Universidade Federal do Oeste do Pará
Centro de Tecnologia da Informação e Comunicação
Coordenação de Segurança da Informação

# SEGURANÇA DA INFORMAÇÃO

## Guia do Usuário

Coordenação de
Segurança da Informação

CSI

UNIVERSIDADE FEDERAL DO OESTE DO PARÁ

**Universidade Federal do Oeste do Pará**
**Comitê Gestor de Segurança da Informação**
**Centro de Tecnologia da Informação e Comunicação**
**Coordenação de Segurança da Informação**

**Redação e Revisão:**
Caio Rego
Marcos Santos

**Projeto gráfico, diagramação e ilustração:**
Marcos Santos
Marcelo Oliveira

**Referências utilizadas para elaboração deste material:**

Site Certbr:
http://cartilha.cert.br/
Site: Ministério do Planejamento:
http://www.planejamento.gov.br/secretarias/upload/Arquivos/publicacao/cartilha_SIC.pdf

**Contato:**
csi.ctic@ufopa.edu.br

UNIVERSIDADE FEDERAL DO OESTE DO PARÁ

UNIVERSIDADE FEDERAL DO OESTE DO PARÁ

# MISSÃO

Promover a cultura da segurança da informação apoiando e desenvolvendo atividades alinhadas com as estratégias de negócio da instituição a partir de um monitoramento contínuo dos seus processos, métodos e ações.

# OBJETIVOS

Zelar pela segurança da informação em todos os formatos e em todos os meios que ela possa trafegar, baseando-se em três pilares:

- Integridade;
- Confidencialidade e Disponibilidade da informação.

## OBJETIVOS ESPECÍFICOS

- Conduzir o processo de criação e manutenção das políticas, diretrizes e normas de segurança da Informação da instituição;
- Monitorar o tráfego de informações em todos os meios disponíveis;
- Preservar a integridade de ambientes e equipamentos que armazenem algum tipo de informação relevante para a instituição;
- Promover treinamentos de Segurança da Informação;
- Orientar e conscientizar usuários sobre Segurança da informação;

# APRESENTAÇÃO

A informação tem se apresentado como um dos principais ativos das organizações. A segurança das informações deve ser tratada de acordo com sua relevância para a continuidade das atividades da instituição. Isto compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada.

As medidas tomadas para garantir a segurança da informação não se aplicam somente aos arquivos armazenados em computadores mas também os documentos impressos em papel, armazenados em mídias removíveis (pendrives, CDs, DVDs, Hds externos), assim como, o transporte de informações seja em meios físicos ou através da rede.

A participação dos usuários é importante no processo da segurança, pois é na adequada utilização dos recursos de Tecnologia da Informação, como instrumento de trabalho, que se inicia a formação de uma sólida cultura de segurança da informação. Com este objetivo, esta cartilha vem auxiliar os usuários com informações, recomendações e dicas sobre como usuário deve se comportar para aumentar a sua segurança e se proteger de possíveis riscos e ameaças.

UNIVERSIDADE FEDERAL DO OESTE DO PARÁ

UNIVERSIDADE FEDERAL DO OESTE DO PARÁ

# SUMÁRIO





# 1. SEGURANÇA DA INFORMAÇÃO

**O que é?**

No Brasil, a norma ABNT NBR ISO/IEC 27002:2007 define a Segurança da Informação como:

"É a proteção contra de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio."

**O que é Informação?**

É todo conteúdo, seja ele impresso, em forma digital, ou mesmo, em mente de interesse de uma instituição ou pessoa. A informação é o ativo mais valioso de uma organização.

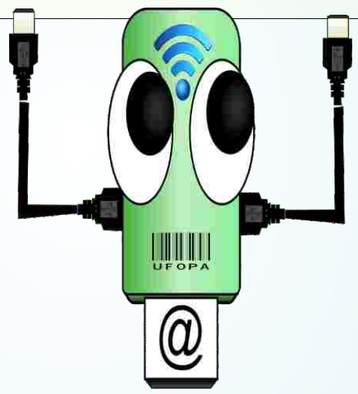
**O que é ativo?**

É tudo aquilo que tem valor para a instituição, seja tangível ou inagitável e tem que ser protegido por aqueles que fazem parte da organização.

