:

- **Autenticação do usuário**
- **Requisitos e manutenção de senhas**
- **Criptografia de dados**
- **Políticas de privacidade**
- **Residência dos dados**
- **Controles de segurança física**
- **Frequências de backup**
- **Segurança de rede**
 - o Testes
 - o Firewall
 - o Registro de auditoria
 - o Criptografia em trânsito
- **Administração de vulnerabilidades**
 - o Aplicação de patch
 - o Varreduras de terceiros
 - o Testes de invasão
- **Segurança organizacional e administrativa**
 - o Políticas de segurança de informações
 - o Comprometimento e treinamento dos funcionários
 - o Prestadores de serviços
- **Acesso**
 - o Acesso a sites de terceiros
 - o Registro de auditoria
 - o Práticas de desenvolvimento de software
 - o Certificados e conformidades
 - o Resolução de violações de segurança



Quem é responsável pela política de segurança e privacidade?

A alta direção estabelece a política de segurança e privacidade da informação e está comprometida com uma gestão efetiva do SGI na Contrei. Desta forma, junto com o ESPI e o comitê de segurança da informação, adota todas as medidas para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da Contrei. O comitê de segurança da informação, contando com a participação dos membros designados, conforme os cargos a seguir:

- Analista de Qualidade (ESPI)
- Consultor Externo de TI
- Coordenador(a) de Projetos e Qualidade
- Gerente de Software
- Gerente Operacional
- Gerente de Pós Vendas

Encarregado de segurança e privacidade da informação: pessoa indicada pela Contrei para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional de proteção de dados (ANPD) e conduzir a gestão e operação do SGI, tendo como base esta política e demais resoluções do SGI.

A CONTREI:

- Orienta quanto à adoção de controles e processos para atendimento dos requisitos para SISTEMA DE GESTÃO INTEGRADO;
- Resguarda as informações da CONTREI, garantindo re- requisitos básicos de confidencialidade, integridade e disponibilidade;
- Previne possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;
- Minimiza os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro

impacto negativo no negócio da CONTREI como resultado de falhas de segurança

- Elabora, implanta e segue por completo políticas, normas e procedimentos do SGI, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da CONTREI sejam atingidos através da adoção de controles, contra ameaças provenientes de fontes tanto externas quanto internas;
- Disponibiliza políticas, normas e procedimentos de segurança e privacidade a todas as partes interessadas e autorizadas, além de garantir a educação e conscientização sobre as práticas adotadas pela CONTREI de segurança e privacidade da informação para colaboradores, terceiros contratados e, onde pertinente, clientes;
- Atende requisitos de SISTEMA DE GESTÃO INTEGRADO aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
- Trata de incidentes de SISTEMA DE GESTÃO INTEGRADO, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;
- Garante a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
- Melhora continuamente a Gestão do SGI através da definição e revisão sistemática de objetivos de segurança e privacidade em todos os níveis da organização.

COMO ACESSAR A POLÍTICA DE SEGURANÇA? Clientes e parceiros: O acesso à política se dá através do menu A CONTREI >> Segurança e Privacidade, presente no site da CONTREI:

Colaboradores:

A política de segurança e privacidade da CONTREI pode ser acessada através do Site: através do menu A CONTREI >> Segurança e Privacidade, presente no site da CONTREI e também Através da Plataforma de treinamentos interna(You RH).

“Site Contrei”



“Plataforma de treinamentos interna(You RH)”



CONCEITO DE RISCO



ORGANIZAÇÃO DA SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

O apoio da diretoria para uma assertiva e efetiva política de segurança é fundamental.

E, aqui, na CONTREI, prezamos por isso!

A área do SGI busca recursos junto à alta gestão da CONTREI para minimizar riscos e ameaças, além de orientar para que todas as áreas da instituição mantenham atividades que colaboram para a efetividade do trabalho voltado a segurança e privacidade da informação.

Toda a informação produzida é de responsabilidade de cada um dos geradores das mesmas. É importante salientar que o comprometimento com a política de SGI é a ação que permeia e valida toda a sua eficácia.

