Código	Título	Versão	Publicação
POL - 0400	PSI - Política de Segurança da Informação	2	20/02/2022

1. Objetivo

Registrar as regras de segurança da informação atinentes à Gerência de Tecnologia da Informação da COBRAPE e estabelecer as diretrizes que devem ser observadas por seus colaboradores e colaboradores terceiros no intuito de salvaguardar a segurança destes dados de responsabilidade da empresa, bem como atender à legislação.

2. Histórico

Com o exponencial avanço da tecnologia, principalmente nas duas últimas décadas, as empresas e usuários ganharam acesso a um número antes inimaginável de informações com os mais diversos tipos de acesso e dispositivos. Nunca o termo “INFORMÁTICA” (que advém de informação automática), já quase em desuso, foi tão correto e atual. Junto com esse volume de informações, dispositivos e formas de acesso, surgiu também a necessidade de tratamento e gestão dos dados.
Governos de diversos países estão trabalhando para estabelecer regras alinhadas com essa nova perspectiva, a fim de manter a segurança de dados e a privacidade dos seus cidadãos. No Brasil, dentre outras, destaca-se a LGPD (Lei Geral de Proteção de Dados Pessoais) sancionada em 2018, entrando em vigor em agosto de 2020.
As empresas e seus profissionais precisam se ajustar a essa nova realidade. Neste sentido, a COBRAPE possui um conjunto de ações, regras e boas práticas que compõem esta Política de Segurança da Informação que, por sua vez, é regida por três pilares (confidencialidade, integridade e disponibilidade), definidos adiante.

3. Definições

3.1. Colaboradores da COBRAPE

Colaborador Próprio - refere-se a toda pessoa física, no Brasil ou no exterior, que tenha vínculo empregatício com a COBRAPE.

Colaborador Terceiro - (i) toda pessoa física ou jurídica, no Brasil ou no exterior, que preste serviços mediante contrato firmado com empresa interposta (prestador de serviço terceirizado); e, (ii) toda pessoa, física ou jurídica, com quem a COBRAPE mantenha qualquer forma de associação comercial ou consórcio para a prestação de serviços ao poder público e setor privado.

Colaborador - para efeito desta Política, engloba o colaborador próprio e o colaborador terceiro.

Gerência de Tecnologia da Informação (TI) - setor responsável por todas as questões relacionadas à Tecnologia da Informação, inclusive administrar a guarda dos acessos de todos os usuários que trafegam na rede da COBRAPE respeitando a LGPD e o Marco Civil da Internet.

Coordenadores de Contrato (CC) - colaboradores responsáveis pela condução de contratos do ponto de vista técnico, financeiro e operacional.

Diretoria (DT) - representam a última instância de decisão sobre as políticas e procedimentos da empresa.

3.2. Confidencialidade

A confidencialidade garante que a informação seja disponível e/ou acessível somente a pessoas ou processos autorizados.

3.3. Integridade

Garante a exatidão da informação.

3.4. Disponibilidade

Garante que as pessoas autorizadas tenham acesso a informação sempre que necessário.

4. Regras de Segurança da Informação

As diretrizes e/ou ações importantes para garantir os pilares da segurança da informação são indicadas a seguir:

4.1. Recursos de comunicação

Os recursos de comunicação homologados pela empresa compreendem hardwares e softwares disponibilizados pela COBRAPE como: desktops, laptops, smartphones, telefones e tablets, dentre outros.

A lista de ferramentas homologadas pela empresa para cada tipo de comunicação encontra-se disponível na intranet da COBRAPE http://intranet.cobrape.com.br e pode ser acessada por todos os colaboradores da empresa através de seu *login* e senha fornecidos.

As ferramentas de comunicação disponíveis devem ser utilizadas unicamente para o desenvolvimento de trabalhos e interesses da empresa, na jornada de trabalho de cada colaborador. Portanto, não devem ser utilizadas para executar trabalhos para outras empresas ou pessoas ou quaisquer outros fins que não os de interesse da COBRAPE. A utilização para fins pessoais como acesso a bancos, grupos de estudo, imposto de renda, entre outros, que requeiram a instalação de softwares adicionais, só é permitida após prévia autorização da TI.

Equipamentos particulares não devem ser utilizados para acesso aos dados da empresa. Exceção se faz:

- Na utilização de smartphones para acesso ao *e-mail* corporativo.
- Em equipamentos previamente homologados pela TI.
- Usuários que possuam acesso VPN.
- Sistemas que não requeiram VPN.
- Sistemas que tenham seu acesso WEB liberados.

Os colaboradores terceiros que necessitem utilizar seus dispositivos próprios terão seus acessos disponibilizados pela TI conforme as regras do projeto em questão através de rede específica para este fim.

