PORTARIA Nº 064/PATRIA, NA DATA DA ASSINATURA.

Ativa a Gerência de Segurança Corporativa e dispõe sobre a emissão de Normas Administrativas na Fundação PATRIA.

O DIRETOR-PRESIDENTE DA FUNDAÇÃO PARQUE DE ALTA TECNOLOGIA DA REGIÃO DE IPERÓ E ADJACÊNCIAS, no uso de suas atribuições legais constantes no Art. 30, Inciso VIII, Alínea f do Regimento Interno 8ª Revisão, resolve:

Art. 1º Ativar a Gerência de Segurança Corporativa criada na 9ª Alteração do Estatuto Social, aprovada em 23/03/2023, diretamente subordinada ao Diretor Administrativo.

Art. 2º Colocar em vigor as Normas Administrativas abaixo, anexas a esta Portaria, no âmbito da Fundação Parque de Alta Tecnologia da Região de Iperó e Adjacências (PATRIA):

DA - NA - 010 - 00 - Norma de Segurança Corporativa;
DA - NA - 011 - 00 - Norma de Segurança das Informações; e
DA – NA – 012 – 00 – Norma de Segurança Orgânica.

Art. 3º Extinguir a Gerência Administrativa, subordinando as Seções de Obtenção, de Apoio Administrativo e Recursos Humanos diretamente ao Diretor Administrativo, conforme estabelecido na 9ª Alteração do Estatuto Social, aprovada em 23/03/2023.

Art. 4º Cancelar a Norma DA – NA – 007 – 00 - Normas de Funcionamento da Gerência Administrativa.

Art. 5º Estabelecer o prazo de 90 (noventa dias) para a emissão das normas relativas ao funcionamento das Seções de Obtenção, de Apoio Administrativo e Recursos Humanos.

Art. 6º Esta Portaria entra na data da assinatura.

NEWTON CALVOSO PINTO HOMEM
Diretor-Presidente

Distribuição: Todos os elementos organizacionais da Fundação, ICT apoiadas e Arquivo.

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

NORMA DE SEGURANÇA DAS INFORMAÇÕES

CONTROLE DE MODIFICAÇÕES		
Modificação	**Data**	**Documento que modifica**
00	09/12/2024	Portaria 064/2024
Itens modificados		
Emissão inicial		

Modificação	**Data**	**Documento que modifica**
Itens modificados		

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

SUMÁRIO

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

1 – PROPÓSITO

Definir normas e procedimentos que deverão pautar as atividades da Fundação no que tange à Segurança das Informações (SI), em complemento DA – NA – 010 – 00 – Norma de Segurança Corporativa.

2 – CONSIDERAÇÕES SOBRE A SEGURANÇA DAS INFORMAÇÕES

Atualmente, a segurança vem se tornando uma das prioridades para as instituições, em especial, no que tange à SI, que passou a ser considerada requisito essencial para competir numa economia globalizada e para atingir resultados sustentáveis a longo prazo.

A crescente utilização de tecnologia nos processos de negócio cria vantagens competitivas. Entretanto, crescentes vulnerabilidades dos sistemas e tecnologias introduzidas no suporte aos negócios, aliadas a crescentes ameaças com elevado grau de sofisticação, expõem as instituições a novos riscos a cada dia.

Nesse cenário, a abordagem tradicional de gestão da segurança da informação, com foco apenas na utilização de ferramentas tecnológicas, torna-se inadequada. A segurança da informação digital situa-se num contexto organizacional e operacional mais amplo e, portanto, não pode ser gerenciada como uma disciplina estanque.

3 – APLICAÇÃO

Esta Norma se aplica aos Empregados da Fundação PATRIA e a todos que trabalham com ela.

4- REFERÊNCIAS

Lei 12.527 (Lei de Acesso à Informação)

NBR ISO/IEC 27001 Associação Brasileira de Normas Técnicas (ABNT). NORMA ISO/IEC 27001- 2006 – Sistemas de Gestão da Segurança da Informação – Requisito, 2006.

NBR ISO/IEC 27002 Associação Brasileira de Normas Técnicas (ABNT). NORMA ISO/IEC 17799:2005 – Código de Prática para a Gestão da Segurança da Informação, 2005.

DA - NA - 010 - 00 - Norma de Segurança Corporativa

5 – DEFINIÇÕES

5.1 - SI e suas Definições

Segurança da Informação: É a garantia dos requisitos da informação a saber: confiabilidade, disponibilidade, sigilo, integridade, autenticidade e não repúdio.

Confiabilidade: Conjunto de atributos que garante a qualidade das informações.

Disponibilidade: Atributo que garante a acessibilidade e utilização sob demanda da informação ou dos ativos de informação por uma pessoa física, órgão, entidade ou sistema.

Sigilo: Atributo que garante que a informação sensível não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada pelo proprietário do documento.

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Integridade: Atributo que garante que a informação não seja modificada ou destruída de maneira não autorizada ou acidental.

Autenticidade: Atributo que garante que uma informação provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo.

Não-Repúdio: Atributo que garante que o autor de uma informação ou dado não negue falsamente a sua autoria.

Evento de Segurança da Informação: Qualquer ocorrência que indique uma possível violação da política de segurança, da segurança, da falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a SI.

Incidente de Segurança da Informação: Indicado por um único ou por uma série de eventos não autorizados, sequenciais ou não, de segurança da informação indesejados ou inesperados, por agentes internos ou externos, voluntários ou não, que tenham potencialidade de comprometer e ameaçar a SI.

Política de Segurança da Informação: Regras a serem cumpridas pela organização para orientação e apoio às medidas de implementação de SI.

Segurança Orgânica no âmbito da SI: compreende a adoção de um conjunto de medidas que visem à prevenção e à obstrução de ações e ocorrências adversas de qualquer natureza contra sistemas de informação.

5.2 Sensibilidade, Criticidade e Acesso Sigiloso

Sensibilidade: qualidade do conteúdo de uma informação que determina as diretrizes para o estabelecimento do seu sigilo.

Criticidade: nível de impacto na administração da Fundação ou de instituições apoiadas, que pode advir da divulgação indevida de informação sensível.

Acesso Sigiloso: É a possibilidade ou a oportunidade de uma pessoa ter contato com dado sigiloso. Expressa, não apenas o ato de uma pessoa obter conhecimentos, dados ou material digital de interesse, mas também a condição para o fazer, seja por meio de autorização oficial emanada de autoridade competente, seja pela exploração das vulnerabilidades das medidas de salvaguarda aplicadas aos mesmos.

5.3 Áreas Sensível e Sigilosa

Compartimentação: É o resultado de todas as medidas que visam restringir o acesso a dados e conhecimentos digitais sigilosos às pessoas que não possuem a necessidade ou autorização de conhecê-los.

