ENCONTRO DAS ÁGUAS

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DOCUMENTO DE DIRETRIZES E NORMAS ADMINISTRATIVAS

V.1.0 PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DATA	VERSÃO	DESCRIÇÃO	AUTOR
26/05/2022	1.0	Versão elaborada e publicada	Marcelo Rabelo Cardoso da Silva
			Eliney Zacarias

SUMÁRIO

1. CONCEITOS, TERMOS E ABREVIAÇÕES

Conceitos

Para efeitos da presente política, considera-se:

Rede Modal: Abrange todos os sistemas, diretórios e Intranet disponibilizados aos Colaboradores da empresa, conforme perfil de acesso definido.

Software: São todos os programas instalados nos computadores, os quais são disponibilizados pela equipe de TI INFRA para o exercício de sua função.

Homologação: Verificação pela equipe de TI INFRA quanto à compatibilidade técnica do software e aplicativos em relação ao parque tecnológico. Confirmação pelo usuário final do sistema do adequado funcionamento das funcionalidades previstas no quando da implantação ou da atualização de versão do mesmo.

Ambiente Lógico: ambiente controlado, eletrônico, onde circulam e são armazenadas Informações Confidenciais, softwares e sistemas.

Ambiente físico: dependências físicas das sociedades que integram a empresa.

Usuário: Colaborador ou Colaboradores que detenham acesso aos ambientes físico e lógico das sociedades da empresa para o desempenho de suas atividades.

Termos e Abreviações

ABNT: Associação Brasileira de Normas Técnicas.

Agente Público: Que serve ao poder público como instrumento de sua vontade ou ação, independentemente do vínculo jurídico, podendo ser por nomeação, contratação, designação ou convocação. Independe, ainda, de ser essa função temporária ou permanente e com ou sem remuneração. Assim, quem quer que desempenhe funções estatais, enquanto as exercita.

Ambiente de Desenvolvimento: Ambiente tecnológico composto por um conjunto de ferramentas necessárias para criação e manutenção de sistemas de informação.

Ambiente de teste: Ambiente tecnológico com configuração similar ao ambiente de desenvolvimento composto por um conjunto de ferramentas necessárias para que usuários recebam e validem versões de sistemas de informação instáveis, para garantir a equalização comportamental dos sistemas de informação em teste.

Ambiente de Homologação: Ambiente tecnológico similar ao ambiente de produção, que possa simular situações muito próximas das que se encontra no dia a dia, composto por um conjunto de ferramentas necessárias para que usuários recebam e validem versões de sistemas de informação.

Ambiente de produção: Entende-se por ambiente de produção o conjunto composto de ferramentas necessárias para que usuários recebam versões finais de sistemas de informação que serão utilizadas no seu dia a dia.

Ameaça: Risco potencial de um incidente indesejado que pode resultar em dano para um sistema ou para a organização.

Aplicação: Programa de computador que auxilia o usuário a desempenhar uma atividade específica (ex.: AutoCAD, para a área de engenharia e arquitetura; Skype, para telefonemas e conferências). Ativo Qualquer coisa, material ou imaterial, que tenha valor para a organização.

Autenticação: Processo que verifica se o usuário identificado é realmente quem ele diz ser, através do uso de sua senha pessoal ou de outros mecanismos (ex.: tokens e smartcards). Backup Cópia de segurança de arquivos e sistemas BYOD (Bring Your Own Device) Traduzido literalmente como “traga seu próprio dispositivo móvel”, refere-se à utilização de dispositivos pessoais no ambiente de trabalho.

Disponibilidade: Termo utilizado em segurança da informação que garante que todas as informações e serviços importantes ao negócio estejam disponíveis, sempre que necessário, a pessoas e processos autorizados.

Evento de Segurança da Informação: Ocorrência identificada em um serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação anteriormente desconhecida, que possa ser relevante para a segurança da informação.

FTP (File Transfer Protocol): Traduzido literalmente como “protocolo de transferência de arquivos”, trata-se de uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na Internet.