UNIVERSIDADE FEDERAL DO OESTE DO PARÁ

## 2. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação possuí alguns princípios básicos. Conheça a CIDA...








# 2.1 CIDA

**Qual o objetivo da segurança da informação?**

A segurança da informação visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização. Conheça o significado da sigla CIDA.

CONFIDENCIALIDADE: é garantia de que somente pessoas autorizadas receberam determinada informação;

INTEGRIDADE: é garantia de que a informação não sofrerá alterações em seu conteúdo, tornando-se integra;

DISPONIBILIDADE: é garantia de que a informação estará acessível sempre que você precisar dela; e

AUTENTICIDADE: é garantia de que aquela informação é verdadeira e garante que as pessoas envolvidas são elas mesmas.

# 3. SEGURANÇA NA INTERNET

Cada vez mais nossas atividades estão diretamente ligadas ao uso do computador e principalmente da rede mundial de computadores, a internet. A presença constante dos usuários conectados exige uma certa cautela na utilização de tantos recursos que a internet disponibiliza .

Um dos principais perigos da internet é a proliferação de vírus que podem corromper ou apagar arquivos, provocar lentidão causando grandes transtornos aos usuários e aos gerentes da rede.

Além dos vírus, a utilização de comércio eletrônico se tornou um atrativo para os criminosos. Cuidados devem ser tomados na utilização de cartões de créditos e senha pela internet. Nesta seção apresentaremos os principais golpes aplicados na Internet, os riscos que estes golpes representam e os cuidados que devem ser tomados para se proteger deles.





## 3.1 USO SEGURO DA INTERNET

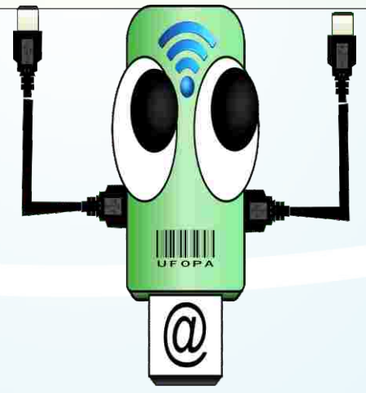
Cada vez mais os golpistas da internet concentram seus esforços na exploração de fragilidades dos usuários. Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

- Existem vários tipos de fraudes cibernéticas, algumas das mais conhecidas são:
- Fraude de antecipação de recursos (Advance fee fraud);
- Phishing;
- Pharming; e
- Golpe do site de comércio eletrônico fraudulento.

É importante conhecer cada uma delas para não cair nos golpes virtuais.

# 3.2 ENGENHARIA SOCIAL

Engenharia social é termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.








## 3.2.1 GOLPES

### Fraude de antecipação de recursos (Advance fee fraud)

A fraude de antecipação de recursos, ou advance fee fraud, e aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

### Phishing

Phishing é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

**Pharming**

Pharming é um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando tenta acessar um site legítimo, o seu navegador Web e redirecionado, de forma transparente, para e uma página falsa.

**Golpe do site de comércio eletrônico fraudulento**

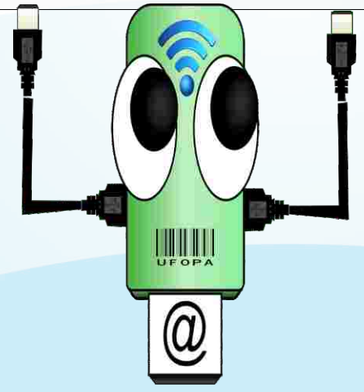
Neste golpe, o golpista cria um site fraudulento, com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias. Para aumentar as chances de sucesso, o golpista costuma utilizar artifícios como: enviar spam, fazer propaganda via links patrocinados, anunciar descontos em sites de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado.





# 4 SOFTWARES MALICIOSOS

Os Softwares Maliciosos ou Vírus de computador são pequenos programas capazes de causar grandes transtornos a indivíduos, empresas e outras instituições, afinal, podem apagar dados, capturar informações, alterar ou impedir o funcionamento do sistema operacional e assim por diante. Como se não bastasse, há ainda outros softwares parecidos, como cavalos de troia, worms, hijackers, spywares e ransomwares.