Área Sensível: Área física ou digital considerada vital para o pleno funcionamento da empresa, em função do material existente na mesma ou das atividades ali desenvolvidas.

Área Sigilosa: São áreas físicas ou digitais sensíveis que abrigam material sigiloso.

5.4 Quanto ao Tipo de Ameaça

Ameaça Não-Intencional: É uma ameaça à segurança e à integridade da informação digital realizada de forma não intencional. Por exemplo: acesso a plataformas não autorizadas na Internet; abandono do computador com dados exibidos na tela; exposição de listagens, relatórios ou outros documentos sigilosos (em mídias eletrônicas ou em papel) facilitando a observação ou extravio; difusão da senha por telefone ou na presença de pessoas não

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

autorizadas; não realização de *logout* após o encerramento dos trabalhos; acesso de pessoal não autorizado à sala do Servidor ou às dependências com microcomputadores e compartilhamento de pastas na rede de forma não autorizada.

Ameaça Intencional: É uma ameaça à segurança e à integridade da informação digital realizada de forma intencional. Tem como objetivo negar a disponibilidade e/ou comprometer a integridade da informação. Por exemplo: tentativa de efetuar *login* na rede como se fosse um usuário legítimo; obtenção de arquivos (listagens e mídias eletrônicas) por furto/pirataria ou cópia; ação de programas maliciosos que buscam quebrar senhas, obter informações ou comprometer a segurança da rede de dados; entrada e saída de mídias eletrônicas da Fundação sem o devido controle; comprometimento de *hardwares* e *softwares*; ação revelando medidas de proteção e acesso de usuários à rede sem as devidas medidas de segurança; instalação de *software* que possibilite a captura total ou parcial dos dados de uma estação de trabalho.

6 – TRATAMENTO DOS RECURSOS COMPUTACIONAIS DISPONÍVEIS

A Gerência de Segurança Corporativa, responsável pela Gestão do Setor de Tecnologia da Informação (TI), provê aos Empregados o uso de computadores, dispositivos periféricos e sistemas de informação como forma de apoio para o desempenho adequado de suas atribuições profissionais.

O acesso aos recursos computacionais está condicionado às necessidades do Empregados para realização das suas atribuições profissionais e somente aqueles cujas atividades requeiram o uso de computador terão acesso a essa ferramenta.

Todo Empregado que tiver necessidade de utilizar recursos computacionais para a realização de suas atividades deverá solicitar tal recurso ao seu Gerente. Este preencherá o formulário "Solicitação de Recursos de Tecnologia da Informação", constante do Anexo I, a fim de solicitar recursos de TI e acesso a sistemas de informação para os Empregados sob sua responsabilidade.

As autorizações de acesso aos recursos computacionais existentes na Fundação, e às informações por eles disponibilizadas, deverão ser controladas pelo Gestor do Setor de TI, sendo sua atribuição validar as condições para a concessão do acesso e conceder o acesso solicitado.

7 – RESPONSABILIDADES E ATRIBUIÇÕES

Para cumprir o que é estabelecido nesta Norma, são definidos dois elementos organizacionais: o Gestor da Segurança das Informações (GSI) e o Administrador da Rede Local (ARL):

7.1 – Do Gestor da Segurança das Informações (GSI)

É desejável que o GSI possua conhecimentos de redes locais de computadores, sistemas operacionais de rede, protocolos de comunicação, serviços disponibilizados pela rede (sistemas de informação, outros) e conhecimento em auditoria de redes.

Cabe ao GSI:

a) Divulgar, fazer cumprir e propor atualizações a esta Norma;

b) Coordenar, junto aos demais setores da Fundação, o estabelecimento dos planos de capacitação de SI e zelar pelo seu cumprimento;

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

c) Assessorar a Diretoria Executiva quanto aos assuntos de SI;

d) Propor à Diretoria Executiva a restrição e/ou a liberação de acesso a sítios da rede mundial de computadores, redes sociais, etc.

e) Orientar e supervisionar o ARL nos assuntos de SI;

f) Identificar os recursos de informática que necessitam de proteção, de acordo com o respectivo grau de sigilo da informação por eles processada ou armazenada;

g) Supervisionar a elaboração e a manutenção do Histórico da Rede Local (HRL);

h) Planejar e implementar um programa de treinamento de SI para os Empregados da Fundação;

i) Divulgar recomendações referentes às técnicas de Engenharia Social, a fim de minimizar a probabilidade de estranhos à Fundação obterem sucesso na aplicação de tais técnicas pelos meios de comunicação disponíveis;

j) Garantir que os usuários estejam cientes das instruções contidas nesta norma por meio da assinatura do Termo de Responsabilidade Individual - TRI (Anexo II);

k) Garantir que os usuários que possuam estações de trabalho (ET) tenham assinado o Termo de Recebimento de Estação de Trabalho - TRE (Anexo III);

l) Realizar auditoria interna de SI, semestralmente, emitindo um relatório;

x) propor auditoria de SI, quando verificar necessidade de tal;

m) Exigir dos prestadores de serviço na rede local a assinatura do TRI (Anexo II) e o cumprimento das regras estabelecidas naquele termo para proteção do sigilo das informações a que possa ter acesso; e

n) Avaliar as solicitações de usuários para acesso a redes ponto-a-ponto (P2P) e redes sociais, autorizando quando atender à necessidade do serviço e não comprometer a SI.

7.2 - Do Administrador da Rede Local (ARL)

O ARL deverá ter, preferencialmente, habilitação em Administração de Rede de Computadores e, se possível, para os sistemas operacionais que estejam sendo utilizados dentro da Fundação, assim como conhecimentos em auditoria de sistemas computacionais.

