POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

EMPRESA PARAIBANA DE COMUNICAÇÃO S.A.

(EPC)

VERSÃO 1.0

COMITÊ DE SEGURANÇA DA INFORMAÇÃO

ABRIL 2024

1 CONTEXTUALIZAÇÃO

A Empresa Paraibana de Comunicação (EPC) possui o compromisso de resguardar e proteger os dados — sejam eles pessoais ou não — que estão sob sua guarda. Nesse sentido, a presente Política de Segurança da Informação apresenta diretrizes gerais de conduta, bem como obrigações a serem seguidas na EPC a fim de mitigar eventuais riscos e danos relacionados a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das informações de qualquer natureza, objetivando garantir sua preservação. Amparada nos preceitos da Norma ISO 27001, padrão internacional para processos de gestão da segurança da informação, a EPC define também papéis e responsabilidades para a implantação dos seguintes controles de segurança da informação, conforme diagrama abaixo:

Figura 1 - Controles previstos na ISO 27001

Fonte: Revista Manutenão, 2023. Disponível em https://www.revistamanutencao.com.br/

2 DEFINIÇÕES

AMEAÇA: evento que tem potencial em si próprio para comprometer os objetivos da empresa, trazendo danos diretos aos ativos ou prejuízos indiretos decorrentes de situações inesperadas;

ATIVOS DE INFORMAÇÃO: são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso a informações, assim como as próprias informações coletadas, produzidas, processadas, armazenadas, custodiadas, descartadas e transmitidas pela EPC;

AUTENTICIDADE: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema, órgão ou entidade.

CLASSIFICAÇÃO DA INFORMAÇÃO: identificação de quais são os níveis de proteção que as informações demandam estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados;

CONFORMIDADE: processo que visa verificar o cumprimento das normas estabelecidas;

CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

CRIPTOGRAFIA: método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas;

CUSTODIANTE DO ATIVO DE INFORMAÇÃO: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

DADOS PESSOAIS: todo e qualquer dado relacionado a pessoa natural identificada ou identificável (conforme definição trazida no art. 5º, I, da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais), inclusive números identificativos, dados locacionais

ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa. Também são considerados dados pessoais, para os fins da lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural se identificada (art. 12, §2°, LGPD);

DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO (ETRISI): grupo de pessoas com a responsabilidade de receber, analisar e responder as notificações relacionadas a incidentes com ativos de informação da EPC;

FORNECEDORES: no contexto da EPC, são considerados fornecedores os terceiros contratados e subcontratados, pessoa física ou jurídica, não enquadrados como parceiros comerciais;

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO (GRSI) conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;

GESTOR DOS ATIVOS DE INFORMAÇÃO: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

GESTOR DE SEGURANÇA DA INFORMAÇÃO: funcionário responsável pela operação do ESI;

GENERAL DATA PROTECTION REGULATION (GDPR) - conjunto de regras sobre tratamento de dados, aprovado em 2016, válido para a União Europeia (EU). Regulamenta também a exportação de dados pessoais para fora da EU;

INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados

(arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

INTEGRIDADE: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira acidental ou não autorizada;

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): Lei n° 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos da Lei (arts. 1° e 17, LGPD);

PARCEIROS COMERCIAIS: no contexto da EPC, são considerados parceiros comerciais os terceiros contratados, pessoa física ou jurídica, que atuam em seu nome: Consultores, Conveniados e Agentes Comerciais (aqueles que indicam atividades em que a EPC pode atuar como contratada);

QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

SEGURANÇA DE COMUNICAÇÕES: processo de proteção de dados digitais em trânsito;

SISTEMA ESTRUTURANTE: conjunto de sistemas de informática fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

TERCEIROS: São os parceiros comerciais e os fornecedores da EPC;

TRATAMENTO DA INFORMAÇÃO: conjunto de ações referentes à recepção, à produção, à reprodução, à utilização, ao acesso, ao transporte, à transmissão, à distribuição, ao armazenamento, à eliminação e ao controle da informação;