Gestor da Informação: Colaborador que exerce a chefia de área na empresa, responsável pela informação em sua área de competência.

ID: Conjunto de caracteres usados para identificar o usuário em um determinado sistema. Também pode ser chamado de logon name, login name ou user name.

Integridade: Termo utilizado em segurança da informação que garante que as informações estejam protegidas de modificações, manipulações ou reproduções não autorizadas.

Login: Processo que permite a identificação, autenticação e autorização de acesso a um determinado sistema por um usuário. Também pode ser chamado de logon.

Não-repúdio: Ato de evitar que uma entidade negue a execução de uma ação.

Negação de Serviço ou DoS (Denial of Service): Técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

PC: Políticas Complementares.

PSI: Política de Segurança da Informação.

Restore: Recuperação de arquivos e sistemas.

Software: Um termo genérico para definir um programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual. Essa sequência deve seguir padrões específicos que resultam em um comportamento desejado.

Sinistro: Fato que remete a um acidente ou desastre que cause prejuízo, podendo provocar perda, dor, morte ou dano material.

VPN (Rede Privada Virtual): Conexão estabelecida sobre uma infraestrutura pública (internet), usando protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas.

2. INTRODUÇÃO

São princípios para o Sistema de Gestão de Segurança da Informação a Confidencialidade, a Integridade e a Disponibilidade, conforme norma de mercado para a Segurança da Informação (NBR/ISO 27001). Esses devem ser preservados, controlados e auditados para garantir que as informações estejam protegidas nas medidas exigidas para sua utilização na empresa ou órgão público Esta Política de Segurança da Informação (PSI), em conjunto com as Políticas Complementares (PC), aprovada através de portaria regida pela empresa pública **Sistemas de comunicação Encontro das Águas** através da **circular nº 001- 26/05/2022**, que compreende a norma NBR/ISO 27001-2013 de segurança da informação.

3. PRINCÍPIOS

A Política de Segurança da Informação tem por princípio a proteção dos dados, informações e conhecimento, classificados como sigilosos, além da preservação do direito pessoal e coletivo no que se refere à intimidade e ao sigilo das correspondências eletrônicas, informações e comunicações individuais.

4. OBJETIVOS

Tornar a segurança da informação como um dos elementos fundamentais no planejamento estratégico do Sistema de Comunicação de Rádio e Tv Encontro das Águas; Definir os padrões mínimos obrigatórios para o devido uso e proteção das informações criadas, recebidas, armazenadas, processadas, transmitidas ou impressas; Estabelecer as competências e atribuições dos atores envolvidos nesta política; Elencar os processos necessários para atingir um padrão aceitável de Segurança da Informação, conforme as legislações existentes e os padrões que o mercado estabelece; Difundir os aspectos relacionados à Segurança da Informação no setor público.

Estabelecer diretrizes que permitam aos colaboradores e clientes do Sistema de Comunicação de Rádio e Tv Encontro das Águas a seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do Sistema de Comunicação de Rádio e Tv Encontro das Águas quanto à:

• **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário

5. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, quais sejam: servidores públicos, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações do Sistema de Comunicação de Rádio e Tv Encontro das Águas. Todos esses colaboradores serão tratados nesta política como usuários.

6. ATRIBUIÇÕES

6.1. Comitê de TI

Formado por colaboradores indicados pelos respectivos Secretários Executivos juntamente com gestor de segurança da informação, o gestor responsável para área de tecnologia da informação e comunicação ou seu representante, com o objetivo de deliberar a respeito de assuntos relacionados à tecnologia da informação e comunicação. Assim deve:

a. Promover a disseminação e conscientização da segurança da informação;

b. Disponibilizar os recursos necessários para que ações de segurança da informação sejam executadas;

c. Coordenar a atualização da Política de Segurança da Informação (PSI), propondo revisão e novas políticas complementares, bem como procedimentos que assegurem o controle das ações de política de segurança da informação.