Cabe ao ARL:

a) Gerenciar a rede local de forma a mantê-la operando dentro dos seus requisitos operacionais e com todos seus serviços em funcionamento;

b) Verificar periodicamente a integridade física dos equipamentos de conectividade instalados na Fundação (roteadores, servidores web, equipamentos de rádio enlace, switches, pares metálicos, cabos ópticos, etc.), comunicando imediatamente ao GSI qualquer avaria detectada ou a impossibilidade de manter os referidos equipamentos em um ambiente adequado ao seu funcionamento;

c) Fazer cumprir o planejamento de treinamento dos Empregados da Fundação em SI;

d) Orientar a não divulgação de características da rede local a pessoas externas à Fundação. No caso de prestação de serviço de TI por pessoas externas à empresa, deve-se ter o cuidado de expor apenas as informações necessárias atinentes ao serviço específico. Além disso, deve-se exigir a assinatura do TRI (Anexo II) por parte dos prestadores de serviço;

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

e) Elaborar, controlar e manter o Histórico da Rede Local (HRL);

f) Auxiliar o GSI na divulgação desta Norma;

g) Assessorar o GSI na avaliação dos incidentes de segurança;

h) Criar, apagar ou alterar perfis ou privilégios de usuários ou grupos de usuários, quando aplicável, documentando estas atividades;

i) Estabelecer o controle dos acessos aos sistemas e serviços disponibilizados na rede local e das suas respectivas autorizações, por meio de um cadastro atualizado dos usuários que utilizam os sistemas da rede local e dos que não têm autorização para tal;

j) Realizar, quando aplicável, manutenções periódicas das contas e direitos dos usuários, observando eventuais inatividades de contas, incidência de algum usuário em grupos diferentes e tentativas de acessos não-autorizados;

k) Efetuar e garantir as atualizações dos sistemas existentes no ambiente computacional e rede local;

l) Garantir que as cópias de segurança (*backups*), sejam feitas e guardadas de forma correta e segura;

m) Configurar as estações de trabalho com privilégio mínimo para o usuário e entregá-las, mediante a assinatura do TRE (Anexo III). No caso de transferência de estações de trabalho entre usuários, realizar cópia de segurança (*backups*) dos dados existentes, antes de "formatar" o disco rígido e restabelecer a configuração padrão da empresa;

n) Garantir que os serviços (instalações, manutenções ou correções) realizados na rede local sejam feitos sem afetar a segurança dos sistemas de informações digitais;

o) Coibir acessos à rede local por modem, celular ou outras redes sem fio não autorizadas; e

p) Garantir que todos estejam cientes das instruções em vigor para a SI do ambiente computacional da empresa, por meio da assinatura do TRI (Anexo II) pelos usuários que acessam a rede local.

7.3 - Do Usuário

O usuário deverá estar ciente das suas responsabilidades sobre SI. Para garantir o atendimento desse requisito, ele estará apto a receber uma estação de trabalho somente após a assinatura do TRE (Anexo III), ficando autorizado a acessar a rede local da Fundação após tomar ciência das normas da SI e assinar o TRI (Anexo II). Dessa forma, o usuário toma formalmente ciência de sua responsabilidade pelas consequências decorrentes da não observância desta Norma e da legislação vigente.

Além de cumprir, rigorosamente, as normas previstas, o usuário deverá atentar para os seguintes procedimentos:

a) Tratar a informação digital como patrimônio da Fundação e como um recurso que deva ter seu sigilo preservado, como definido no Termo de Manutenção de Sigilo assinado quando da sua contratação;

b) Utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso da Fundação exclusivamente para o interesse do serviço;

c) Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

d) Não tentar obter acesso à informação cujo teor não tenha autorização ou necessidade de conhecer;

e) Não se fazer passar por outro usuário usando a identificação de acesso (*login*) e senha de terceiros;

f) Não alterar o endereço de rede ou qualquer outro dado de identificação de sua estação de trabalho e estar ciente de que é proibida a instalação de modem ou outro dispositivo de comunicação externa em equipamento interligado à rede local da Fundação;

g) Utilizar, em sua estação de trabalho, somente programas homologados e licenciados para uso na Fundação. Casos específicos devem ser analisados pelo GSI;

h) No caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos a que teve acesso;

i) Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional da Fundação, com terceiros;

j) Seguir as regras básicas para a elaboração e uso de senhas, como descrito no item 8.6;

k) Seguir as orientações do GSI relativas ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;

l) Comunicar imediatamente ao seu superior hierárquico e ao GSI a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de SI estabelecidos;

m) Responder, perante a Fundação, por acessos, tentativas de acessos ou uso indevidos da informação digital, realizados com a sua identificação ou autenticação;

n) Não praticar quaisquer atos que possam afetar a confiabilidade e o sigilo da informação;

o) Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

p) Não realizar nenhum tipo de acesso a redes ponto-a-ponto (“P2P”) e redes sociais sem a devida autorização e obedecer a instruções próprias para os casos autorizados;

q) Não transferir qualquer tipo de arquivo que pertença à Fundação para outro local, seja por meio magnético ou não, exceto no interesse do serviço;

r) Adotar a “política de mesa e tela limpas”, durante e fora do horário normal de trabalho. Essa política leva em consideração que:

- Informações sensíveis em papel ou mídia de armazenamento eletrônico devem ser guardadas em lugar seguro (idealmente em cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando a estação de trabalho estiver desocupada;

- Computadores e terminais devem ser mantidos desligados ou protegidos com mecanismos de travamento de tela, com senha, ou mecanismos de autenticação similar quando não usados; e

- Documentos com informação sensível devem ser removidos de impressoras imediatamente.

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

s) Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam do interesse do serviço são expressamente proibidos no ambiente computacional da Fundação;

t) Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional da Fundação pode ser auditada;

u) Estar ciente de que o correio eletrônico e o "*chat*" devem ser utilizados para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida, no ambiente computacional da Fundação, pode ser auditada;

v) Não movimentar qualquer equipamento ou parte dele, sem o conhecimento do ARL;

w) Não conectar computadores pessoais na rede local da Fundação, sem autorização do ARL;

x) Realizar uma prévia análise ou varredura por programas antivírus, antes de executar, copiar ou reter arquivos recebidos de outras empresas e de usuários externos; e

y) Observar os procedimentos para *backup* de arquivos descritos no item 14.

7.4 Do responsável pelo cumprimento da Lei de Acesso à Informação

O GSI será o responsável pelo cumprimento da Lei 12.527 (Lei de Acesso à Informação), no que cabe à Fundação:

I - Assegurar o cumprimento da Lei de Acesso à Informação, de forma eficiente e adequada;

II - Monitorar a implementação do disposto naquela Lei, no que se refere à Fundação; e

III - Recomendar as medidas indispensáveis à implementação dos procedimentos necessários ao correto cumprimento do disposto naquela Lei.

8 –PRIORIDADES E AÇÕES DE SEGURANÇA (AS)

No ambiente computacional integrado por uma rede local, alguns recursos são considerados críticos em relação aos riscos de segurança aos quais são expostos, pois suas vulnerabilidades afetarão diretamente os requisitos básicos de SI.

Para efeito deste Manual, são considerados críticos o Servidor SAGI, o Servidor de Arquivos, os Equipamentos e a Infraestrutura de Conectividade da Rede e as Estações de Trabalho.

São listados a seguir os recursos críticos com as respectivas prioridades e ações de segurança físicas para manutenção do funcionamento da rede local e sua conectividade.