VULNERABILIDADE: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EPC

Estabelece o compromisso da Empresa Paraibana de Comunicação em resguardar e proteger as informações — sejam elas pessoais ou não — que estão

sob sua guarda, além de definir a governança de segurança da informação na EPC. A Política de Segurança da Informação exige o cumprimento do Código de Conduta EPC, de todas as leis e de regulamentações aplicáveis em vigor, relacionadas à proteção de dados incluindo, sem limitação, a Lei Geral de Proteção de Dados Pessoais (LGPD) e a General Data Protection Regulation (GDPR). Essa Política se insere-se no Sistema de Controles Internos e de Conformidade EPC como sendo o documento que estabelece as diretrizes do Programa de Conformidade para com a Lei Geral de Proteção de Dados Pessoais.

4 DESTINATÁRIOS

A presente Política aplica-se a todos os membros do Conselho Diretor, Conselho Curador, Presidente, Vice-Presidentes, empregados, parceiros comerciais (consultores, agentes comerciais e conveniados) que atuam em nome da EPC e fornecedores (outros contratados e subcontratados pela EPC) que, no âmbito dessa relação, possam acessar as áreas, equipamentos, informações, arquivos, redes e dados de titularidade ou propriedade da EPC.

Desta forma: todos os destinatários deverão observar as presentes regras e recomendações em quaisquer operações que possam impactar na segurança das informações na EPC. O não cumprimento das disposições ora previstas sujeitará o infrator às sanções previstas fixadas pelo Comitê de Segurança de Informação (CSI) previsto nessa Política, sem prejuízo das medidas previstas em lei, caso se aplique.

5 CLASSIFICAÇÃO DA INFORMAÇÃO

Uma informação possui níveis de acesso, divididos em confidencial, restrito, interno e público. Classificar uma informação é essencial para determinar quem pode ter acesso a ela.

Confidencial: uma informação confidencial é aquela que deve ser de uso dentro do órgão. Este nível de informação é um dos mais elevados, pois, caso a informação venha a ser vazada, pode causar sérios prejuízos para o órgão.

Restrita: uma informação restrita é similar a uma informação confidencial. A diferença é que uma informação restrita tem um nível de acesso dentro do órgão, mas apenas para pessoas selecionadas. Uma informação restrita, se vazada, também traz grandes prejuízos.

Interna: uma informação interna é aquela que deve ser utilizada por todos os colaboradores do órgão. O vazamento dela não acarreta grandes danos para o órgão, porém deve-se evitar que ela venha a ser vazada.

Pública: uma informação pública é aquela onde seu acesso é aberto para o público em geral. São informações que não causam problemas para o órgão.

6 POLÍTICA DE SENHAS

A senha é o meio que os colaboradores possuem para terem acesso aos dispositivos do órgão.

As senhas são pessoais e intransferíveis, não podendo o colaborador passar seus dados de acesso para terceiros. Com o acesso conduzido de forma correta, pelo próprio usuário da conta, terceiros não podem ter acesso aos arquivos.

Os usuários e senhas são cadastrados no sistema Active Directory, da Microsoft. O objetivo é o controle de arquivos e pastas do órgão. As senhas devem ser trocadas a cada 45 (quarenta e cindo) dias e o usuário recebe o aviso com 5 (cinco) dias de antecedência.

O RH (Recursos Humanos) tem uma participação importante nessa questão, pois é por meio dele que a Gerência de Tecnologia da Informação tomará conhecimento da situação dos colaboradores. Caso o colaborador venha a ser desligado do órgão, o setor de Recursos Humanos deverá comunicar, se possível com antecedência, sobre o desligamento do colaborador para que a Gerência de TI tome as providências para que o acesso aos arquivos e pastas venha a ser bloqueado a fim de evitar que o colaborador desligado apague os arquivos, pois muitos deles são importantes.