NOTA: A deliberação só se dará, se houver no mínimo 3(três) representantes presentes

6.2. Gestores das Áreas

Formado pelos colaboradores que exercem a chefia de área ou setor no Sistema de Comunicação de Rádio e Tv Encontro das Águas, responsáveis pela informação em sua área de competência. Assim devem:

a. Gerenciar as informações sob sua competência;

b. Autorizar os colaboradores acesso ou decesso às informações sob sua competência;

c. Informar o desligamento dos colaboradores de sua respectiva área ou setor;

d. Indicar a classificação da informação sob sua competência, de modo a estabelecer como essas informações podem ser acessadas e administradas, garantindo a segurança da acessibilidade e disponibilidade destas.

6.**3. Equipe Técnica**

Formado por colaboradores da área de tecnologia da informação para:

a. Manter o ambiente tecnológico estável, operacional, atualizado, íntegro, disponível e monitorado;

b. Elaborar e atualizar os procedimentos relativos à operacionalidade do ambiente tecnológico;

c. Instalar e configurar os ativos de software e hardware necessários à operacionalidade do ambiente tecnológico;

d. Relatar mensalmente ao Comitê de TI ou representante indicado os incidentes de Segurança da Informação identificados, ocorridos no ambiente tecnológico.

e. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

6.4. Usuários e responsabilidades específicas

Todos os colaboradores, quais sejam: servidores públicos, privados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da empresa.

a. Cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta política;

b. Informar, imediatamente, à Central de Atendimento qualquer falha em dispositivo, serviço ou processo relacionado à Segurança da Informação para que uma ação seja tomada urgentemente;

c. Utilizar as informações como patrimônio e mantê-las disponíveis, conforme sua classificação.

6.5. Equipe de Segurança da Informação

Formada por equipe multidisciplinar de funcionários públicos ou comissionados, indicados pelos respectivos Secretários Executivos, com o objetivo de deliberar a respeito de assuntos relacionados à segurança da informação. Assim deve:

a. Implementar mecanismos de segurança com base no valor associado às informações e ao impacto oriundo da perda dessas informações;

b. Promover instrução relacionada à Segurança da Informação;

c. Acompanhar e analisar as transações e alterações relacionadas à Segurança da Informação, para fins de rastreamento e auditoria;

d. Realizar, periodicamente, monitoramento e auditoria de segurança no ambiente tecnológico;

e. Priorizar medidas preventivas, em detrimento de controles reativos;

f. Viabilizar monitoração e controles com soluções técnicas que não dependam de processos manuais ou não estejam sujeitas a erros humanos.

NOTA: A deliberação só se dará, se houver no mínimo 3(três) representantes presentes.

7. DIRETRIZES

a. Fica terminantemente proibida a cópia, envio, reprodução e divulgação a terceiros de quaisquer dados, informações, som e imagem, pertencentes aos acervos de informações em geral sem autorização prévia do Diretor de departamento e Diretor Presidente do Sistema de Comunicação de Rádio e Tv Encontro das Águas.

b. Será de inteira responsabilidade de cada servidor ou prestador de serviço, todo prejuízo ou dano que vier a sofrer ou causar ao Sistema de Comunicação de Rádio e Tv Encontro das Águas e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas, estarão sujeitas a penalidades administrativas e judiciais previstas em lei.

c. Cabe a cada usuário vinculado ao Sistema de Comunicação Encontro das Águas, zelar e proteger as informações criadas, manuseadas, tramitadas e guardadas no exercício de suas atividades, agindo no sentido de preservar as diretrizes e normas que estão relacionadas à segurança dessa informação, pois são de propriedade da empresa pública ou privada;

d. A Política de Segurança da Informação da empresa parte do pressuposto de atender às leis e regulamentações no âmbito federal e estadual, além de seguir as melhores práticas do mercado oriundas de recomendações tratadas em diretrizes e normas estabelecidas em padrões técnicos de mercado;

e. Os direitos de propriedade intelectual devem ser preservados, conforme legislações e acordos contratuais;