8.1 - Prioridade 1 -Servidor do SAGI e Servidor de Arquivos

AS1.1 - Segurança Física dos Servidores: Para atender à segurança física citada, as seguintes ações de segurança devem ser implementadas:

a) A sala dos servidores poderá ser acessada apenas por pessoal da Gerência de Segurança Corporativa (GSC);

b) A sala de servidores deverá ter instalada uma câmera que registre o acesso com gravação em mídia externa à Fundação mantida por, pelo menos, 7 dias; e

c) Proibir o porte de equipamentos de armazenamento de informações, câmeras fotográficas e celulares com câmera dentro da sala dos servidores.

AS1.2 – Segurança Lógica de Servidores: Para atender à segurança lógica citada, as seguintes ações de segurança devem ser implementadas:

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

a) Analisar as vulnerabilidades lógicas atinentes aos protocolos e à configuração implementada com os mesmos;

b) Atualizar os programas e as correções (*patches*), disponibilizadas pelos fabricantes ou distribuidores dos sistemas operacionais e dos aplicativos em uso; e

c) Desabilitar todos os serviços não necessários, observando o princípio do privilégio mínimo, desinstalando-se todos esses serviços e fechando-se as portas lógicas que não estiverem efetivamente em uso. Estes dispositivos serão habilitados somente quando for estritamente necessário ao serviço.

8.2 - Prioridade 2 - Equipamentos e Infraestrutura de Conectividade da Rede

AS2.1 - Segurança Física dos Dispositivos de Conectividade: Para assegurar que os equipamentos (roteadores e switches) e cabeamento que compõem os elementos ativos de conectividade, não sejam alvo de manipulação imperceptível (cópia, alteração, inserção ou destruição) das mensagens que ali trafegam, as seguintes ações de segurança devem ser implementadas:

a) Proteger todos os equipamentos de conectividade, utilizando gabinetes com lacre numerado; e

b) No caso dos cabeamentos, os segmentos dos mesmos devem ser lançados em sua maioria de forma que não fiquem visíveis. Apenas os Line Cord poderão ter alguma visibilidade.

AS2.2 – Segurança Lógica dos Dispositivos de Conectividade: Para minimizar ou dirimir as vulnerabilidades lógicas normalmente encontradas nos dispositivos de conectividade, as seguintes ações de segurança devem ser implementadas:

a) No caso de roteadores e switches gerenciáveis alterar a configuração de fábrica para uma configuração segura (mudança de senha, alteração de portas, etc); e

b) No caso dos cabeamentos, os segmentos dos mesmos devem ser lançados em sua maioria de forma que não fiquem visíveis. Apenas os Line Cord poderão ter alguma visibilidade.

8.3 - Prioridade 3 -Estações de Trabalho

AS3.1 - Segurança Física das Estações de Trabalho: Para mitigar os efeitos da ação maliciosa, intencional ou não, com relação à segurança da Estação de Trabalho, as seguintes ações de segurança devem ser implementadas:

a) Evitar o uso de microfones em estações de trabalho, quando não for estritamente necessário, pois estes podem ser ativados indevidamente, por vírus ou por ataques direcionados, capturando toda e qualquer conversa efetuada nas áreas próximas ao equipamento; e

b) Quando uma estação de trabalho necessitar de manutenção fora da Fundação, a manutenção somente poderá ser feita com a autorização formal do GSI.

AS3.2 – Segurança Lógica das Estações de Trabalho: Para mitigar os efeitos de ação lógica maliciosa, intencional ou não, as seguintes ações de segurança devem ser implementadas:

a) Utilizar programas de proteção de estação de trabalho contra atividades e programas maliciosos e homologados pela Fundação, tais como antivírus e *anti-spyware*;

b) Manter a verificação automática pelo antivírus ativada em todas as estações de trabalho;

c) Efetuar as atualizações de aplicativos, de acordo com a orientação do GSI;

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

d) Configurar a Estação de Trabalho segundo o princípio do privilégio mínimo;

e) Ter somente os programas homologados e licenciados pela Fundação instalados na Estação de Trabalho e todas as portas e serviços desnecessários desabilitados;

f) Retirar do usuário os direitos de administrador das Estações de Trabalho.

g) Desabilitar ou desinstalar, sem prejuízo das funções inerentes ao usuário, qualquer dispositivo de entrada e saída de dados, portas USB e impressoras locais. Estes dispositivos serão habilitados somente quando for estritamente necessário ao serviço e a solicitação de liberação deverá ser enviada ao GSI;

h) Submeter as estações de trabalho a um serviço de diretório, gerenciado pelo GSI e não permitir acesso aos serviços disponibilizados sem o registro de acesso do usuário nesse serviço;

i) Cada estação de trabalho deverá ter uma senha de configuração (*setup*), de conhecimento exclusivo do ARL, a fim de evitar que o próprio usuário ou qualquer pessoa não autorizada altere a configuração da máquina. A senha deverá ficar em envelope lacrado de posse do GSI;

j) Cada estação de trabalho deverá ter uma senha de usuário para acesso ao ambiente de trabalho a fim de evitar que qualquer pessoa não autorizada utilize a referida estação para acesso à rede e consequentemente aos Servidores;

k) Quando houver a necessidade de não estar à frente da estação de trabalho por qualquer razão, o usuário deverá se utilizar das teclas Ctrl+Alt+Del ou Windows + L de forma a bloquear a tela do computador sendo necessário a partir desse ponto reinserir a senha de acesso ao ambiente de trabalho;

l) É vedada a configuração e a disponibilização de discos, diretórios ou arquivos compartilhados nas estações de trabalho, mesmo que se configure seu acesso por senha, em virtude da vulnerabilidade desses compartilhamentos. Deve ser utilizado um servidor de arquivos ou outra solução homologada para suprir tal necessidade;

m) O uso de redes sem fio para a interligação de equipamentos na rede local deve ser o meio alternativo válido apenas para mitigação de problemas que porventura ocorram no segmento físico devendo ser evitado a sua utilização sempre que possível; e

n) Não permitir acesso remoto às máquinas por pessoas não autorizadas.

9 – OUTRAS AÇÕES DE SEGURANÇAS FÍSICA E LÓGICA

9.1 Proteção da Alimentação Elétrica dos Equipamentos

A alimentação elétrica dos equipamentos também requer cuidado, pois sua falha pode impactar o requisito básico de disponibilidade. Para tal, é desejável que todos os equipamentos críticos estejam protegidos por fontes estabilizadas e sistemas de alimentação em emergência (*nobreaks*).

9.2 Realização de Serviços na Rede Local

Para a execução de quaisquer serviços (implementações, instalações, configurações, correções, verificações, medições, substituições, interligações, elaborações de projetos, suporte técnico, manutenções, etc.) na rede local, por pessoal externo, deve ser exigido assinatura do TRI (Anexo II).