6.1 SENHAS

6.1.1 As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da EPC são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

6.1.2 A EPC adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais;

6.2.2.1 A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata dela;

6.2.2.2 As senhas possuem validade, passado o prazo, os sistemas poderão solicitar automaticamente a troca da senha;

6.2.2.3 As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 8 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
6.2.2.4 As senhas associadas a contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
6.2.2.5 Após 5 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário poderá ser bloqueada, permanecendo assim por no mínimo, 30 (trinta) minutos;
6.2.2.6 Os sistemas de informação podem manter um histórico das últimas 12 (doze) senhas utilizadas, não permitindo sua reutilização;
6.2.3 Quando criada uma nova senha, usuários devem estar atentos às seguintes recomendações:
6.2.3.1 Não utilizar nenhuma parte de sua credencial na composição da senha;
6.2.3.2 Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;
6.2.3.3 Não utilizar repetição ou sequência de caracteres, números ou letras;
6.2.3.4 Qualquer parte ou variação do nome Empresa Paraibana de Comunicação - EPC;
6.2.3.5 Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

7 APLICABILIDADE

Essa Política estabelece as diretrizes para garantir que seus destinatários entendam e cumpram as leis de proteção de dados pessoais, bem como os padrões e medidas técnicas que visam a segurança da informação na EPC.

8 OBJETIVOS POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta Política de Segurança da Informação (PSI EPC) tem como objetivos:

I. Estabelecer as diretrizes que assegurem e reforcem o compromisso da Instituição com as práticas e medidas preventivas garantidoras de segurança da informação;
II. Definir o referencial para a normatização das questões de segurança da informação na EPC;
III. Criar condições para que a EPC eleve continuamente a sua maturidade

em segurança da informação por meio da adoção de diretrizes, normas e procedimentos destinados a proteger os ativos de informação da EPC visando a promoção da Integridade, Confidencialidade, Autenticidade e Disponibilidade dos ativos de informação da EPC;

IV. Prover a EPC de mecanismos de atendimento e conformidade às leis de segurança da informação, nacionais e internacionais;

V. Descrever as regras comportamentais e diretrizes a serem seguidas na condução das atividades desenvolvidas pela EPC que garantam a prevenção de incidentes de segurança da informação e a proteção de dados pessoais.

Os demais documentos da EPC que se relacionam com esta Política são:

I. Código de Ética e Conduta Política de Controles Internos e de Conformidade;
II. Política geral de uso de dispositivos móveis ;
III. Modelo de Segurança para ambientes computacionais na EPC;
IV. Normas para uso da rede EPC, da Internet e do Correio Eletrônico da EPC.

Cada um desses documentos tem objetivos específicos, mas em todos está reforçado o compromisso da EPC com a segurança da informação.

9 PRINCÍPIOS

O compromisso da EPC com o tratamento adequado das informações baseia-se nos seguinte princípios:

I. Autenticidade: todos os esforços serão feitos para que as informações sejam confiáveis e corretas, ou seja, as informações não serão alteradas de forma não autorizada ou indevida;
II. Confidencialidade: o acesso à informação é permitido somente para pessoas autorizadas e quando ele for de fato necessário;
III. Disponibilidade: somente as pessoas autorizadas têm acesso à informação sempre que necessário;
IV. Integridade: todos os esforços serão feitos para que as informações sejam exatas e completas bem como seu processamento.

10 DIRETRIZES

10.1 DIRETRIZES GERAIS:

I. A gestão da segurança da informação na EPC é de responsabilidade do Comitê de Segurança da Informação (CSI), cujos membros são indicados pelo Presidente da EPC;

II. O cumprimento dessa Política e de suas normas de procedimentos complementares deve ser avaliado periodicamente por meio de verificações de conformidade, realizadas por um grupo de trabalho designado pelo Comitê de Segurança da Informação (CSI);

III. A EPC, além das diretrizes estabelecidas nessa PSI, deve também se orientar pelas melhores práticas e procedimentos de segurança da informação recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões relacionados à segurança da informação.

10.2 DIRETRIZES E NORMAS COMPLEMENTARES ESPECÍFICAS:

Para cada um dos controles complementares propostos pela ISO 27001 o Comitê de Segurança da Informação deve elaborar estratégias, diretrizes e normas de procedimentos complementares (Políticas de SI — controle ISO 27001 #2), assim como manuais, procedimentos de conduta e avaliações periódicas de conformidade.

