POLÍTICA DE

SEGURANÇA DA INFORMAÇÃO

CIMENTO NACIONAL

SUMÁRIO

1. Objetivos

Este procedimento visa instruir e informar todos os pontos necessários para o conhecimento, avaliação, implementação e gerenciamento de riscos e controles do ambiente de Informática da Cimento Nacional, sendo aplicável a todos os usuários de equipamentos de informática da empresa, de seus colaboradores, terceiros, acionistas e clientes.

Identificar e gerenciar riscos de segurança da informação e implementar controles para mitigar o impacto do acesso não autorizado, uso indevido, modificação ou destruição de ativos de informação.

2. Termos e Definições

→ **CONFIDENCIALIDADE:** Propriedade da informação que objetiva garantir-lhe a não disponibilidade ou revelação a indivíduos ou entidades não autorizadas.

→ **DISPONIBILIDADE:** Propriedade da informação que lhe garante a possibilidade de ser disponibilizada a indivíduos ou entidades autorizadas.

→ **INFORMAÇÃO:** Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

→ **INTEGRIDADE:** Propriedade da informação que objetiva garantir-lhe a não alteração por indivíduos, entidades ou processos não autorizados.

→ **PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI):** Conjunto de diretrizes gerais da organização formalmente expressas com o objetivo de garantir a segurança da informação no âmbito da Empresa.

→ **SEGURANÇA DA INFORMAÇÃO:** Preservação da Confidencialidade, Integridade e Disponibilidade da Informação.

→ **TI OU TIC - TECNOLOGIA DA INFORMAÇÃO:** Área da Cimento Nacional responsável pela gestão e monitoramento da informação em seus diversos meios e dos recursos utilizados.

→ **USUÁRIO:** Qualquer pessoa que utilize sistemas e/ou demais recursos de TI, incluindo Colaboradores e Prestadores de Serviço.

3. Responsabilidade

3.1. *Responsabilidade Usuários*

→ Zelar pela proteção das informações da Empresa contra acesso, destruição ou divulgação não autorizados.

→ Proteger suas credenciais de acesso, a exemplo de senhas.

→ Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades definidas pela Empresa.

→ Cumprir as leis e normas que regulamentam a propriedade intelectual.

→ Comunicar imediatamente ao gestor da área de TI qualquer descumprimento desta Política de Segurança e/ou das normas e procedimentos a ela relacionados que tenham conhecimento.

3.2. *Responsabilidade Tecnologia da Informação*

→ Operacionalizar as normas e procedimentos relacionados a essa Política de Segurança por meio dos recursos de TI.

→ Assegurar que as Informações tenham cópias de segurança (backup), que os acessos lógicos e físicos sejam registrados, a exemplo, mas não se limitando, a trilhas de auditoria e logs.

→ Propor iniciativas para a melhoria do nível de segurança da informação na Empresa.

→ Garantir a implementação e cumprimento desta política e que ela esteja disponível para todos colaboradores e terceiros, quando apropriado, de forma que entendam as suas responsabilidades em proteger a confidencialidade, integridade e disponibilidade das informações da Cimento Nacional.

3.3. *Detalhamento da Política*

3.3.1. Responsabilidades dos Ativos de TI

→ Todo recurso de TI (Desktops, Notebooks, Smartphones, Licenças e acessos aos Sistemas) devem ter um proprietário designado e registrado com os formulários " RE - GG - 035 - Formulario Termo de Responsabilidade de Equipamentos de TI _Computadores e RE-GG-035.1- Formulário Termo de Responsabilidade de Equipamentos TI_Mobile".

→ Todos os usuários devem estar cientes de que são responsáveis pelos ativos de informação que foram disponibilizados para a execução do trabalho cuidando do ambiente físico (Notebooks, Celulares etc.) e lógico (Senhas, Sistemas, e-mails, etc...).

3.3.2. Licenças e Softwares

A Cimento Nacional possui um inventário de Softwares de forma a garantir que não haja nenhuma violação de direitos autorais de qualquer empresa, por isso:

→ Todo e qualquer software (incluindo aplicativos grátis) só poderá ser instalado nos computadores com o consentimento de TI. O gestor da área deverá aprovar a instalação do aplicativo.

→ Nenhum usuário está autorizado a realizar instalações, desinstalações ou atualizações de qualquer aplicativo instalado no computador.

→ Caso necessite de uma licença de software, o time de TI deverá ser contatado para avaliação da necessidade.