9.3 – Regras Básicas para a Confecção e o Uso de Senhas

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Toda e qualquer senha é sempre individual e intransferível, devendo seu responsável:

a) Nunca a compartilhar;

b) As senhas utilizadas para acesso à rede local devem ter, no mínimo, 08 (oito) caracteres.

c) Não utilizar sequência fácil ou óbvia de caracteres, que facilite a sua descoberta;

d) Não utilizar palavras existentes em dicionários;

e) Utilizar aleatoriamente letras minúsculas, letras maiúsculas, números e caracteres especiais, cumprindo a política de configuração e de tamanho de senhas que estiver em vigor nos programas e serviços em uso;

f) Não a escrever em lugares visíveis, de fácil acesso ou em claro; e

g) Proceder às devidas precauções para mantê-la em sigilo, conforme previsto também no TRI (Anexo II).

9.4 - Uso de Antivírus e outros Programas de Proteção Individual

Devido ao caráter dinâmico, rápido e agressivo dos programas maliciosos e de outras ameaças, as configurações de uso e de atualização dos programas de proteção individuais devem ter seu gerenciamento centralizado, permitindo o sincronismo, velocidade de reação e atualização, fundamentais para a proteção de uma rede.

Ressalta-se que somente devem ser utilizados os programas homologados e previamente autorizados para uso na Fundação. O emprego de programas não homologados pode impactar negativamente o desempenho e a segurança da rede, além de possibilitar o surgimento de novas vulnerabilidades. O uso indevido de tais programas ou sua configuração incorreta, podem, além do acima citado, causar uma falsa impressão de segurança e facilitar determinados tipos de ataque.

9.5 – Instalação de Programas para Uso em Rede, Equipamentos ou Dispositivos

É vedada a instalação de qualquer programa, equipamento ou dispositivo voltado à segurança de rede local (*softwares* para análise de tráfego, etc.) ou de Estações de Trabalho (antivírus, anti *spywares*, etc.), sem análise e autorização prévia do GSI.

Por serem mecanismos voltados à SI, o uso indevido ou a configuração incorreta podem, além de impactar negativamente o desempenho e a segurança da rede, causar uma falsa impressão de segurança e facilitar determinados tipos de ataques.

9.6 – Segurança do Tráfego da Informação e Comunicações

Por questões de segurança, de forma a minimizar ou mesmo evitar a entrada de softwares maliciosos, é vedado o uso de redes sociais, tais como, Facebook, Instagram e Twitter a partir de estações de trabalho, por esta ser uma rede para fins operacionais da Fundação. Os usuários que, de acordo com o seu exercício funcional e a missão da empresa, tiverem a necessidade de acesso às mídias e redes sociais a partir de estações de trabalho, deverão ter autorização concedida pelo GSI.

Para utilização de ambientes de software, que funcionam como ferramentas de WorkFlow, tais como, Whatsapp e o Workspace Google, pelo qual, trafegam informações administrativas sensíveis, o usuário deve observar o item 7.3, em especial, ao que se refere às alíneas a, b, c, d, q, i, m, n, o, q, s, u e o item 10.

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

9.7 – Engenharia Social

A engenharia social corresponde ao conjunto de técnicas para se obter ou comprometer informações sobre uma organização ou seus sistemas computacionais, utilizando-se como ferramenta de ataque a interação humana ou as habilidades e fragilidades sociais do ser humano.

A engenharia social deve ser tratada por todos da empresa como uma ameaça à SI, onde toda informação sobre as características da empresa e de sua rede local é considerada sigilosa, exigindo o tratamento adequado de segurança.

Para minimizar a probabilidade de estranhos à empresa obterem sucesso na aplicação de tais técnicas pelos meios de comunicação disponíveis, devem ser seguidas, no mínimo, as seguintes orientações:

a. Não passar informações de nomes, telefones e outras informações pessoais de qualquer Empregado;

b. Não confirmar a estranhos a existência de determinada pessoa na Fundação;

c. Ao atender uma chamada telefônica, não se identificar sem que antes o interlocutor, que efetuou a ligação, tenha se identificado;

d. Não passar a estranhos nenhuma informação sobre os sistemas utilizados na rede local, tais como: sistemas operacionais, aplicativos, serviços disponibilizados, endereços de rede, computadores, roteadores, servidores, localizações físicas, topologia da rede, sistemas de segurança, entre outros; e

e. Não passar para estranhos informações a respeito da rotina e dos procedimentos internos da Fundação.

f. Qualquer suspeita de tentativa de Engenharia Social (e-mails suspeitos, links, contatos por *WhatsApp*, etc.) deve ser comunicada ao GSI.

9.8 – Uso de Modem em Estações de Trabalho e Equipamentos Servidores

Não é permitida a instalação de modem de nenhuma espécie, inclusive os 3G/4G/5G, em equipamento interligado à rede local da empresa. No caso da eventual necessidade de se utilizar modem 3G/4G/5G como solução de acesso, tal procedimento deverá ser autorizado pelo GSI.

10 – CORREIO ELETRÔNICO

O correio eletrônico corresponde ao serviço de troca de mensagens entre usuários da Fundação ou entre estes e usuários externos. As mensagens de correio eletrônico também podem transportar arquivos digitais em anexo. Pela sua eficiência como meio de comunicação, a propagação de ameaças e ataques pelo serviço de correio eletrônico é rápida e muitas vezes avassaladora, como, por exemplo, a propagação de um ataque por vírus.

Para utilizar o serviço de correio eletrônico de forma segura e minimizar possíveis ameaças à SI que podem vir tanto no corpo da mensagem quanto em seus anexos, as seguintes regras devem ser seguidas por todos os usuários:

a. O uso do correio eletrônico deve ser feito com cautela e apenas para assuntos de trabalho;

b. Não é permitido mandar e-mails com correntes, propagandas não solicitadas e com ofensas a terceiros;

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

c. Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

d. Apenas retransmitir e-mails encadeados quando o destinatário realmente tiver necessidade de conhecer os e-mails retransmitidos;

e. Caso sejam instalados na rede local da Fundação, servidores de correio eletrônico, os mesmos devem ficar em compartimentos de acesso restrito e controlado;

f. Não devem ser executados, copiados ou retidos arquivos recebidos em anexo a mensagens de correio eletrônico sem uma prévia análise ou varredura por programas específicos de controle e verificação de ataques, como por exemplo programas antivírus;

g. Se houver qualquer dúvida quanto à origem de mensagem recebida, esta ocorrência deve ser notificada ao ARL, para análise, antes da abertura da mensagem;

h. Devem ser utilizados os programas certificados pela Fundação para assinatura digital, em especial, quando de seu uso para envio pelo serviço de correio eletrônico;

i. É proibido o uso de programas para criptografia de arquivos e mensagens que não sejam autorizados pela Fundação;

j. Conforme indicado no TRI, toda informação processada, armazenada ou em trâmite no ambiente computacional da Fundação pode ser auditada, incluindo o correio eletrônico; e

k. Utilizar o correio eletrônico para envio de boato pode gerar responsabilidade civil e criminal.

11 - TREINAMENTO

11.1 – Treinamentos de SI versus Mentalidade de Segurança

O esforço para as atividades da SI deve ser de todos e não somente do pessoal diretamente envolvido com o setor de TI da Fundação. O fator mais importante para a SI é a existência de uma mentalidade de segurança incutida em todo o pessoal. Pouco adiantará o estabelecimento de rigorosas medidas de segurança se os envolvidos em sua aplicação não estiverem conscientizados.

Para tal conscientização o GSI deverá planejar um programa de treinamento de SI, em acordo com o item 12.2, de modo a auxiliar na manutenção e garantia de uma elevada mentalidade de segurança. Consequentemente, deverá haver um controle desses adestramentos, indicando qual o pessoal treinado e o tipo de treinamento ministrado a cada Empregado, de modo a possibilitar novos planejamentos para a manutenção dos níveis mínimos de conhecimento de SI na organização.

Como regra fundamental, todo pessoal recém-contratado deverá receber um treinamento básico de SI antes de iniciar o desempenho de qualquer atividade.

11.2 - Planos de Adestramento de SI

São documentos ostensivos que visam ações de treinamento de um determinado tema de SI. Exemplos de temas que podem ser contemplados em um Plano de Adestramento de SI:

a) Treinamento Básico de SI (para o pessoal que tenha recém-chegado à Fundação, incluindo esta Norma);

b) Conceitos Gerais de SI;

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

c) Recursos de SI;

d) Legislação, Normas e Documentos de SI;

e) Ativação dos Planos de Contingência da empresa (teoria e prática);

f) Segurança Orgânica, no que se refere à SI;

g) Recursos Criptológicos;

h) Engenharia Social; e

i) Crimes de Informática.

Os assuntos acima formam um conjunto mínimo de temas a serem abordados, podendo o ARL juntar vários em um mesmo treinamento ou acrescentar outros novos, de acordo com a necessidade.

12 – GESTÃO DE RISCOS EM SEGURANÇA DAS INFORMAÇÕES (GRSI)

A Gestão de Riscos em Segurança das Informações (GRSI) é uma abordagem sistemática para apoio à decisão que visa priorizar as medidas que contribuam para aumentar a eficiência da Segurança das Informações, as quais serão agrupadas sob o significado de Segurança das Informações (SI). Faz-se necessário que as ações de SI lidem com os riscos de maneira efetiva e no tempo apropriado, onde e quando forem necessários e que a GRSI seja parte integrante das atividades inerentes à SIC.

A GRSI é um processo contínuo e deve possuir contextos definidos, avaliar os riscos e tratá-los por meio de um plano de tratamento, a fim de implementar as recomendações e decisões em ordem de prioridade. Neste processo, é necessário que a gestão de riscos analise os possíveis acontecimentos e suas consequências (impacto), antes do processo de decisão, a fim de reduzir os riscos a níveis aceitáveis. Ou seja, o processo de GRSI deve ser aplicado com metodologia própria, sendo essencial na identificação das necessidades da Fundação nessas áreas. Portanto, a GRSI deve contribuir para a (o):

a. Identificação de riscos;

b. Análise e avaliação dos riscos em função do impacto e da probabilidade de sua ocorrência;

c. Compreensão dos significados das probabilidades e das consequências dos riscos;

d. Estabelecimento da ordem prioritária das ações para tratamento do risco;

e. Envolvimento das diversas áreas partícipes do processo de gestão do risco; e

f. Eficácia do monitoramento do tratamento do risco.

13 – DOCUMENTOS DE SEGURANÇA DAS INFORMAÇÕES

13.1 - Histórico da Rede Local (HRL)

O HRL tem por objetivo manter um memorial descritivo e o registro de todas as atividades e transações normais e de rotina que podem afetar de alguma forma a SI. O HRL está voltado às ações de histórico, análise de incidentes, prevenção e correção. A elaboração, o controle e a manutenção do HRL são de responsabilidade do ARL, sob supervisão do GSI. O HRL deve ser composto de três partes:

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

13.1.1 - Parte I: Descrição da Rede

Esta parte deve apresentar o estado atualizado da rede local e seu respectivo ambiente (diagrama de rede, número de máquinas, configuração, licenças instaladas, etc.)

13.1.2 - Parte II: Atividades de Rotina

Estas atividades correspondem aos eventos rotineiros de segurança da rede (manutenção, verificação de licenças, verificação de vírus, instalação e atualização de softwares, etc.)

13.1.3 - Parte III: Incidentes

Esta parte tem como objetivo registrar qualquer incidente que afete a SI. O relato imediato de qualquer incidente é de responsabilidade de todos os usuários da rede local. A omissão de relato, pelo usuário, de um incidente que possa afetar a SI está sujeita a responsabilização, pois contraria a presente Norma e o previsto no TRI. O registro do incidente (Anexo IV) deve ser feito de forma clara e objetiva e a análise do ocorrido deverá ser feita pelo ARL para posterior apresentação ao GSI.

14 – AUDITORIAS DE SEGURANÇA DAS INFORMAÇÕES

14.1 - Finalidade das Auditorias de SI

A auditoria de SI é composta por uma Equipe de Auditoria (EA) designada previamente, cujo objetivo é verificar o fiel cumprimento das normas da SI, bem como estabelecer possíveis ações de correção e divulgação da mentalidade de SI.

14.2 - Tipos de Auditorias de SI

Os aspectos de SI podem ser verificados pelos seguintes tipos de auditoria:

a) Auditoria Inopinada: requerida pela Diretoria Executiva ou agente externo; e

b) Auditoria Normal: realizada periodicamente, no mínimo, uma por ano.

15 - INCIDENTES

Os incidentes que afetam a SI devem ser registrados conforme modelo constante no formulário Incidentes da Rede Local (Anexo IV). As ocorrências de incidentes que afetam os equipamentos críticos devem ser comunicadas ao GSI que levará o assunto à esfera da Diretoria Executiva, indicando procedimentos tomados ou a tomar e seu(s) respectivo(s) resultado (s).

16 - ANÁLISE DAS VULNERABILIDADES E RISCOS

A análise das vulnerabilidades e dos riscos tem por objetivo avaliar as possíveis ameaças à rede local. É necessário identificar os pontos onde a operação da rede local possa ser ameaçada ou posta em risco. A análise das vulnerabilidades e riscos deve ser realizada pelo GSI com base nos registros de Incidentes da Rede Local.

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

17 – ACESSO ÀS INFORMAÇÕES CONTIDAS NOS SERVIDORES

17.1 Servidor de Arquivos

O Servidor de Arquivos é acessado somente pela rede local e suas informações podem ser visualizadas através do drive G:.

Cada usuário poderá acessar as pastas do Servidor de Arquivos conforme estabelecido no Anexo V.

Para compartilhamento de arquivos entre usuários deverá ser utilizada a pasta "PÚBLICA".

A necessidade de acesso remoto ao servidor deverá ser comunicada ao GSI que poderá autorizar, desde que, tal acesso seja por meios seguros.

17.2 Servidor SAGI

O Servidor do SAGI pode ser acessado tanto pela rede local com o respectivo Login e Senha de acesso como remotamente através do *link* disponibilizado no site da Fundação.

O acesso do usuário aos Servidores citados somente será possível nos moldes do item 17.1.

18 – PROCEDIMENTOS DE *BACKUP*

Backup é uma cópia de segurança realizada em outro dispositivo de armazenamento, podendo este ser um HD externo, Nuvem, *Pendrive* ou *Storage*.

18.1 *Backup* dos Servidores de Arquivo e SAGI

O *backup* dos dados dos servidores é diário, ou seja, através de espelhamento, e em horário específico de forma automática no *storage,* que está posicionado em local distinto. O backup automático no *storage* é realizado, como segue:

Backup do Servidor de Arquivos - Todo dia às 21:00 é realizado um *backup* total das informações do Servidor de Arquivos em disco dedicado (*storage*); e

Backup do Servidor SAGI - Todo dia as 21:00 é realizado um *backup* total das informações do Servidor SAGI em disco dedicado (*storage*), como também, o período dos 30 dias mais recentes do banco de dados SAGI no drive C:.

19 – VIGÊNCIA

Esta Norma entra em vigor na presente data e revoga quaisquer disposições internas em contrário.

20 - DISTRIBUIÇÃO

Todos os elementos organizacionais.

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Anexo I – Modelo de Formulário de Solicitação de Recursos de Tecnologia da Informação

Pelo presente instrumento, eu, **(Nome completo, N° do CPF)**, perante a Fundação PATRIA, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, solicito o seguinte recurso de TI:

_____

_____

_____

Estou ciente da minha responsabilidade e pelas consequências decorrentes da utilização do recurso solicitado.

Iperó/SP, em _____ de _____ de _____

_____

Assinatura

Nome Completo, CPF

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Anexo II – Modelo de Termo de Responsabilidade Individual (TRI)

TERMO DE RESPONSABILIDADE INDIVIDUAL

Pelo presente instrumento, eu, **(Nome completo, N° do CPF)**, perante a Fundação PATRIA na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, **declaro estar ciente** das normas de segurança das informações digitais da organização, segundo as quais devo:

a) Tratar a informação digital como patrimônio da Fundação PATRIA e como um recurso que deva ter seu sigilo preservado, em consonância com a legislação vigente;

b) Utilizar as informações disponíveis e os sistemas e produtos computacionais, dos quais a Fundação PATRIA é proprietária ou possui o direito de uso, exclusivamente para o interesse do serviço;

c) Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas;

d) Não tentar obter acesso à informação que eu não tenha autorização ou necessidade de conhecer;

e) Não compartilhar o uso de senha com outros usuários;

f) Não me fazer passar por outro usuário usando a sua identificação de acesso e senha;

g) Não alterar o endereço de rede ou qualquer outro dado de identificação do microcomputador de meu uso;

h) Instalar e utilizar em meu microcomputador somente programas homologados para uso na Fundação PATRIA e que esta possua as respectivas licenças de uso ou, no caso de programas de domínio público, mediante autorização formal do GSI;

i) No caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o conteúdo das informações e documentos sigilosos a que tive acesso e não os divulga rpara pessoas não autorizadas;

j) Guardar segredo das minhas autenticações de acesso (senhas) utilizadas no ambiente computacional da Fundação, não cedendo, não transferindo, não divulgando e não permitindo o seu conhecimento por terceiros;

k) Não utilizar senha com sequência fácil ou obvia de caracteres que facilite a sua descoberta e não escrevera senha em lugares visíveis ou de fácil acesso;

l) Utilizar, ao me afastar momentaneamente da minha estação de trabalho, descanso de tela ("*screen saver*") protegido por senha, a fim de evitar que alguém possa ver as informações que estejam disponíveis na tela do computador;

m) Ao me ausentar do local de trabalho, momentaneamente ou ao término de minhas atividades diárias, certificar-me de que a sessão aberta no ambiente computacional com minha identificação foi fechada e as informações que exigem sigilo foram adequadamente salvaguardadas;

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

n) Seguir as orientações da área de informática da Fundação relativas à instalação, à manutenção e ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;

o) Comunicar imediatamente ao meu superior hierárquico e ao GSI a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de segurança estabelecidos;

p) Responder, perante a Fundação PATRIA, as auditorias e o GSI, por acessos, tentativas de acessos ou uso indevido da informação digital realizados com a minha identificação ou autenticação;

q) Não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;

r) Estar ciente de que toda informação digital armazenada e processada no ambiente computacional da Fundação PATRIA pode ser auditada, como no caso de páginas informativas ("sites") visitadas por mim;

s) Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

t) Não transferir qualquer tipo de arquivo que pertença à Fundação PATRIA para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização formal do superior hierárquico ou GSI;

u) Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da Fundação PATRIA;

v) Estar ciente de que a Fundação PATRIA poderá auditar os arquivos em trâmite ou armazenados nos equipamentos do ambiente computacional da organização sob meu uso ou responsabilidade;

w) Estar ciente de que o correio eletrônico e de uso exclusivo para o interesse do serviço e qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da Fundação PATRIA deve obedecer a este preceito;

x) Estar ciente de que a Fundação PATRIA poderá auditar as correspondências eletrônicas originadas ou retransmitidas por mim no ambiente computacional da organização; e

y) Estar ciente de que a utilização de jogos em dispositivos móveis, corporativo ou particular, e estações de trabalho é proibido em horário de expediente.

Desta forma, estou ciente da minha responsabilidade pelas consequências decorrentes da não observância do acima exposto e da legislação vigente.

Iperó/SP, em _____ de _____ de _____.