A PSI EPC preconiza a implantação priorizada das seguintes normas de procedimentos com as seguintes diretrizes:

10.2.1 GESTÃO DE ATIVOS DE INFORMAÇÃO (CONTROLE ISO 27001 #4):

Os ativos de informação devem:

I. Ser inventariados e protegidos;
II. Ter identificados os seus proprietários e custodiantes;
III. Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
IV. Ter a sua a entrada e saída nas dependências da EPC autorizadas e registradas por autoridade competente;
V. Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;
VI. Ser regulamentados por norma de procedimentos específica quanto a sua utilização;
VII. Ser utilizados particulares ou estritamente dentro do seu propósito, sendo vedado seu uso para fins religiosos, discriminatórios de terceiros e afins. E, além disso: entretenimento, opiniões político-partidárias, religiosas, discriminatórias e afins.

E, além disso:

I. A EPC deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor;
II. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas;
III. Os sistemas de informação e as aplicações da EPC devem ser protegidos contra indisponibilidade, alterações programadas;
IV. O acesso dos usuários ou os acessos ativos de indivíduos, falhas e interrupções não informados e sua utilização, quando autorizados, devem ser condicionados ao aceite do termo de sigilo e responsabilidade;
V. Os ativos de informação devem possuir mecanismos que permitam a auditoria dos eventos de acesso e alteração dos registros. Essa auditoria deve estar sempre ativa (salvo quando explicitamente dispensado este requisito) e os registros devem ser armazenados pelo período mínimo de um ano.

10.2.2 GESTÃO DE RISCOS E INCIDENTES (CONTROLE ISO 27001 #12):

I. O gestor dos ativos de informação deve estabelecer processos de Gestão de Riscos de Segurança da Informação (GRSI) que possibilitem identificar ameaças e reduzir vulnerabilidades dos ativos de informação, assim como reduzir os impactos de eventuais incidentes;
II. A da GRSI é um processo contínuo e deve ser aplicado na implementação e operação Gestão de Segurança da Informação, levando em consideração o planejamento, execução, análise crítica e melhoria da SI na EPC.

10.2.3 SEGURANÇA EM RECURSOS HUMANOS (CONTROLE ISO 27001 #3):

I. Os destinatários devem ter ciência:
    A. Das ameaças e preocupações relativas à segurança da informação;
    B. De suas responsabilidades e obrigações no âmbito desta PSI.
II. Todos os destinatários devem difundir e exigir o cumprimento da PSI, das normas de segurança e da legislação vigente acerca do tema;
III. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os destinatários, de acordo com seu relacionamento e atribuições na EPC.

10.2.4 OS USUÁRIOS DEVEM SER SENSIBILIZADOS E CONSCIENTIZADOS:

I. O controle de usuários de sistemas:
   A. É de responsabilidade do titular da unidade da EPC juntamente com o DRH;
   B. Devem ser implementados controles de perfis e permissões, necessários para a salvaguarda dos ativos de informação da EPC.

10.2.5 SEGURANÇA DAS OPERAÇÕES DE TI DA EPC (CONTROLE ISO 27001 #7):

O Comitê de Segurança da Informação deve estabelecer normas de procedimentos específicos contendo diretrizes de segurança da informação para a disponibilização e execução dos serviços, sistemas e infraestruturas de TIC da EPC.

10.2.6 SEGURANÇA DAS COMUNICAÇÕES DA EPC (CONTROLE ISO 27001 #9):

O Comitê de Segurança da Informação deve estabelecer normas de procedimentos específicos contendo diretrizes de segurança da informação para a disponibilização e utilização de serviços de comunicação relacionados aos ativos de informação da EPC.

10.2.7 ASSINATURA DIGITAL E CRIPTOGRAFIA (CONTROLE ISO 27001 #6):

O Comitê de Segurança da Informação deve estabelecer normas de procedimentos específicos contendo parâmetros para o uso de assinaturas digitais que reflitam as necessidades específicas de garantia de autenticidade dos dados da EPC. Também devem ser estabelecidas normas específicas ditando quando e onde recursos criptográficos devem ser utilizados dentro da EPC para proteger suas informações, além de estabelecer quais padrões de criptografia são aceitáveis.