## 4.1 TIPOS DE SOFTWARES MALICIOSOS

### Malware

- Malware é a abreviação de malicious software (software malicioso); um termo abrangente que se refere a qualquer programa de software intencionalmente criado para executar uma ação não autorizada e muitas vezes prejudicial. Vírus, backdoors, keyloggers, ladrões desenhas e outros cavalos de Troia, vírus de macro do Word e do Excel, vírus do setor de inicialização, vírus de script (em lote, windows shell, java, etc.) e cavalos de Troia, crimeware, spyware e adware são alguns exemplos do que é considerado malware. Antigamente, podíamos falar em 'vírus' ou em 'cavalo de Troia', mas os vetores e métodos de infecção evoluíram de tal forma que esses termos não são mais suficientes para definir todos os tipos de programas anômalo existentes.

### Vírus

- Um vírus é um programa que se replica, ou seja, ele se dissemina de um arquivo para outro em seu sistema e de um computador para outro. Além disso, ele pode ser programado para apagar ou danificar dados. Em geral, os worms são considerados como um subconjunto dos vírus, mas com algumas diferenças importantes.





### Worm

- Um worm é um programa de computador que se replica, mas não infecta outros arquivos. Em vez disso, ele se instala em um computador e procura formas de se disseminar para outros computadores.

- No caso dos vírus, quanto mais tempo ele passar desapercebido, mais arquivos infectados haverá no computador. Os worms, por outro lado, criam uma única instância de seu código. Além disso, diferentemente dos vírus, o código dos worms é autônomo. Em outras palavras, um worm é um arquivo independente, enquanto um vírus é um conjunto de código que se adiciona a arquivos existentes.

### Keylogger

- São programas que registram os pressionamentos do teclado (ou seja, aquilo que o usuário digita no teclado), que podem ser usados por um hacker para obter dados confidenciais (detalhes de login, senhas, números de cartão de crédito, PINs, etc.). Normalmente, os cavalos de Troia do tipo Backdoor têm um keylogger integrado.

### Adware

- Adware é o termo geral aplicado a programas que abrem anúncios publicitários (frequentemente banners pop-up) ou redirecionam os resultados de pesquisas para sites promocionais. Muitas vezes, os adwares estão incorporados em programas freeware ou shareware: se você baixar um programa freeware, o adware é instalado no sistema sem seu conhecimento ou consentimento. Às vezes, um cavalo de Troia baixa um programa adware de um site e o instala em seu computador de maneira oculta.

Normalmente, os programas adware não são exibidos no sistema: eles não estão listados em Iniciar Programas, não há ícones na bandeja do sistema, nem na lista de tarefas. Raramente eles têm um procedimento de desinstalação e as tentativas de removê-los manualmente podem causar o funcionamento incorreto do programa original.

## Cavalos de Troia (Trojan Horse)

- Atualmente, os cavalos de Troia são instalados de maneira oculta e executam sua carga maliciosa sem o conhecimento do usuário. Grande parte do crimeware de hoje compreende diferentes tipos de cavalos de Troia, todos criados intencionalmente com uma função maliciosa. Os mais comuns são os cavalos de Troia dos tipos Backdoor (que Frequentemente incluem Um keylogger), espiões, ladrões de senhas e cavalos de Troia de proxy, que convertem o computador em uma máquina de distribuição de spam.

## Spyware

- Como o nome sugere, são softwares criados para coletar seus dados e encaminhá-los para terceiros sem o seu consentimento ou conhecimento.

Esses programas podem monitorar o pressionamento do teclado ('keyloggers'), coletar informações confidenciais (senhas, números de cartões de crédito, PINs, etc.), coletar endereços de e-mail ou rastrear comportamentos de navegação. Além de tudo isso, inevitavelmente os spywares afetam o desempenho do computador.