_____

Assinatura
Nome Completo, CPF

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Anexo III - Modelo de Termo de Recebimento de Estação De Trabalho (TRE)

TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO

Pelo presente instrumento, eu, **(Nome completo, N° do CPF)**, perante a Fundação PATRIA, na qualidade de usuário do ambiente computacional de propriedade da Fundação PATRIA, **declaro ter recebido** uma estação de trabalho com as seguintes configurações:

I. De identificação:

a) **Endereço Físico de Rede:** (especificar a identificação exclusiva da placa de rede da máquina);

c) **Identificação da máquina:** (especificar o nome e outros dados de identificação da máquina);

II. De instalação de programas:

a) Especificar todos os programas pré-instalados:

III. De senha de acesso à máquina ("boot"), inicialmente estabelecida pelo Administrador da Rede Local (ARL) e por mim alterada, sendo agora de meu conhecimento exclusivo; e

IV. De senha de configuração ("setup"), de conhecimento exclusivo do ARL e a qual não devo tomar conhecimento.

Assim, quaisquer alterações ou inclusões nos dados acima são de minha inteira responsabilidade e devem ser previamente autorizadas pelo Gerente de Segurança da Informação (GSI), conforme previsto nas Normas de Segurança da Informação e Comunicação da Fundação.

Estou ciente que o ARL (**executou / não executou)** a "formatação" previa dos discos rígidos da referida estação de trabalho e sua correspondente reconfiguração e que, a qualquer momento e sempre que julgar necessário, poderei solicitar ao ARL auxilio para a realização dessa "formatação", de modo a garantir a configuração padronizada da Fundação e a inexistência de arquivos ou programas irregulares.

Iperó/SP, em _____ de _____ de _____.

_____

Assinatura
Nome Completo, CPF

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Anexo IV – Modelo de Incidentes na Rede Local

HISTÓRICO DA REDE LOCAL

INCIDENTE NA REDE LOCAL No: _____ (*a ser preenchido pelo GSI*)

1 - Responsável pela informação do incidente: _____

Função: _____

2 - Data e hora do Incidente: _____ / _____ / _____ - _____ horas

Data e hora do relato: _____ / _____ / _____ - _____ horas

3 - Relato do incidente:

(Relatar detalhadamente o incidente, utilizando quantas linhas forem necessárias)

4 - Comentários, Análise sobre o Incidente e respectivas correções:

(Escrever detalhadamente, utilizando quantas linhas forem necessárias)

5 - Afetou algum Recurso Computacional Crítico? () sim () não

Data: _____/_____/_____

Assinatura do Responsável pela informação:_____

Assinatura do GSI: _____

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Anexo V – Acesso às Pastas do Servidor de Arquivos por Usuários

USUÁRIO REDE	PASTAS MACROS DE ACESSO VINCULADAS AO USUÁRIO REDE
PRESIDENCIA	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 300 - ÓRGÃOS GESTORES / 400 - ACORDOS ADMINISTRATIVOS / 600 - ADMINISTRAÇÃO / 800 - DIRETORIA FINANCEIRA / 900 - RELAÇÕES INSTITUCIONAISINSTITUCIONAIS / 1000 - PÚBLICA
GIRCI	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 300 - ÓRGÃOS GESTORES / 1000 - PÚBLICA
ASSESSJUR	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 300 - ÓRGÃOS GESTORES / 800 - DIRETORIA FINANCEIRA / 1000 - PÚBLICA
DIRTEC	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 300 - ÓRGÃOS GESTORES / 400 - ACORDOS ADMINISTRATIVOS / 600 - ADMINISTRAÇÃO / 900 - RELAÇÕES INSTITUCIONAIS / 1000 - PÚBLICA
GERPROJ	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 400 - ACORDOS ADMINISTRATIVOS / 1000 - PÚBLICA
SECPROJ	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 400 - ACORDOS ADMINISTRATIVOS / 1000 - PÚBLICA
DIRADM	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO /300 - ÓRGÃOS GESTORES / 400 - ACORDOS ADMINISTRATIVOS / 600 - ADMINISTRAÇÃO / 700 - SECRETARIA / 900 - RELAÇÕES INSTITUCIONAIS / 1000 - PÚBLICA
GERCORP	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 400 - ACORDOS ADMINISTRATIVOS / 600 - ADMINISTRAÇÃO / 700 - SECRETARIA / 1000 - PÚBLICA
SECOBT	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 400 - ACORDOS ADMINISTRATIVOS / 1000 - PÚBLICA
SECRH	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO /500 - RECURSOS HUMANOS / 1000 - PÚBLICA
SECAPOIO	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO /300 - ÓRGÃOS GESTORES / 600 - ADMINISTRAÇÃO / 700 - SECRETARIA / 900 - RELAÇÕES INSTITUCIONAIS / 1000 - PÚBLICA
DIRFIN	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO /300 - ÓRGÃOS GESTORES / 400 - ACORDOS ADMINISTRATIVOS / 600 - ADMINISTRAÇÃO / 700 - SECRETARIA /800 - DIRETORIA FINANCEIRA / 1000 - PÚBLICA
GERFIN	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 400 - ACORDOS ADMINISTRATIVOS / 700 - SECRETARIA /800 - DIRETORIA FINANCEIRA / 1000 - PÚBLICA
GERCONT	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 400 - ACORDOS ADMINISTRATIVOS / 800 - DIRETORIA FINANCEIRA / 1000 - PÚBLICA
SECFIN	100 - DOCUMENTOS INSTITUCIONAIS / 200 - LEGISLAÇÃO / 400 - ACORDOS ADMINISTRATIVOS / 700 - SECRETARIA /800 - DIRETORIA FINANCEIRA / 1000 - PÚBLICA

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

Relatório de Incidentes de Segurança Orgânica

FUNDAÇÃO PATRIA	
RELATÓRIO DE INCIDENTES DE SEGURANÇA ORGÂNICA	
INFORMAÇÕES DO FUNCIONÁRIO	
Nome:	
Direção/Gerência:	
DESCRIÇÃO DO INCIDENTE	
Data: Hora:	Polícia Notificada (Sim ou Não)?
DETALHES DO INCIDENTE	
CAUSAS DO INCIDENTE	
RECOMENDAÇÕES/SUGESTÕES	
ACOMPANHAMENTO DAS AÇÕES	

Este documento foi assinado digitalmente por Newton Calvoso Pinto Homem.
Para verificar as assinaturas vá ao site https://assinaturas.certisign.com.br:443 e utilize o código 7AC4-94D2-79F3-CB8F.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Certisign Assinaturas. Para verificar as assinaturas clique no link: https://assinaturas.certisign.com.br/Verificar/7AC4-94D2-79F3-CB8F ou vá até o site https://assinaturas.certisign.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 7AC4-94D2-79F3-CB8F

Hash do Documento

A19EDE17EFD08F44205B167156A5E71EC42151DF547F59062D00055ECDF51A64

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 09/12/2024 é(são) :

- Newton Calvoso Pinto Homem (Diretor-Presidente) - 758.618.607-34 em 09/12/2024 11:51 UTC-03:00
  Tipo: Certificado Digital