4. Trabalho Remoto

Para trabalhos remotos os usuários e terceiros devem seguir algumas premissas listadas abaixo:

→ O trabalho remoto deverá ser solicitado a TI somente após a autorização do gestor responsável.

→ Só será permitido o trabalho remoto quando os usuários e terceiros estiverem utilizando mecanismos de segurança física, lógica como VPN e conectar-se apenas a rede da empresa, exceto quando acessar e-mail ou tecnologia de acesso remoto seguro.

→ Os equipamentos deverão ser mantidos e guardados em lugares adequados.

→ Dispositivos móveis não pertencentes à empresa, não devem ser usados para armazenar informações da empresa.

5. Gestão de Acesso de Usuários

→ O acesso deve ser autorizado pelo dono do processo relacionado ao sistema ou serviço de informação.

→ O nível de acesso concedido deve ser verificado de acordo com as políticas de controle de acesso local e ser consistente com outros requisitos, tal como: Segregação de funções, privilégio mínimo e necessidade de conhecimento.

→ O acesso de terceiros é concedido apenas em um período temporário acordado e com termo de responsabilidade assinado.

→ Os direitos de acesso do usuário devem ser definidos e alocados de acordo com papéis de trabalho predefinidos e cóntroles de separação de tarefas.

→ Os Gestores devem revisar os direitos de acesso à rede e aos sistemas críticos pelo menos uma vez por ano.

6. **Gestão de Senhas de Usuários**

→ Os usuários devem proteger as credenciais de autenticação pessoal (manter as senhas confidenciais e não compartilhar com ninguém sob nenhuma circunstância).

→ Não usar as mesmas senhas para fins de negócio e particulares, principalmente em sites que possam trazer riscos para a segurança da informação.

→ Escolher uma senha que atenda ou exceda os requisitos da política de senha de acordo com as regras estabelecidas para os sistemas da rede corporativa da Cimento Nacional.

7. **Acessos à Rede**

→ Os usuários só devem ter acesso à rede e aos seus serviços que foram especificamente autorizados, de acordo com políticas e procedimentos de controle de acesso definidos.

→ O acesso ao serviço de rede deve ser aprovado pelo gestor responsável, dono da informação.

8. **Transferência de Informações**

→ A informação da empresa deve ser mantida em segurança e protegida contra divulgações não autorizadas ou uso inadequado durante as transferências, por exemplo: e-mail, transferências físicas de documentos em papel e transferências em nuvem.

9. **Mensagens Eletrônicas**

→ As informações transferidas por meio de mensagens eletrônicas ou instantâneas devem estar protegidas por criptografia, devese garantir se os destinatários estão corretos.

→ É absolutamente proibida a transferência de arquivos por meio de aplicativos de mensagens instantâneas.

10. **Backup de Dados**

→ O processo de backup, deve incluir informações críticas da empresa para permitir a recuperação no caso de um desastre.

→ Informações e dados operacionais devem ser armazenados em nos servidores ou em nuvem para proteger contra exclusão ou perda acidental.

→ Os backups dos servidores são realizados de acordo com as regras definidas para cada sistema, e as suas características legais.

→ As restaurações de backup devem ser testadas regularmente para garantir que possam ser utilizadas para uso emergencial quando necessário.

→ Os desktops e notebooks NÃO possuem backups automá perativo que os dados críticos não fiquem armazenados somente nos dispositivos locais.

11. **Controles contra Vírus e Malware**

→ Todos os dispositivos móveis que suportam antivírus devem ter uma solução antivírus instalada e atualizada para o nível de assinatura mais recente.

→ A proteção contra malware para sistemas, dispositivos de usuários e mídia deve ser fornecida pela instalação de programas de proteção contra malwares (antimalwares), aprovados e gerenciados centralmente.

→ Caso ocorram os incidentes de segurança da informação devem ser reportados à TI local e ao e-mail: cyberseguranca@cimentonacional.com.br

12. **Demais Demandas**

→ Toda e qualquer demanda relacionada à segurança da informação e não listada neste documento deve ser informada à equipe de TI para análise.

13. Registros

Para o armazenamento correto dos registros/evidências citados ao longo desse procedimento, verificar a tabela de "Controle de Registros do Sistema de Gestão", disponível na unidade.

Registros armazenados na área da Tecnologia da Informação:

→ Backups de informações RE-GG-035 - Formulário Termo de Responsabilidade de Equipamentos de TI _Computadores.

→ RE-GG-035.1- Formulário Termo de responsabilidade de equipamentos TI _ Mobile.


CIMENTO
NACIONAL