**Você Sabia?**

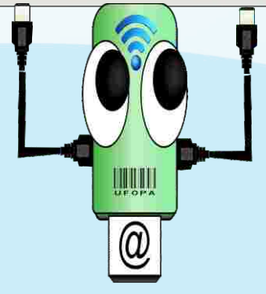
O termo cavalo de Troia refere-se ao cavalo de madeira usado pelos gregos para se infiltrar na cidade de Troia e capturá-la. A definição clássica de cavalo de Troia é um programa que representa um software legítimo mas que, quando executado, realiza algo prejudicial.


## Antivírus

- Os antivírus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus de computador. Existem diversos produtos com esse intuito no mercado, a diferença entre eles é utilizar um antivírus gratuito ou um pago. A diferença está nas camadas a mais de proteção que a versão paga oferece, além do suporte técnico realizado pela equipe especializada.

Apesar de ser uma ferramenta importante para a segurança do seu computador, a presença do antivírus não garante 100% de segurança. Portanto, a presença de um antivírus não dá liberdade total de fazer o que bem entender.

**A presença de um antivírus dá 100% de proteção ?**



# 5 USO DO E-MAIL

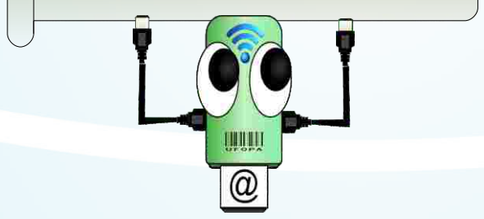
O Email é uma ferramenta fundamental para a comunicação institucional. Um meio rápido e simples de transmitir mensagens. Porém, toda esta facilidade também pode implicar em riscos para o usuário.

Através de links, anexos ou spam o e-mail pode disseminar vírus ou simplesmente causar transtornos ao usuário. Fique sempre atento a mensagens de quem você desconhece e não clique em links ou anexos duvidosos.

## SPAM

- Spam é o termo usado para se referir aos emails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial Email).

Confira algumas dicas sobre o uso de Email.








# 5.1 E-MAIL INSTITUCIONAL

- Informações de interesse da instituição devem trafegar prioritariamente por contas de email institucionais;

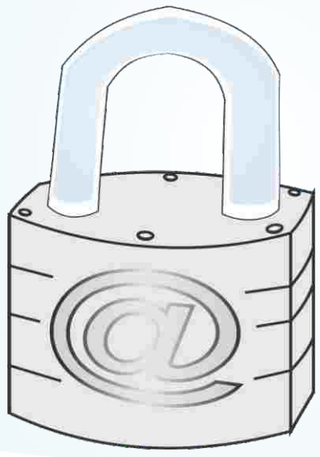
- Evite utilizar emails pessoais para se comunicar no ambiente de trabalho. Setores devem utilizar obrigatoriamente contas de email com domínio ufopa.edu.br;

- A utilização de email também exige atenção dos usuários e a troca de mensagens nas contas de e-mail institucional requerem cuidados redobrados;

- Da mesma forma o usuário deve zelar por sua privacidade e evitar exposições excessivas em redes sociais. Aproveite estas dicas para uma navegação mais segura.

# 6 PRIVACIDADE

▪ A internet mudou a forma como nos comunicamos. A quantidade de informações e a velocidade com que elas se propagam na rede é impressionante. A presença dos usuários na rede e o tempo que passam conectados cresce a cada dia principalmente devido aos sites de relacionamentos ou redes sociais.



▪ Seja cuidadoso ao se associar a comunidades e grupos, pois por meio deles muitas vezes é possível deduzir informações pessoais, como hábitos, rotina e classe social;

▪ Considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa, tanto agora como futuramente;

▪ Pense bem antes de divulgar algo, pois não há possibilidade de arrependimento. Uma frase ou imagem fora de contexto pode ser mal interpretada e causar mal entendidos. Após uma informação ou imagem se propagar, dificilmente ela poderá ser totalmente excluída;

## 6.1 DICAS DE PRIVACIDADE

▪ Use as opções de privacidade oferecidas pelos sites e procure ser o mais restritivo possível (algumas opções costumam vir, por padrão, configuradas como públicas e devem ser alteradas);