A organização do SGI também é um aspecto primordial. Por isso, é importante que todos os recursos utilizados para acesso às informações tenham controle de pessoas que podem acessá-los, ou ainda que possuam restrições para um número exato de pessoas, isso vale tanto para colaboradores quanto para terceiros.

A política de SGI é assegurada por lei e precisa ser seguida conforme estabelecida. Para tanto, nos valemos dos acordos de confiabilidade, juridicamente válidos, realizados entre a CONTREI e colaboradores, terceiros, fornecedores, ou qualquer outro público interno ou externo que esteja envolvido de alguma forma nos processos.



Gerenciamento de ativos

ENTENDENDO O CONCEITO DE “ATIVO DE INFORMAÇÃO”

O nome “Ativo” talvez não seja muito familiar a você, mas é muito utilizado no texto da norma ISO 27001. Por Ativo entende-se qualquer componente (seja humano, tecnológico, software ou etc,) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

Uma outra boa definição de Ativo é tudo aquilo que tem valor para a sua empresa. A ISO 27001 pede que todos os ativos relevantes sejam identificados e inventariados. Existe um pouco de confusão porque costumamos associar a expressão “inventário de ativos” ao usual inventário de hardware e software.

Quando o assunto é SISTEMA DE GESTÃO INTEGRADO, por “inventário de ativos” devemos compreender um conjunto mais abrangente de ativos, que contempla sistemas, pessoas, ambientes físicos entre outros.

Para manter todos esses ativos (físicos ou não) cria-se controles, para tanto, daí a necessidade de gerenciá-los.

Dessa forma devemos:

- Definir claramente os proprietários pelos ativos da CONTREI e suas responsabilidades;
- Definir claramente as regras para que seja permitido o uso de informações e de ativos associados.



CLASSIFICAÇÃO A INFORMAÇÃO?

Em geral, a classificação dada à informação é uma maneira de determinar como esta informação vai ser tratada e protegida, identificando sua criticidade para o negócio e garantindo sua:

- **Confidencialidade:** garantir que a informação seja acessível somente para aqueles que tenham autorização.
- **Integridade:** garantir que um conteúdo específico não seja alterado acidentalmente ou por pessoas mal intencionadas.
- **Disponibilidade:** garantir que os usuários autorizados tenham acesso às informações e ativos associados quando necessário. É muito importante considerar que, para classificação de uma informação o responsável deve conhecê-la a fim de não produzir um rótulo erroneamente.

