	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

1. OBJETIVO

A Política de Segurança da Informação da Rede Cidadã – PSI-RC, foi preparada para definir os padrões mínimos obrigatórios para o devido uso e proteção das informações tratadas dentro da Rede Cidadã, sejam elas, criadas, recebidas, armazenadas, processadas ou impressas.

2. PRINCÍPIOS


Esta Política tem por princípio a proteção dos dados, informações e conhecimento, bem como a preservação dos direitos do uso de dados Pessoais com foco na Confidencialidade, Integridade e Disponibilidade.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

3. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, estagiários, jovens aprendizes, empregados, associados, voluntários e parceiros que tratam as informações na Rede Cidadã em âmbito nacional.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

4. DOCUMENTOS DE REFERÊNCIAS

NBR ISO/IEC 27002:2013

NBR ISO/IEC 27001:2013

5. TERMOS E DEFINIÇÕES

Para os efeitos desta política, aplicam-se os seguintes termos e definições.

- Ativo

Qualquer coisa que tenha valor para a organização, como Hardware, Software, Documentos, etc.

- Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

- Confidencialidade


Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

- Integridade

Propriedade de salvaguarda da exatidão e completeza de ativos.

- Segurança da informação

É a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

- Não-Repúdio

Ato de evitar que uma entidade negue a execução de uma ação.

- Incidente de segurança da informação

Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

- Colaboradores

São todos os empregados, estagiários, jovens aprendizes, associados, voluntários e parceiros que direta ou indiretamente prestam serviços para a Rede Cidadã.


- PSI-RC

Política de Segurança da Informação da Rede Cidadã.

6. DIRETRIZES

I - Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários, de acordo com privilégios estabelecidos em seu perfil, acessar arquivos e dados de outros usuários, sendo que só será permitido quando for estritamente necessário para a execução de suas atividades e caberá a si garantir o sigilo da informação de acordo com sua classificação.

II - Assegurar que a contratação de serviços relevantes de processamento e armazenamento de dados contemple as políticas, estratégias e estruturas necessárias para o adequado gerenciamento dos riscos quanto à terceirização de serviços.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

III - Comunicar imediatamente à área de Tecnologia da Informação, bem como a Diretoria e seu coordenador imediato, qualquer violação desta política de segurança da informação, a fim de se aplicar as medidas de remediação e penalidades cabíveis.

IV - Os contratos e termos de confidencialidade e/ou responsabilidade devem ser respeitados por todos os colaboradores da Rede Cidadã.

V - A segurança da informação deve fazer parte da rotina diária dos colaboradores da Rede Cidadã a fim de garantir confidencialidade, integridade e a disponibilidade da informação.

VI - Os gestores das áreas devem analisar e auxiliar seu subordinados e prestadores de serviços a classificar as informações de acordo com o item 10 desta política.


VII - Esta Política de Segurança da Informação deverá ser revisada no mínimo uma vez por ano e as alterações que por ventura forem necessárias, deverão ser amplamente divulgadas aos colaboradores.

VIII - A diretoria da Rede Cidadã participa ativamente e aprova as normas e procedimentos definidos na PSI-RC.

IX - O não cumprimento do estabelecido nesta Política de Segurança da Informação poderá acarretar sanções administrativas disciplinares e/ou contratuais.

7. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

Equipe multidisciplinar formada pela Diretoria, Gerencia Administrativa Financeira e Coordenador de TI, cabendo a esta equipe, atualizar, divulgar e monitorar o cumprimento da Política de Segurança da Informação.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

8. POLÍTICAS E PROCEDIMENTOS INTERNOS

Os procedimentos a seguir integram a Política de Segurança da Informação da Rede Cidadã:

PI01 - Política de Uso de Senha

PI02 - Uso do Correio Eletrônico

PI03 - Registro e Resposta a Incidentes de Segurança da Informação

PI04 - Política de Gestão de Ativos e Tratamento de Mídias RC

PI05 - Política de Controle de Acesso

PI06 - Combate a Softwares Maliciosos

PI09 - Política de Mesa e Tela limpa

PI10 - Política de trabalho remoto


PI11 - Termo de Confidencialidade

FTI01 – Formulário de Registro de incidente de segurança da Informação

PCN01 – Plano de continuidade do Negócio

9. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Com o objetivo de disseminar o conhecimento e manter o comprometimento de seus empregados, estagiários, aprendizes, colaboradores, voluntários, associados e terceirizados, a Rede Cidadã mantém um processo anual de treinamento de Conscientização em Segurança da Informação. Este treinamento tem como escopo principal a divulgação da Política de Segurança da Informação, além de abordar assuntos como conceitos sobre Segurança da Informação, tipos de ataques cibernéticos mais comuns, tipos de vírus, dicas de segurança e as barreiras de proteção adotadas pela Rede Cidadã.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

10. CLASSIFICAÇÃO DA INFORMAÇÃO

Todo e qualquer documento produzido pela Rede Cidadã deverá ser classificado obedecendo os seguintes critérios, informação:

PÚBLICA - Informações cuja integridade não é vital, se forem divulgadas fora da Organização não trarão impactos aos negócios.