▪ Mantenha seu perfil e seus dados privados, permitindo o acesso somente a pessoas ou grupos específicos;

▪ Procure restringir quem pode ter acesso ao seu endereço de email, pois muitos spammers utilizam esses dados para alimentar listas de envio de spam;

▪ Seja seletivo ao aceitar seus contatos, pois quanto maior for a sua rede, maior será o número de pessoas com acesso às suas informações. Aceite convites de pessoas que você realmente conheça e para quem contaria as informações que costuma divulgar;

▪ Não acredite em tudo que você lê. Nunca repasse mensagens que possam gerar pânico ou afetar outras pessoas, sem antes verificar a veracidade da informação.



UNIVERSIDADE FEDERAL DO OESTE DO PARÁ

# 7. CONTAS DE USUÁRIO

A sua conta de usuário é de conhecimento geral e é o que permite a sua identificação nos sistemas da instituição. Na UFOPA ela é formada na forma "**primeironome.últimonome**" e através dela você terá acesso a todos os sistemas da instituição, acesso a internet em redes sem fio e acesso a computadores. Para garantir que ela seja usada apenas por você, e por mais ninguém, é que existem os mecanismos de autenticação.

- Para manter sua conta em segurança é importante que sua senha não seja compartilhada com ninguém. Também é preciso alguns cuidados na hora de escolher a sua senha.
- Não use senhas óbvias que possam ser adivinhadas facilmente, como o nome de seu cônjuge, seus filhos, seu animal de estimação, a placa do carro ou o CEP, etc (Ver mais na Seção Criando senhas seguras).
- Não informe sua senha a ninguém. Se uma organização entrar em contato com você pedindo sua senha, mesmo por telefone, não forneça nenhuma informação pessoal. Lembrese, você não sabe quem está do outro lado da linha.





## 7.1 SENHAS

- Se uma loja virtual ou qualquer site enviar uma confirmação por email que contém uma nova senha, efetue login novamente e altere a senha imediatamente.
- Verifique se o seu software de segurança de Internet bloqueia as tentativas de criminosos virtuais de interceptar ou roubar senhas.
- Para manter sua conta em segurança é importante que sua senha não seja compartilhada com ninguém. Também é preciso alguns cuidados na hora de escolher a sua senha.

- Não use senhas óbvias que possam ser adivinhadas facilmente, como o nome de seu cônjuge, seus filhos, seu animal de estimação, a placa do carro ou o CEP, etc (Ver mais na Seção Criando senhas seguras).
- Não informe sua senha a ninguém. Se uma organização entrar em contato com você pedindo sua senha, mesmo por telefone, não forneça nenhuma informação pessoal. Lembre-se, você não sabe quem está do outro lado da linha.

## 7.2 CRIANDO SENHAS SEGURAS

As senhas são sua principal segurança no uso de emails e outros serviços disponíveis na rede da UFOPA ou na internet. O primeiro passo para sua segurança está na criação de uma boa senha. Uma senha bem elaborada é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

Ao escolher as senhas:

- Especifique senhas fáceis de memorizar;
- Mantenha-as em segredo;
- Não seja enganado para revelá-las a organizações aparentemente legítimas;
- Misture letras minúsculas e maiúsculas, números e caracteres não alfanuméricos;
- Não use a mesma senha para várias contas;
- Não recicle senhas ('senha1', 'senha2', etc.).

Alguns elementos que você não deve usar na elaboração de suas senhas são:

- Qualquer tipo de dado pessoal: evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carro, números de telefones e datas (estes dados podem ser facilmente obtidos e usados por pessoas que queiram tentar se autenticar como você).

- Sequências de teclado: evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG", pois são bastante conhecidas e podem ser facilmente observadas ao serem digitadas.

- Palavras que façam parte de listas: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas.