CATEGORIA/	GUIA DE MANUSEIO						
	DESCRIÇÃO	DOCUMENTOS / REGISTROS DE AMOSTRA	RESPONSÁVEIS	ARMAZENAMENTO	REPRODUÇÃO	DISTRIBUIÇÃO	DESTRUIÇÃO / ELIMINAÇÃO
PÚBLICO - Nenhuma marcação	Informação oficialmente liberada pela CONTREI para o público geral. A divulgação deste tipo de informação não causa problemas a CONTREI ou a seus clientes, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade.	Materiais de marketing autorizados para lançamento público, como anúncios, brochuras, contas anuais publicadas, páginas da Web na Internet, catálogos, avisos de vagas externos	Gestor da Informação: responsável pela integridade e distribuição. Usuário: manter a integridade da informação.	Sem restrições	Sem restrições	Sem restrições	Reciclagem / lixo
USO INTERNO - Aplicar no canto superior direito de cada página.	Informação liberada exclusivamente para usuários e departamentos específicos da CONTREI, não podendo ser compartilhada com o público em geral. Estas informações só podem ser compartilhadas mediante autorização do Gestor da Informação.	A maioria das informações corporativas se enquadra nesta categoria. Memorandos departamentais, informações em quadros de avisos internos, materiais de treinamento, políticas, procedimentos operacionais, instruções de trabalho, diretrizes, listas telefônicas e de e-mail, informações de marketing ou promocionais (antes do lançamento autorizado), opções de investimento, dados de transações, relatórios de produtividade, relatórios disciplinares, contratos, Acordos de Nível de Serviço, avisos de vagas internos, páginas da Web da intranet	Gestor da Informação: responsável pelas marcações adequadas. Usuário: responsável pelo armazenamento adequado e controle de documentos.	Físico: Permitido em locais de acesso restrito aos interessados. Eletrônico: Permitido em qualquer tipo de armazenamento, desde que limitado o acesso (Exemplo: Aplicando permissão NTFS, senha de arquivos etc.)	Cópias limitadas podem ser feitas apenas por funcionários ou por contratados e terceiros que assinaram um acordo de não divulgação apropriado.	Interno: Entregar em mãos, se possível. Externo: use um envelope de correios. Verbal: Permitido nas dependências da empresa, entre os interessados. Eletrônico: use o sistema de e-mail interno. A criptografia é necessária para transmissão para endereços de e-mail externos.	Documentos em papel: Destruir. Dados eletrônicos: apagar ou desmagnetizar a mídia magnética. Envie CDs, DVDs, discos rígidos mortos, laptops etc. para a TI para descarte apropriado
CONFIDENCIAL - Aplicar no canto superior direito de cada página.	Informação de caráter sigiloso, podendo ser comunicada exclusivamente a usuários especificamente autorizados e que necessitem conhecê-las para o desempenho de suas tarefas profissionais na CONTREI. A divulgação ou alteração não autorizada desse tipo de informação pode causar graves danos e prejuízos para a CONTREI e/ou seus clientes, portanto seu compartilhamento deve ser restrito e feito de maneira controlada.	Senhas e códigos PIN, tokens VPN, números de cartão de crédito e débito, Dados pessoais (como registros de RH de funcionários, números de previdência social etc.), a maioria dos dados contábeis, outras informações proprietárias altamente confidenciais ou valiosas, informações que só interessam aos proprietários dos dados.	Gestor da Informação: responsável por garantir que as informações confidenciais sejam distribuídas com base na estrita necessidade de conhecimento. Usuário: responsável por garantir que as informações confidenciais sejam criptografadas e / ou mantidas trancadas e fechadas quando não estiverem em uso.	Físico: Armazenado em local de acesso controlado. Eletrônico: Permitido em locais de armazenamento controlados. (Exemplo: Aplicando permissão NTFS, senha de acesso a arquivos etc.)	Cópias limitadas podem ser feitas apenas com a permissão do Proprietário ou de seus Destinatários. Será solicitado por e-mail.	Interno: use um envelope lacrado. Entregar em mãos, se possível. Externo: use um envelope lacrado. Entregar em mãos ou enviar por correio registrado, correio etc. Verbal: Permitido somente em ambiente em que os interessados estiverem. Proibido em locais públicos. Eletrônico: use apenas o sistema de e-mail interno. Dados criptografados. confirmação de recebimento	Documentos em papel: desfile usando um triturador de corte transversal aprovado. Dados eletrônicos: apagar ou desmagnetizar a mídia magnética. Envie CDs, DVDs, discos rígidos mortos, laptops etc. para a TI para descarte adequado.

Segurança Física e do Ambiente

As instalações de processamento das informações da CONTREI serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.

É importante observar as seguintes disposições específicas quanto à segurança física:

- Na chegada de visitantes, os mesmos serão recebidos e direcionados pela recepcionista ou pelo responsável pela visita. O indivíduo deverá estar acompanhado durante todo o seu trajeto dentro das dependências da CONTREI;
- Exceto se formalmente autorizados, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;
- É proibida qualquer tentativa de se obter ou permitir o acesso de indivíduos não autorizados a áreas sensíveis da CONTREI;
- A CONTREI verifica junto aos visitantes, a existência de quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis. Nesses casos, procedimentos específicos são orientados;
- A CONTREI monitora seus ambientes físicos utilizando sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas são armazenadas e protegidas contra qualquer tipo de acesso / manipulação indevida;
- Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas, assim, ao se ausentar cabe ao usuário mantê-los guardados ou descartá-los de acordo com os procedimentos determinados pela CONTREI;
- É permitido consumir qualquer tipo de alimentos nas áreas designadas, e nunca nas áreas sensíveis.



Gerenciamento das Operações e Comunicações

Para atender os requisitos de SGI, as ações são arquitetadas através do planejamento, implementação e controle.