INTERNA - Informação cujo acesso externo deve ser evitado, entretanto se esses dados tornarem públicos, as consequências não serão críticas. Documentos classificados como INTERNOS devem ser protegidos de forma que somente o pessoal autorizado tenha acesso.

CONFIDENCIAL - As informações com essa classificação devem ser confidenciais dentro da Organização e fortemente protegidas contra acessos externos por se tratarem de dados que podem comprometer as operações normais.


11. TRATAMENTO DE DADOS PESSOAIS

11.1. OBJETIVO

Estabelecer procedimentos e padrões para o tratamento de dados pessoais nos meios físicos e digitais na Rede Cidadã com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade da pessoa física natural.

11.2. DEFINIÇÕES

Tratamento de Dados pessoais: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

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.

Encarregado de dados ou DPO: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

11.3. DIRETRIZ

a) **Propósito** - De acordo com os princípios da finalidade, adequação e necessidade, os dados pessoais só devem ser coletados e tratados pela Rede Cidadã para os propósitos específicos e legítimos que tenham sido informados ao titular de dados e sejam compatíveis com o contexto do tratamento. O tratamento deve ser limitado ao mínimo necessário para aquelas finalidades que foram informadas aos titulares.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

b) **Registro de Incidente de Segurança da Informação** - a Rede Cidadã deverá manter um plano escrito e estruturado para casos de ocorrência de incidentes envolvendo Dados Pessoais, contendo no mínimo os seguintes itens:


- Data e hora do incidente;
- Dados de contato do Encarregado pela Proteção de Dados
- Descrição do incidente;
- Descrição da natureza dos dados pessoais afetados;
- Informações sobre os titulares envolvidos
- Medidas técnicas e de segurança utilizadas para a proteção dos dados, preservando os segredos comercial e industrial;
- Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

c) **Termo de confidencialidade** – Todos os prestadores de serviços, subcontratadas e empregados que tenham acesso aos dados pessoais controlados pela Rede Cidadã deverão assinar um Termo de Confidencialidade e de conhecimento da Lei de Proteção de Dados Pessoais-LGPD.

d) **Diretos dos Titulares** – A Rede Cidadã garantirá todos os direitos dos titulares conforme Art. 18 de LGPD.

e) **Encarregado de proteção dados-DPO** – A Rede Cidadã coloca à disposição o canal dpo@redecidada.org.br para esclarecimentos de quaisquer dúvidas relacionadas ao tratamento de dados pessoais. As principais atribuições do DPO são:

- Acatar as reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

- Receber comunicações da autoridade nacional de proteção de dados e adotar providências;
- Orientar os empregados e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

f) Tratamento de Dados Pessoais Sensíveis

Os dados pessoais sensíveis deverão ser tratados com extrema confidencialidade e com o objetivo específico, de acordo com o informado aos titulares. Na geração de estatísticas de impacto social os dados sensíveis, quando cabíveis deverão ser anonimizados.

g) Descarte de dados pessoais


Quando descartados eletronicamente, deverão garantir impossibilidade da reversão.

Quando descartados fisicamente, deverão ser triturados de forma a garantir a impossibilidade de sua identificação.

h) Proteção do dado pessoal.

O dado pessoal deverá ser protegido contra acesso indevido. Quando armazenado eletronicamente, o sistema de controle de acesso deverá garantir que somente pessoas autorizadas tenha acesso e que seja registrado em log quem acessou, com registro de data e hora.

Quando o armazenamento for físico, os documentos deverão estar protegidos com chave e o controle de acesso registrado em formulário específico contendo, no mínimo, nome, local, data e hora da retirada da chave.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

f) Tipo de dados pessoais tratados

O tipo de dado pessoal tratado pela Rede Cidadã está descrito na Política de Tratamento de Dados Pessoais, estabelecendo a finalidade específica do tratamento, o período de retenção, a forma de obtenção do consentimento dos titulares e o processo de eliminação/esquecimento após o período de retenção.

12. REVISÃO E AUDITORIAS

A Equipe de Segurança da Informação da Rede Cidadã é responsável pela revisão regular desta Política com foco nas mudanças circunstanciais.

Esta Política é auditada pela Equipe de Segurança da Informação com o objetivo de verificar se a mesma está apropriada para assegurar os interesses da Organização e proteção de seus ativos.