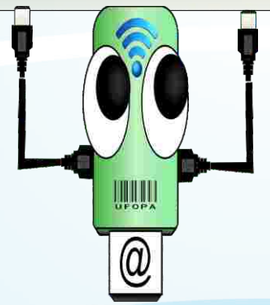




# 8 SEGURANÇA DOS RECUROS DE TI

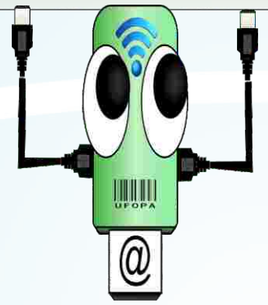
A responsabilidade pela segurança dos recursos de T.I disponibilizados pela UFOPA tem uma parcela significativa dos usuário. Isso porque o parque computacional da instituição é grande e de difícil manutenção. Diariamente ocorrem situações que podem prejudicar computadores, monitores, impressoras e outros equipamentos que auxiliam os servidores em suas atividades. A manipulação destes recursos pelo usuário requer alguns cuidados para prevenir danos a informação.

Para ajudá-lo a entender um pouco sobre as políticas de uso dos computadores observe as perguntas a seguir:



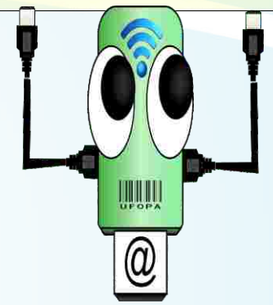
- São medidas que visam melhorar a vida útil dos equipamentos computacionais da instituição preservando e protegendo as informações contidas no computador, assim como, o acesso indevido aos recursos do sistema operacional.

O que é a política de uso dos computadores?

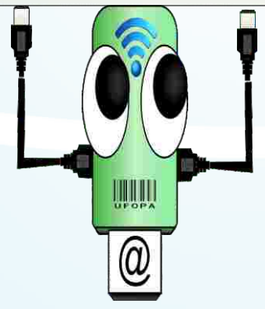


- Quaisquer equipamentos, programas, meios físicos de tráfego e sistemas de armazenamento digital inseridos no ambiente computacional da instituição, incluindo notebooks, pendrives, HD externos, impressoras, além das estações de trabalho.

Quais os recursos computacionais que devem seguir as políticas de uso?



O que pode ser ligado ao No-Break?



- O No-break, assim como o estabilizador, são equipamentos que procuram proteger outros equipamentos de oscilações de energia. Estes equipamentos possuem uma limitação e devem ser usados exclusivamente para o computador e monitor. Não devem ser ligados no No-break ou estabilizador: Ventiladores, Bebedouros, Cafeteiras, Impressoras.

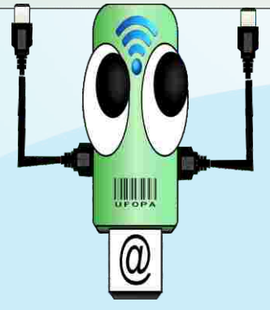




- A política de tela limpa define um bloqueio automático do computador quando um usuário se ausentar do mesmo por um determinado tempo configurado. Isto evita o acesso indevido ao computador por pessoas não autorizadas durante a ausência do servidor. A política de mesa limpa define que documentos e carimbos não devem ser mantidos na mesa do usuário ao fim do expediente ou em caso de ausência prolongada.

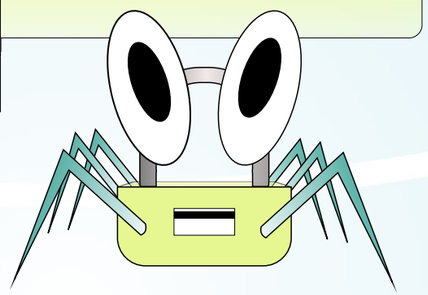
O que são as políticas de Tela Limpa e Mesa Limpa?

Quais os programas disponíveis para instalação?



- Somente técnicos do CTIC/Suporte possuem privilégios de administrador nos computadores da instituição. Esta medida é necessária por questões de segurança.

Quem pode ter privilégios de Administrador nos Computadores?



- O suporte disponibiliza uma lista de aplicativos padrão para instalação em Sistemas Operacionais Windows. Além destes existem aplicativos opcionais para cada categoria de acordo com a necessidade do usuário.