10.2.8 CONTROLES DE ACESSOS (CONTROLE ISO 27001 #5):

O Comitê de Segurança da Informação deve estabelecer norma de procedimentos específica contendo parâmetros para a gestão de acesso aos dados EPC, atendendo os requisitos abaixo:

I. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações;
II. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação;

III. Os usuários da EPC são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital;

IV. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento;

V. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação;

VI. Todos os sistemas de informação da EPC, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações;

VII. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento da EPC ou bloqueados em caso de afastamento;

VIII. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regem o controle de acesso quanto:

   A. Ao acesso às suas bases de dados;
   B. À extração, carga e transformação de dados;
   C. Aos serviços acessíveis via linguagem de programação.

IX. Deve ser possível no sistema:

   A. Revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;
   B. Bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor;
   C. Tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

10.2.9 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS (CONTROLE ISO 27001 #10):

O Comitê de Segurança da Informação deve editar norma de procedimentos específica estabelecendo critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e sustentação de sistemas.

10.2.10 RELAÇÃO COM FORNECEDORES (CONTROLES ISO 27001 #11):

O Comitê de Segurança da Informação deve estabelecer norma de procedimentos específica que vise o atendimento de demandas em segurança da informação para contratos, convênios, acordos e afins, conforme os requisitos abaixo:

I. Os acordos com terceiros que possuam algum relacionamento com ativos de informação da EPC devem observar as disposições e normas da PSI EPC;
II. Os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância dessa PSI e de suas normas complementares;
III. O contrato, convênio, acordo ou instrumento congênere deve prever a obrigação da outra parte de divulgar essa PSI e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na EPC;
IV. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

10.2.11 GESTÃO DE INCIDENTES (CONTROLE ISO 27001 #12):

O Comitê de Segurança da Informação deve instituir uma Equipe de Tratamento e Resposta a Incidentes de Segurança.

10.2.12 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO EM CONTINUIDADE DAS ATIVIDADES (CONTROLE ISO 27001 #13):

O Comitê de Segurança da Informação deve instituir metodologias e normas de procedimentos que enderecem tratativas de segurança da informação relacionadas à disponibilidade dos ativos de informação da EPC.

10.12.13 GESTÃO DE CONFORMIDADE (CONTROLE ISO 27001 #1):

I. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de segurança da informação da EPC e de suas unidades administrativas com essa PSI e suas normas de procedimentos complementares, bem como com a legislação específica de segurança da informação;
II. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a EPC;

III. O calendário de ações de verificação de conformidade é elaborado com base na priorização dos riscos identificados ou percebidos;
IV. Nenhuma unidade da EPC pode permanecer sem verificação de conformidade de suas práticas de segurança da informação por período superior a 2 (dois) anos;
V. É vedado a prestadores de serviços executar a verificação da conformidade de segurança da informação dos próprios serviços prestados;
VI. A verificação de conformidade pode combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevista e testes de invasão;
VII. Os resultados de cada ação de verificação de conformidade são documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de segurança da informação ao Gestor da unidade verificada para ciência e tomada das ações cabíveis;
VIII. Para que seja possível efetuar as verificações de conformidade, a equipe delegada pelo CSI deve possuir acesso aos ambientes computacionais da EPC.

10.2.14 PLANO DE INVESTIMENTOS EM SEGURANÇA DA INFORMAÇÃO DA EPC:

I. Os investimentos em segurança da informação serão realizados de forma planejada e consolidados em um plano de investimentos plurianual;
II. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, o produtor entre a probabilidade de ocorrência e o impacto do risco no negócio ou imagem da EPC;
III. Os planos de investimento e seus orçamentos são produzidos, apresentados e geridos pelo Comitê de Segurança da Informação.