13. OBJETIVOS DE CONTROLES

✓ Documento da Política de Segurança da Informação

Um documento da Política de Segurança da Informação deve ser aprovado pela direção, publicado e comunicado a todos os empregados, colaboradores e parceiros.

✓ Análise crítica da Política de Segurança da Informação

A política de segurança da informação deve ser analisada criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

✓ **Comprometimento da direção com a segurança da informação**

A Direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.

✓ **Acordos de confidencialidade.**

Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização.

✓ **Identificação dos riscos relacionados com partes externas.**


Os riscos para os recursos de processamento da informação e para a informação da organização oriundos de processos do negócio que envolvam as partes externas devem ser identificados e controles apropriados devem ser implementados antes de se conceder o acesso.

✓ **Identificando a segurança da informação quando tratando com os clientes.**

Todos os requisitos de segurança da informação identificados devem ser considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização.

✓ **Identificando segurança da informação nos acordos com terceiros.**

Os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou o acréscimo de produtos ou serviços aos recursos de processamento da informação devem cobrir todos os requisitos de segurança da informação relevantes.

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

✓ **Termos e condições de contratação.**

Como parte das obrigações contratuais, os empregados, colaboradores, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar suas responsabilidades e da organização para a segurança da informação.


14. PAPÉIS E RESPONSABILIDADES

As funções e responsabilidades associadas à segurança da informação estão definidas conforme matriz RACI a seguir:

Matriz RACI				
ATIVIDADES	FUNÇÕES			
	Equipe de Segurança da Informação	Gestor da Área	Gerente Administrativo	Usuário
Controlar e monitorar o cumprimento da Política de Segurança da Informação	R	I	I	I
Controlar o tratamento de Ativos	R	A	C	R
Acordos de Confidencialidade	C	R	A	I
Atualização da Política de Segurança da Informação	R	I	I	I

Legenda:

- R** – Responsável: Quem é designado para trabalhar na atividade ou executar a ação.
- A** – Autoridade: Quem tem a autoridade para tomar a decisão
- C** – Consultado: Quem deve ser consultado e participar da decisão
- I** – Informado: Quem deve receber a informação

	<p style="text-align: center;">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	Identificação	PSI-RC
		Versão	1.0
		Atualização	20/10/2020

15. HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
23/08/2020	1.0	Elaboração	Equipe de Segurança da Informação
21/10/2020	1.0	Aprovação	Fernando Almeida Alves
22/10/2020	1.0	Publicação	Equipe de Segurança da Informação

Matriz: Rua Alvarenga Peixoto, 295 - 5º Andar - Bairro Lourdes
Belo Horizonte / MG - CEP: 30180-120 - Telefone: (31) 3290-8000
redecidada@redecidada.org.br | www.redecidada.org.br

PSI-RC - Política de Seguraca Rede Cidadã_V1.pdf

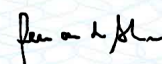
Código do documento 027bbe4b-60bc-4545-b7c2-357fba6018d4



Assinaturas



Fernando Almeida Alves
falves@redecidada.org.br
Aprovou



Eventos do documento

21 Oct 2020, 19:48:37

Documento número 027bbe4b-60bc-4545-b7c2-357fba6018d4 **criado** por AULERUSIA RENE ANDRADE CASSEMIRO (Conta a4db796e-a217-4eef-9432-13ca48983af5). Email :aulerusia.cassemiro@redecidada.org.br. - DATE_ATOM: 2020-10-21T19:48:37-03:00

21 Oct 2020, 19:49:54

Lista de assinatura **iniciada** por AULERUSIA RENE ANDRADE CASSEMIRO (Conta a4db796e-a217-4eef-9432-13ca48983af5). Email: aulerusia.cassemiro@redecidada.org.br. - DATE_ATOM: 2020-10-21T19:49:54-03:00

21 Oct 2020, 19:51:45

FERNANDO ALMEIDA ALVES **Aprovou** (Conta caff0fb5-07d5-4e1b-8d2f-fedab17716f1) - Email: falves@redecidada.org.br - IP: 201.80.194.75 (c950c24b.virtua.com.br porta: 7176) - Documento de identificação informado: 432.715.536-53 - DATE_ATOM: 2020-10-21T19:51:45-03:00

Hash do documento original

(SHA256):03ac3fd79705782db47c013634424740980a95ce5756d7aea370a2c65643f347

(SHA512):2f0ad2b8efd9199b22dc843d8e8f930c1363d3bc2d0268774917b46b7330dbb7653d7d5d07c2f6ed9bd174244adf0d4df4ee300909ba18139d59c5e80f8d4481

Esse log pertence **única e exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign