TERMO DE USO DOS SISTEMAS INTERNOS

COMITÊ DE SEGURANÇA DA INFORMAÇÃO

EMPRESA PARAIBANA DE COMUNICAÇÃO

EMPRESA PARAIBANA DE COMUNICAÇÃO S.A. (EPC)

Naná Garcez de Castro Dória
Diretora Presidente

William Costa
Diretor de Mídia Impressa

Rui Leitão
Diretor de Rádio e TV

Amanda Lacerda
Diretora Administrativa, Financeira e de Pessoas

COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Adriana Borba de Medeiros (Encarregada pelo tratamento de dados - DPO)
Augusto César Sandino (Presidente)
Francisco de Assis A. Marques (Membro)
Zeilton Gomes Sousa (Membro)
Amanda Lacerda (Membro)

Colaborador
Lucas Fernandes da Silva (Analista de Sistema)

Diagramador
Naudimilson Ricarte (Designer Gráfico)

EMPRESA PARAIBANA DE COMUNICAÇÃO

TERMO DE USO DOS SISTEMAS INTERNOS

EMPRESA PARAIBANA DE COMUNICAÇÃO S.A.

(EPC)

VERSÃO 1.0

EQUIPE DA TECNOLOGIA DA INFORMAÇÃO

ABRIL 2024

CONSIDERANDO que a Empresa Paraibana de Comunicação - EPC disponibiliza a seus usuários ativos de informação e recursos computacionais exclusivamente para que os mesmos possam desempenhar suas atividades profissionais;

CONSIDERANDO que a EPC é a única proprietária de todos os ativos de informação e recursos computacionais, dessa forma, sendo responsável por todos os custos com os mesmos, não existindo assim qualquer tipo de expectativa de privacidade no uso dos recursos acima mencionados;

CONSIDERANDO que a EPC poderá ser seriamente impactada pela má utilização de seus ativos de informação e recursos computacionais;

DECLARO QUE:

Tenho conhecimento e acesso a Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessários ao meu trabalho, que se encontram disponíveis no portal corporativo, aos quais li na íntegra, tomando conhecimento e ciência de suas disposições;

Compreendi completamente os termos, diretrizes, conceitos e condições de uso Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessários ao meu trabalho, me comprometendo a cumprir integralmente as disposições constantes em tais documentos;

Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica da EPC somente poderão ser utilizados para fins exclusivamente profissionais e relacionados às atividades da organização;

Estou ciente de que todos os acessos e comunicações realizados por meio da infraestrutura tecnológica da EPC são monitorados. A infraestrutura tecnológica compreende os meios de comunicação e as plataformas informáticas oficiais da EPC. Esse monitoramento não se estende a dispositivos pessoais.

Estou ciente que violações da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação são passíveis de

sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativas, cíveis e penal, nos termos da legislação em vigor;

Comprometo-me a não revelar, fato ou informações de qualquer natureza a que tenha conhecimento por forças das minhas atribuições, mesmo após o encerramento do contrato de trabalho com a Empresa Paraibana de Comunicação - EPC;

João Pessoa, _____ de _____ de 2024

Nome:

_____

Cargo:

_____

CPF:

_____

Sanções e Punições

Introdução

As políticas de segurança da informação são medidas essenciais para proteger os ativos de informação da organização contra acessos não autorizados, uso indevido, divulgação ou destruição. O descumprimento dessas políticas pode resultar em sanções e punições para os infratores, a fim de garantir a confidencialidade, integridade e disponibilidade dos dados.

Estrutura das Regras

As regras de sanções e punições estão organizadas por **criticidade** e **relevância** da violação, conforme pode ser visto a seguir:

- **Crítica:** violações que causam impacto significativo à organização, como perda de dados confidenciais, interrupção de serviços ou danos à reputação;
- **Alta:** violações que podem ter impacto significativo à organização, como acesso não autorizado a dados confidenciais ou uso indevido de recursos de TI;
- **Média:** violações que podem ter impacto moderado à organização, como instalação de software não autorizado ou descumprimento de normas de segurança;
- **Baixa:** violações que causam impacto mínimo à organização, como navegação em sites não recomendados ou uso indevido de e-mail corporativo.

Relevância da Violação

- **Intencionalidade:** ação deliberada para violar a política;
- **Frequência:** reincidência na violação da mesma política;
- **Impacto:** nível de dano causado à organização pela violação.

Tipos de Sanções e Punições

- **Admoestação verbal:** advertência verbal em caso de violações de baixa relevância;
- **Admoestação escrita:** advertência formal por escrito em caso de violações de média ou alta relevância;

- **Suspensão do acesso a recursos de TI:** restrição do acesso a sistemas, aplicativos, dados ou dispositivos em caso de violações de alta ou crítica relevância;
- **Treinamento de conscientização:** participação obrigatória em treinamentos sobre segurança da informação para reincidências em violações de qualquer nível;
- **Demissão por justa causa:** rescisão do contrato de trabalho em caso de violações graves e intencionais que causem danos à organização.

Aplicação das punições

- **Nível Crítico:**
  - **Divulgação de dados confidenciais a terceiros:** demissão por justa causa;
  - **Ataque cibernético que causa perda de dados:** suspensão do acesso a recursos de TI e investigação interna;
- **Nível Alto:**
  - **Acesso não autorizado a dados confidenciais:** admoestação escrita e possível suspensão do acesso aos dados;
  - **Instalação de software não autorizado:** admoestação verbal e remoção do software.
- **Nível Médio:**
  - **Descumprimento de normas de segurança, como uso de senhas fracas:** admoestação verbal e treinamento de conscientização;
  - **Navegação em sites não recomendados:** admoestação verbal e bloqueio dos sites.
- **Nível Baixo:**
  - **Uso indevido de e-mail corporativo:** admoestação verbal e orientação sobre o uso correto;
  - **Atraso na atualização de softwares:** admoestação verbal e atualização obrigatória do software.

Observações

- A aplicação das sanções e punições será feita de forma justa e imparcial com base na gravidade da violação e no histórico do colaborador;
- Em caso de dúvidas sobre as políticas de segurança da informação ou sobre as sanções e punições, consulte o seu superior hierárquico ou o setor de segurança da informação da organização;
- A organização reserva-se o direito de alterar essas regras a qualquer momento, mediante comunicação aos colaboradores.

EMPRESA
PARAIBANA DE
COMUNICAÇÃO