f. A empresa recomenda que se deve manter todos os licenciamentos apropriados na utilização de seus recursos e todos os usuários devem honrar os direitos de propriedade intelectual, bem como relatar à Central de Serviço se houver conhecimento de quaisquer violações;

g. Os contratos e termos de confidencialidade e/ou responsabilidade devem ser respeitados por todos os usuários ligados à empresa;

h. A segurança da informação deve fazer parte da rotina diária dos usuários ligados ao Sistema de Comunicação de Rádio e Tv Encontro das Águas, buscando garantir a disponibilidade, confidencialidade e integridade;

i. Qualquer violação da Política de Segurança da Informação deve ser relatada à Central de Serviços para que ações urgentes sejam tomadas na preservação dos aspectos de Segurança da Informação da empresa;

j. Os acessos aos ambientes tecnológicos devem ser realizados através de autenticação (ID e senha, logon e senha, digital, etc.) e de acordo com o perfil funcional do usuário, sendo a autenticação pessoal e intransferível;

k. O gestor da área deve analisar e classificar as informações sob sua competência, conforme grau de importância em relação ao impacto de sua divulgação;

l. A utilização de serviços de conectividade (ex.: internet, e-mail, etc.) deve ser restrita, controlada e voltada às atividades de trabalho do usuário;

m. Todos os equipamentos disponibilizados pela empresa às respectivas áreas devem ser utilizados no exercício das atividades de trabalho e ter um responsável;

n. O desenvolvimento, aquisição e manutenção das aplicações sistêmicas devem estar em conformidade com as legislações, regulamentações, contratos, acordos e procedimentos existentes, que preservem entre as respectivas partes os princípios base da segurança da informação;

o. Como forma de garantir e preservar a segurança da informação, o ambiente tecnológico deve ser monitorado e auditado periodicamente;

p. A Política de Segurança da Informação deverá ser revisada a cada 3(três) anos, ou quando a Equipe de Segurança da Informação e/ou o Comitê de TI achar necessário, assim como todos os outros documentos relacionados devem estar disponíveis a todos os usuários.

8. POLÍTICAS COMPLEMENTARES (PC)

A Política de Segurança da Informação (PSI) no âmbito do Sistema de Comunicação de Rádio e Tv Encontro das Águas, está estruturada com as Políticas Complementares indicadas a seguir, que tratam da gestão dos recursos tecnológicos e devem ser atendidas conforme sua especificidade:

8.1. PC01 – Política de Uso de Senhas

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso. Cabe aos usuários a memorização de suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário e números sequenciais, etc.

8.2. PC02 – Política de Uso do Correio Eletrônico

É vedada a utilização de webmail para envio de documentos ou informações do Sistema de Comunicação de Rádio e Tv Encontro das Águas a terceiros.

8.3. PC03 – Política de Resposta a Incidentes de Segurança da Informação

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas e redes. Alguns exemplos são: tentativa de uso ou acesso não autorizado a sistemas e dados, tentativa de tornar serviços indisponíveis, desrespeito à política de segurança. É responsabilidade dos Associados notificar a área de Risco Operacional ou Compliance, sempre que se deparar com uma atitude que considere abusiva ou com um incidente de segurança para que sejam tomadas as devidas ações, minimizando os impactos da ocorrência.

8.4. PC04 – Política de Classificação da Informação

As informações que transitam pelo Sistema de Comunicação de Rádio e Tv Encontro das Águas são, para fins desta Política, classificadas em quatro padrões distintos, a saber:

INFORMAÇÕES PÚBLICAS: Aquelas destinadas a disseminação fora da empresa. Possuem caráter informativo geral e são direcionadas a clientes ou investidores. Exemplos: material de marketing, clipping information, registros regulamentares e da Comissão de Valores Mobiliários.

INFORMAÇÕES INTERNAS: São aquelas destinadas ao uso dentro do Sistema de Comunicação de Rádio e Tv Encontro das Águas. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente a empresa ou seus clientes e associados. Essas informações não exigem proteções especiais salvo aquelas entendidas como mínimas para impedir a divulgação externa não intencional.

INFORMAÇÕES CONFIDENCIAIS: Também destinam-se a uso interno do Sistemas de Comunicação de Rádio e Tv Encontro das Águas. Entretanto, diferem das informações de natureza interna à medida que sua extensão em uma eventual divulgação, poderia afetar significativamente os negócios da empresa, seus clientes, investidores e associados. Exemplos: registros de funcionários, planos salariais, informações sobre clientes, sejam elas genéricas ou específicas, classificação de crédito, saldos de contas-correntes. Sua divulgação é proibida, salvo se solicitada por órgão fiscalizador competente (BACEN, CVM e Receita Federal, por exemplo), situação na qual deverá ser prestada por uma das seguintes pessoas: Contador, Controller, Auditor Interno, Advogado ou um dos sócios.

INFORMAÇÕES ALTAMENTE RESTRITAS: Correspondem a mais alta classificação de segurança para as informações que transitam na empresa. Destina-se às informações cuja divulgação não autorizada, provavelmente provocaria danos substanciais, constrangimentos ou penalidades a empresa, seus clientes, investidores ou associados. As pessoas designadas para o trato e uso de tais informações, têm a responsabilidade de garantir que elas sejam devidamente protegidas e seguramente armazenadas quando não estiverem em uso. Exemplos: informação antecipada e não autorizada de novos produtos ou serviços, informações de fusões, aquisições ou outras atividades do mercado de capitais não disponíveis ao público em geral. Em função desta categorização, é possível, quando do envio de informações sensíveis, a utilização de funcionalidade do Outlook, que permite classificar arquivos e mensagens conforme sua criticidade, que devem ser considerados sempre quando o mesmo for disponibilizado ou encaminhado para terceiros. Sempre que forem trocadas informações sensíveis, orienta-se a utilização de senhas, sistemas de criptografia ou EDI (Eletronic Data Interchange) minimizando riscos de que informações sensíveis à empresa sejam acessadas por terceiros.

8.5. PC05 – Política de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações

Para mantermos o ambiente lógico, todos os softwares/aplicações operacionais devem ser homologados pelos usuários das áreas envolvidas, que devem verificar os impactos das novas versões nos procedimentos, resultados e impostos.

Aquisição: A aquisição de softwares ocorrerá conforme planejamento orçamentário, com base na homologação técnica por parte da equipe de TI, após validação das necessidades de uso pela diretoria da empresa.

Instalação: Somente a equipe de TI INFRA está autorizada a realizar instalação de qualquer tipo de software, seja este um sistema ou um aplicativo simples, principalmente aqueles obtidos gratuitamente e/ou baixados da internet.

Licença de Uso: Somente poderão ser instalados e utilizados softwares devidamente licenciados para uso da empresa. Não é permitido instalar softwares pessoais, emprestados, de terceiros, que não sejam devidamente licenciados para uso da empresa pelo fabricante do produto.

Auditoria: Poderá ser utilizada pela equipe de TI INFRA uma ferramenta automatizada para auditoria de softwares instalados nos computadores.

Marcas e Modelos: Utilização de equipamentos padronizados pela equipe de TI INFRA.

Distribuição: Os computadores são disponibilizados conforme necessidades de uso de cada colaborador, com base nos softwares destinados à automação de sua área.

As impressoras ficarão distribuídas em centros de impressão, localizados em pontos que melhor atendam a maioria dos colaboradores e não estejam em áreas que impliquem em risco à segurança do patrimônio.

Propriedade: Os softwares, incluindo os desenvolvidos internamente, e recursos computacionais diversos pertencem exclusivamente a empresa, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas e criações intelectuais elaboradas e desenvolvidas pelos Servidores, Colaboradores, Prestadores de Serviços e Consultores, durante a vigência da relação de emprego ou relação contratual.

8.6. PC06 – Política de Uso da Internet

O acesso à Internet é permitido a todos os Associados usuários de computador, com o objetivo de facilitar suas tarefas. Assim como qualquer outro material de trabalho, as páginas da Internet também devem ser usadas somente para fins profissionais. Para uma utilização eficiente e produtiva algumas regras devem ser obedecidas:

- É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, atividades de hacker e quaisquer outras atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento da área de TI – HelpDesk;

- Fica proibido também o download de arquivos e programas não autorizados ou sem revisão e aprovação da TI – Infra;

- É vedado também o acesso à sites de Corretoras, com o objetivo de efetuar operações de renda variável.

8.7. PC07 – Política de Acesso Remoto

O Sistema de comunicação Encontro das Águas disponibiliza ainda acesso ao ambiente interno através de conexão remota segura, para a qual é necessária a utilização de um login e senha. Todos os usuários que eventualmente tenham necessidade de utilizar a rede interna deverão solicitar a aquisição de login e senha, que deverá ser autorizado pelo presidente, diretor ou chefe de departamento. O login e senha deverá ser utilizado com o máximo de cuidado em função da possibilidade de acesso ao ambiente interno da empresa, além de envolver custo por conta da aquisição de licença específica para esse fim.

8.8. PC08 – Política de Gestão de Ativos

Estabelecer a formalização da gestão de ativos da empresa.

8.9. PC09 – Política de Controle de Acesso

A empresa utiliza em sua plataforma de softwares sistemas desenvolvidos internamente e adquiridos de terceiros. Quando da admissão ou transferência de Associado a área de RH emite um Check list de admissão ou de transferência, para o qual cada área deve tomar uma ação específica. Dessa forma, para os acessos a sistemas, o novo funcionário recebe apenas acesso ao sistema em conformidade com o perfil espelho.

8.10. PC10 – Política de Dispositivos Móveis

Estabelecer regras e padrões na utilização e armazenamento dos dispositivos móveis utilizados nas atividades de trabalho da empresa

8.11. PC11 – Política de Backup Corporativo

O backup dos diretórios de rede é realizado diariamente através de processo automatizado ou manual, em fita e servidores específicos para essa função pelo setor de informática, sendo encaminhados para armazenamento (D+1).

8.12. PC12 – Política de Combate a Softwares Maliciosos

A qualquer indício de existência de vírus, o Associado deve interromper suas tarefas e comunicá-lo imediatamente à TI Infraestrutura, que executará os procedimentos para a erradicação de vírus determinados na Política de Segurança. Mesmo em caso de falta de notificação por parte

do Associado, o SEP (anti-vírus) envia um email de alerta para a área de TI passando todos os detalhes do fato ocorrido, facilitando uma ação rápida no intuito de evitar a propagação do problema.

Os esforços individuais e isolados dos usuários para acabar com os vírus podem contribuir para provocar danos ainda maiores, pois, em geral, estes usuários não estão capacitados para esta atividade.

O uso de softwares freeware ou shareware e arquivos em outras mídias constituem formas muito comuns de transferência de vírus para os computadores, portanto, sua utilização sem a prévia autorização da TI Infraestrutura é terminantemente proibida.

Além dos programas que protegem a rede, todos os computadores possuem software de verificação de integridade (agente do antivírus), que detecta alterações nos arquivos de configuração e nos softwares e alertam ao usuário da possibilidade de existência de vírus. Isso ocorrendo, o mesmo deve notificar a TI - Infra imediatamente.

Todos os equipamentos utilizados para gravação de informações em computadores que ligados à empresa deverão ser apresentados ao Departamento de TI para verificação e certificação da inexistência de vírus que possam ocasionar danos estrutura da empresa.

9. ADEQUAÇÃO À POLÍTICA

a. Os novos projetos de desenvolvimento ou novas aquisições de sistemas devem seguir os padrões estabelecidos nesta política;

b. As implementações para o ambiente tecnológico existente deverão ser adequadas a esta política no prazo máximo de 3(três) anos, a partir de sua publicação.