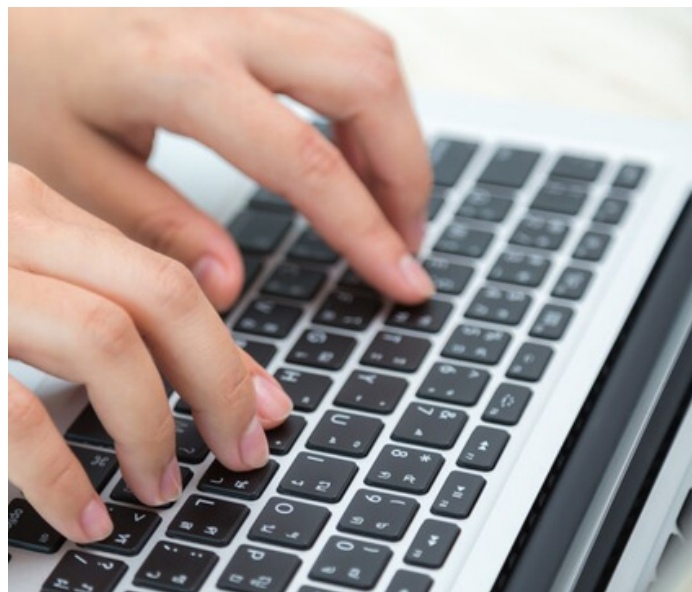
Outra nuance importante da segurança e privacidade é a organização que precisa ser mantida quanto a documentação de toda informação gerada. Isso gera confiabilidade dos processos e a certeza de que os trâmites estão sendo realizados de acordo com o que foi estruturado.

A CONTREI é a responsável por controlar todas as mudanças planejadas, bem como analisar minuciosamente as consequências das mudanças não previstas. É necessário tomar iniciativas para minimizar quaisquer adversidades nesse sentido.

Aqui na CONTREI, utilizamos Documentos Técnicos (DTO) e Políticas para a gestão das informações de segurança e privacidade. Abaixo, segue a lista das Políticas da segurança e Privacidade dos dados:

Abaixo, segue a lista:

- POL 000-23 Política Integrada
- POL 001-23 Política Geral de Segurança da Informação
- POL 002-25 Política de Nomeação do ESPI
- POL 003-25 Política de Nomeação do CSPI
- POL 004-25 Política de Gestão de Segurança de Redes e Sistemas
- POL 005-25 Política de Gestão de Continuidade de Negócios e Resiliência
- POL 007-25 Política de Gestão de Fornecedores e Terceiros
- POL 008-25 Política de Gestão de Incidentes e Resposta a Eventos de Segurança
- POL 009-25 Política de Conformidade e Requisitos Legais
- POL 010-25 Política de Gestão de Pessoal e Conscientização em Segurança
- POL 011-25 Política de Gestão de Ativos e Inventário
- POL 012-25 Política de Gestão de Mudanças e Configurações
- POL 013-25 Política de Gestão de Acesso e Identidade
- POL 014-25 Política de Gestão de Segurança de Dados e Informações
- POL 015-25 Política de Gestão de Segurança Física e Ambiental
- POL 016-25 Política de Cookies



POR QUE ESSE GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES?

Quando gerenciamos as operações limitando o uso de mídias removíveis, acesso, conexões remotas, dentre outros, estamos prevenindo que informações sejam acessadas por pessoas não autorizadas.

Quais os riscos associados ao depararmos com situações de trabalho conforme abaixo?



Se você não conseguiu identificar pelo menos 01 erro evidente, está na hora de você rever nossa política de SGI.

Nessa imagem, existem 5 erros que impactam diretamente na confidencialidade, integridade e ou disponibilidade da informação.

Gerenciamento das Operações e Comunicações (continuação)

“VOCÊ AINDA ACHA QUE NÃO TEM NADA ERRADO?”