11 PAPÉIS E RESPONSABILIDADES REFERENTES A SEGURANÇA DA INFORMAÇÃO

11.1 COMITÊ DE SEGURANÇA DA INFORMAÇÃO:

I. Supervisionar a segurança da informação no âmbito da EPC;
II. Constituir a Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI);
III. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

IV. Elaborar normas específicas que complementam essa Política em consonância com a Política da Estrutura Normativa EPC;
V. Conduzir apurações quando da suspeita de ocorrências e incidentes em segurança da informação na EPC;
VI. Avaliar e aprimorar continuamente a PSI EPC e suas normas de procedimentos complementares, visando a sua aderência aos objetivos institucionais da EPC e as legislações aplicáveis vigentes;
VII. Dirimir eventuais dúvidas e deliberar sobre assuntos relativos a PSI EPC;
VIII. Monitorar e avaliar periodicamente o plano estratégico de segurança da informação, assim como determinar os ajustes cabíveis;
IX. Apoiar a Alta Administração da EPC no planejamento dos investimentos em segurança da informação com base nas exigências estratégicas e legais.

11.2 EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO (ETRISI):

Cabe à Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI):

I. Coordenar as atividades de tratamento e resposta a incidentes de segurança;
II. Promover a recuperação de sistemas junto a área de TIC responsável;
III. Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança da informação e avaliando condições de segurança de redes por meio de verificações de conformidade;
IV. Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
V. Analisar ataques e intrusões na rede da EPC;
VI. Executar as ações necessárias para tratar quebras de segurança;
VII. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
VIII. Cooperar com outras equipes de Tratamento e Resposta a Incidentes;
IX. Apurar ações que violem a PSI EPC ou quaisquer de suas diretrizes e normas de procedimento. Aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor;

X. Participar em fóruns, redes nacionais e internacionais relativos à segurança da informação.

11.3 GESTOR DO ATIVO DE INFORMAÇÃO

Cabe ao Gestor do Ativo de Informação:

I. Seguir as diretrizes dessa Política;
II. Garantir a segurança dos ativos de informação sob sua responsabilidade;
III. Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com essa Política;
IV. O Conceder e revogar acessos aos ativos de informação;
V. Comunicar à ETRISI a ocorrência de incidentes de segurança da informação;
VI. Designar custodiante dos ativos de informação, quando aplicável.

11.4 CUSTODIANTE DO ATIVO DA INFORMAÇÃO

O Custodiante do Ativo de Informação:

I. Deve proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PSI;
II. Deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

11.5 TITULAR DA UNIDADE EPC:

Cabe ao Titular da Unidade EPC:

I. Conscientizar os usuários sob sua supervisão em relação às políticas e normas de segurança da informação da EPC;
II. Incorporar aos processos de trabalho de sua unidade ou de sua área boas práticas em segurança da informação;
III. Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão.
IV. Garantir a realização do tratamento e a classificação da informação definidos nas Políticas e normas de procedimentos;
V. Autorizar, de acordo com a legislação vigente e as diretrizes do Comitê de Segurança da Informação, a divulgação das informações produzidas na sua unidade administrativa;

VI. Comunicar à ETRISI os casos de quebra de segurança;
VII. Solicitar suporte à ETRISI quando perceber riscos ou suspeitas de incidentes em segurança da informação;
VIII. Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores;
IX. Informar a Diretoria de Recursos Humanos sobre a movimentação de pessoal de sua Unidade.

11.6 TERCEIROS E PARCEIROS COMERCIAIS DA EPC:

Cabe aos Terceiros e Parceiros Comerciais:

Tomar conhecimento e seguir as diretrizes estabelecidas pela EPC em relação à segurança da informação;

Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação, objetos do contrato;

Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

Documento	Política de Segurança da Informação EPC
Dimensão	Estrutura Normativa de Procedimentos
Tipo de Instrumento Normativo	Política
Categoria do Assunto	Tecnologia da Informação
Assunto	Segurança da Informação
Identificação	TI.01.001.2024
Elaboração	**Aprovação**
Lucas Fernandes da Silva	Francisco de Assis
Analista de Sistemas	Gerente de TI
Versão: 1.0/2024	

EMPRESA
PARAIBANA DE
COMUNICAÇÃO