O acesso a internet efetuado por dispositivos de terceiros será disponibilizado por rede WIFI específica. O sistema identifica o usuário e registro da utilização.

Todas as solicitações à TI devem ser efetuadas através de software específico de *help-desk,* para fins de registro, agilidade e análise de dados. O *help-desk* está disponível em diversas plataformas de acesso: Mobile (Android e iOS), WEB e Intranet. Saiba mais em http://intranet.cobrape.com.br.

4.2. Servidores de armazenamento e acesso

No momento da admissão, o colaborar recebe *login* e senha provisórios para acesso ao sistema da empresa. No primeiro acesso será apresentado um “termo de compromisso”, contendo as regras e políticas dos sistemas de informação, incluindo o direito da empresa ao acesso a conteúdos pessoais armazenados nos servidores e outros equipamentos da empresa.

O colaborador deverá assiná-lo digitalmente, concordando e dando ciência de seu conteúdo. Cada colaborador possui *login* e senha pessoais e intransferíveis, que possibilitam o ingresso a: portais, intranet, servidores, demais conexões e serviços da empresa. Inicialmente todo colaborador terá acesso somente ao ambiente padrão, no qual os dados disponíveis não possuem restrição de acesso.

Para acesso aos dados do seu setor ou projeto específico, o superior imediato do colaborador deverá autorizar a liberação, via *help-desk*, que será analisada pela TI. Os colaboradores devem salvar os dados nos servidores e/ou softwares disponibilizados pela empresa, sendo vetado o armazenamento de dados fora dos servidores e/ou softwares disponibilizados para tal finalidade.

Os colaboradores terceiros que necessitem utilizar a rede da empresa e/ou acessar a internet terão seu acesso disponibilizado pela TI conforme as regras do projeto em questão, através de rede específica para este fim.

A TI administra a guarda dos acessos de todos os usuários que trafegam na rede da COBRAPE respeitando a LGPD e o Marco Civil da Internet.

Os backups dos servidores e sistemas são de responsabilidade da TI e sua periodicidade pode ser consultada no portal da intranet em http://intranet.cobrape.com.br.

4.3. Compartilhamento e armazenamento em nuvem

As ferramentas de compartilhamento de arquivos em nuvem homologadas pela COBRAPE estão disponíveis aos colaboradores. Os tutoriais de acesso a esse recurso estão disponíveis em http://intranet.cobrape.com.br. Por motivos de segurança e atendimento às leis que regem a guarda da informação no Brasil, é vetada a utilização de softwares de compartilhamento de arquivos não homologados.

4.4. E-mail corporativo

A COBRAPE disponibiliza caixas de *e-mail* corporativo em nuvem para seus colaboradores e o acesso pode se dar de diversas formas: *WebApp*, *Mobile* e *softwares* de gerenciamento de *e-mails.*
Os colaboradores devem fazer uso da caixa de *e-mail* disponibilizada pela COBRAPE unicamente para troca de informações de interesse da empresa, quer seja entre os colaboradores da própria COBRAPE ou com seus parceiros e clientes.
É vetada a utilização de *e-mails* particulares para tratar de assuntos da empresa.
Os consórcios em que a COBRAPE participa recebem domínios próprios para utilização das caixas de *e-mail*. Os colaboradores devem fazer uso dessas caixas para tratar de assuntos do consórcio, mesmo quando o colaborador possuir *e-mail* da COBRAPE.
As caixas de correio não devem ser utilizadas como repositório de dados. Isto significa que os usuários devem salvar os documentos recebidos via *e-mail* nas respectivas pastas dos servidores de dados.
E-mails relevantes (aqueles que tratam de assuntos específicos de contratos com os clientes) devem ser encaminhados para as *"caixas de e-mail relevantes"*, que são criadas automaticamente para cada contrato. Aos CC cabe estabelecer procedimentos e orientar as equipes dos respectivos contratos, para que todos os *e-mails* relevantes sejam encaminhados e salvos adequadamente.

4.5. Licenciamento de software

A COBRAPE disponibiliza todas as licenças de software necessárias para o cumprimento das atividades do colaborador. É vetada a instalação de quaisquer softwares por parte do usuário, inclusive os que possuem licenças *free ou trial*, sem prévia homologação e anuência da TI.

5. Situações Especiais

Quaisquer exceções a esta política somente são permitidas se houver aprovação prévia e formal da DT.

6. Disposições finais

Qualquer dúvida sobre a aplicação desta política deve ser esclarecida junto à TI da COBRAPE.
Esta Política entra em vigor na data de sua publicação no *Espaço de Compliance*, acessível aos colaboradores pela Intranet corporativa.

7. Vigência

Esta Política entra em vigência na data de sua publicação.

8. Atualizações

Esta Política será revisada a cada 12 meses, e submetida à nova aprovação pela DT caso ocorram alterações.