	IMPACTO	VIOLAÇÃO	RISCOS	POLÍTICA SUGERIDA
1	Além da mesa de trabalho	Cesto de lixo com papéis não destruídos	Documentos sensíveis no lixo podem ser roubados fora do expediente ou serem recuperados em depósitos fora da empresa.	Destrua os documentos impressos antes de descartá-los.
2	Ferramentas de TI	Senhas expostas no computador	Acesso a mensagens eletrônicas (pessoais ou corporativas) ou senhas podem permitir acesso à intrusão.	- Feche aplicativos e desligue ou trave seu monitor quando deixar sua mesa; - Habilite o protetor de telas protegido por senha; - Desligue seu computador quando sair da sala por longos períodos; - Limpe arquivos de cache regularmente; - Nunca deixe senhas visíveis ou anote as mesmas.
3	Informação proprietária	Senha sendo falada ao telefone	Informações pessoais e profissionais, incluindo senhas em geral, estão vulneráveis.	Nunca fale sua senha ao telefone ou compartilhe essa informação com colegas.
4	Ferramentas de acesso	Pendrive sendo entregue a um estranho	Pendrives podem ser roubados contendo dados históricos comprometidos. O acesso a áreas restritas por intrusos pode ocasionar esses roubos.	- Mantenha equipamentos como esse com você, nunca deixando-os disponíveis em qualquer lugar; - Notifique o pessoal da segurança imediatamente caso note o desaparecimentos desse tipo de mídia.
5	Ferramentas de acesso	HD sobre a mesa	HDs podem ser roubados contendo dados históricos comprometidos. O acesso a áreas restritas por intrusos pode ocasionar esses roubos.	- Mantenha equipamentos como esse com você, nunca deixando-os disponíveis em qualquer lugar; - Notifique o pessoal da segurança imediatamente caso note o desaparecimentos desse tipo de mídia.

Controle de acesso

Toda informação relevante e confidencial deve ser protegida. Por isso, a CONTREI trabalha várias formas de controle de acesso.

Acesso a ativos e sistemas de informação

- A CONTREI fornece a seus colaboradores autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa; As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;
- Toda conta de acesso é pessoal e intransferível. Desta forma, o colaborador é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso, cabendo uma análise da infração pelo SGI e aplicação das sanções e punições previstas na Política Geral de SISTEMA DE GESTÃO INTEGRADO, conforme a gravidade da violação.



Senha de acesso

As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da CONTREI são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo. Nossa política prevê os padrões e cuidados que devem ser tomados por parte do colaborador para a segurança dessa informação.

Autorização de acesso (privilégios de acesso)

A autorização e o nível permitido de acesso ativos/serviços de informação da CONTREI é feita com base em perfis que definem o nível de privilégio dos usuários, de acordo com as necessidades laborais dos colaboradores.

Gerenciamento de Incidentes e Melhorias

Incidentes de segurança e privacidade

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da CONTREI serão caracterizadas como um incidente de SISTEMA DE GESTÃO INTEGRADO, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de SISTEMA DE GESTÃO INTEGRADO dos itens afetados.

Todos os incidentes de SISTEMA DE GESTÃO INTEGRADO ou suspeitas de incidentes de SISTEMA DE GESTÃO INTEGRADO devem ser imediatamente comunicados a área de SISTEMA DE GESTÃO INTEGRADO.

Após a erradicação completa do incidente, é realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

Plano de continuidade de negócios

A CONTREI determina seus requisitos para a SISTEMA DE GESTÃO INTEGRADO/privacidade e a continuidade da gestão em situações adversas, por exemplo, durante uma crise ou desastre, através do Plano de Continuidade do Negócio.

Melhorias

O Sistema SGI da CONTREI tem as melhorias e a busca da eficácia como principal foco. Para isso são utilizados: auditorias internas e externas, análise crítica da gestão, indicadores, testes de invasão, ações de correção e corretivas, além de uma extensa matriz, compreendendo dezenas de controles para o atingimento dos objetivos e a manutenção segura dos níveis de serviço.



Para finalizar, esperamos que a explanação do tema de segurança e privacidade da informação sob a perspectiva do Sistema de Gestão SGI da CONTREI, tenha sido clara e objetiva. O principal intuito foi de instruir quanto aos principais aspectos da nossa política de SGI. E, certamente, colaborar com a qualidade, confiabilidade, segurança e privacidade de nossos processos.

Mais informações podem ser encontradas no Manual de Segurança e Privacidade da Informação.