- Os técnicos do Suporte estão autorizados a instalar quaisquer programas para atender a necessidade dos usuários desde que estes sejam licenciados ou gratuitos. Não são permitidos em hipótese alguma a instalação de Softwares sem licença de uso ou que apresentem algum risco ao computador ou ao funcionamento da rede da instituição.

- Atualmente a UFOPA possui computadores com licenças para o Sistema Operacional Windows XP, Windows Vista e Windows 7, sendo estas licenças atribuídas a um único equipamento o qual deverá apresentar a etiqueta com a chave do produto no gabinete do Computador. Caso o usuário opte pela utilização do Sistema Operacional Linux poderá solicitar junto ao suporte através de Memorando ou via GLPI.






## 9 AÇÕES DESENVOLVIDAS PELA UFOPA PARA GARANTIR A SEGURANÇA DAS INFORMAÇÕES E COMUNICAÇÕES

Conforme determinação do Gabinete de Segurança Institucional da Presidência da República GSI/PR, a Universidade Federal do Oeste do Pará, por meio da Portaria Nº 461, de 26 de fevereiro de 2014, resolve instituir o Comitê Gestor de Segurança da Informação.

Entre suas principais atribuições estão:

I- Propor normas e procedimentos relativos a segurança da informação e comunicações;

II- Assessorar na implantação das ações de segurança da informação e comunicações; e

III- Sugerir a criação do grupo de trabalho para tratar dos temas e propor soluções específicas sobre segurança da informação e comunicações.

- **Coordenação de Segurança da Informação**

É responsável por promover a cultura da segurança da informação apoiando e desenvolvendo atividades alinhadas com as estratégias de negócio da instituição a partir de um monitoramento contínuo dos seus processos, métodos e ações.

- **Elaboração da Política de Segurança da Informação e Comunicações (POSIC)**

Documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

- **Apoio a criação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**

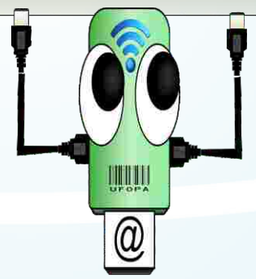
Constituído por servidores do Centro de Tecnologia da Informação e Comunicação- CTIC, a ETIR é um grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores dentro da instituição.

## 10 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Ao receber email de origem ou conteúdo duvidoso você pode solicitar orientações junto a coordenação de Segurança da Informação.

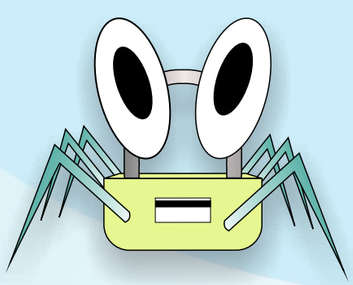
Quaisquer incidentes de segurança da informação devem ser registrados pelo usuário através do sistema de abertura de chamados de suporte ou através do envio de um email para a coordenação de segurança da informação.

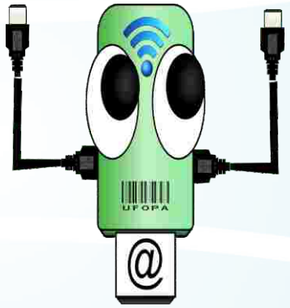
Contatos
Email: csi.ctic@ufopa.edu.br
Abertura de chamados: suporte.ufopa.edu.br

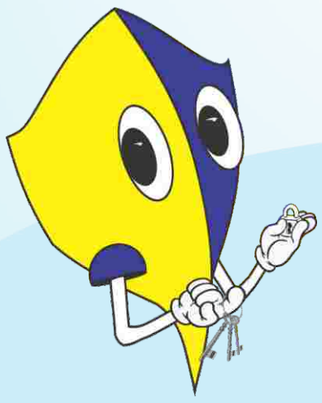








**UNIVERSIDADE FEDERAL DO OESTE DO PARÁ**

Esta cartilha foi desenvolvida no intuito de orientar o servidor a cerca das boas práticas do uso das tecnologias, as ameaças que cercam a tecnologia da informação e os cuidados a serem tomados para proteger os recursos da informação, tanto pessoal como institucional.

**Coordenação de Segurança da Informação**

**CSI**