O escalonamento de implementação, deve seguir a seguinte ordem:

01- PC07 – Política de Acesso Remoto; 02- PC11 – Política de Backup Corporativo; 03- PC01 – Política de Uso de Senhas; 04- PC09 – Política de Controle de Acesso; 05- PC02 – Política de Uso do Correio Eletrônico; 06- PC06 – Política de Uso da Internet; 07- PC08 – Política de Gestão de Ativos; 08- PC10 – Política de Dispositivos Móveis; 09- PC04 – Política de Classificação da Informação; 10- PC03 – Política de Resposta a Incidentes de Segurança da Informação; 11- PC12 – Política de Combate a Softwares Maliciosos; e 12- PC05 – Política de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações.

c. Caso não seja possível a adequação das ferramentas, o Comitê de TI do Sistema de Comunicação de Rádio e Tv Encontro das Águas ou seus representantes devem documentar essa informação, bem como seus motivos, para fins de auditoria interna.

10. CONSIDERAÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do Sistema de Comunicação de Rádio e Tv Encontro das Águas. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição

11. REFERÊNCIAS LEGAIS E NORMATIVAS

Os documentos de referência desta política são normas e legislações referentes às estratégias públicas adotadas pela FUNTEC, quais sejam:

DOCUMENTOS DE REFERÊNCIA

Referência Legal Teor

ISO 27001: é uma norma internacional de Gestão de Segurança da Informação, que tem como princípio geral a adoção de um conjunto de requisitos, processos e controles, que visam gerir adequadamente os riscos de Segurança da Informação presentes nas organizações.

A ISO 27002: é mais um código de prática para controles de segurança. Ela descreve as melhores práticas para aqueles que implementam o SGSI, fornecendo diretrizes sobre a seleção, implementação e gerenciamento de controles levando em consideração os ambientes de risco da organização

A **Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP)**, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

ISO 27040:2013: Código de prática de armazenamento. Fornece orientações sobre como as organizações devem armazenar suas informações, tais como: documentos, planilhas e até mesmo a base de sistemas. Também conscientiza sobre políticas de recuperação de backup e a maneira de descarte de mídias que já foram utilizadas como backup.

NBR ISO 55000: 2014: Norma que fornece uma visão geral de gestão de ativos, seus princípios e terminologia, bem como os benefícios esperados.

NBR ISO 55001:2014: Norma que especifica requisitos para um sistema de gestão de ativos dentro do contexto da organização.

NBR ISO 55002:2014: Norma que fornece diretrizes para a aplicação de um sistema de gestão de ativos, de acordo com os requisitos da ABNT NBR ISO 55001.

NBR ISO/IEC 27001:2013: Norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

NBR ISO/IEC 27002:2013: Norma que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

NBR ISO/IEC 27005:2011: Norma que fornece diretrizes para o processo de gestão de riscos de segurança da informação.

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. ABNT NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação

ISO/IEC 15504: Tecnologia da Informação – Estabelece uma estrutura padrão para os processos de vida no desenvolvimento de software.

PASS 55: Especificação da Instituição Britânica de Padrões (British Standards Institution) para o gerenciamento de ativos físicos e infraestrutura.

CMMI (Capability Maturity Model – Integration ou Modelo de Maturidade em Capacitação – Integração) Modelo de referência para desenvolvimento e manutenção de software.

Control Objectives For Information end Related Technology - COBIT 5: Conjunto de boas práticas que visa dar suporte a Governança e Gerenciamento dos processos de tecnologia da informação.

Information Technology Infrastructure Library – ITIL V3: Conjunto de boas práticas para utilização na infraestrutura, operação e gerenciamento de serviços de tecnologia da informação.

MPS.BR (Melhoria de Processos do Software Brasileiro: Movimento para melhoria da qualidade de processo do Software Brasileiro.

Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet): Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Decreto nº 8.771, de 11 de maio de 2016 Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Lei nº 12.527, de 18 de novembro de 2011 Lei de acesso a informações. Lei nº 9.609, de 19 de fevereiro de 1998 Lei dos Direitos Autorais.

BIBLIOGRAFIA COMPLEMENTAR

Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, que passou a ser obrigatório em 25 de maio de 2018 e aplicável a todos os países da União Europeia