

GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO

DOCUMENTAÇÃO



1 INTRODUÇÃO

1.1 Descrição

O SGI é um sistema que permite que colaboradores de uma empresa notifiquem casos de incidentes de TI. Desta forma, medidas apropriadas podem ser tomadas a tempo no sentido de se evitar que ativos de informação da empresa corram riscos ou sejam comprometidos. O sistema possibilita o registro e controle, em tempo real, das notificações de incidentes abertos e das resoluções e providências tomadas pela equipe de TI da empresa.

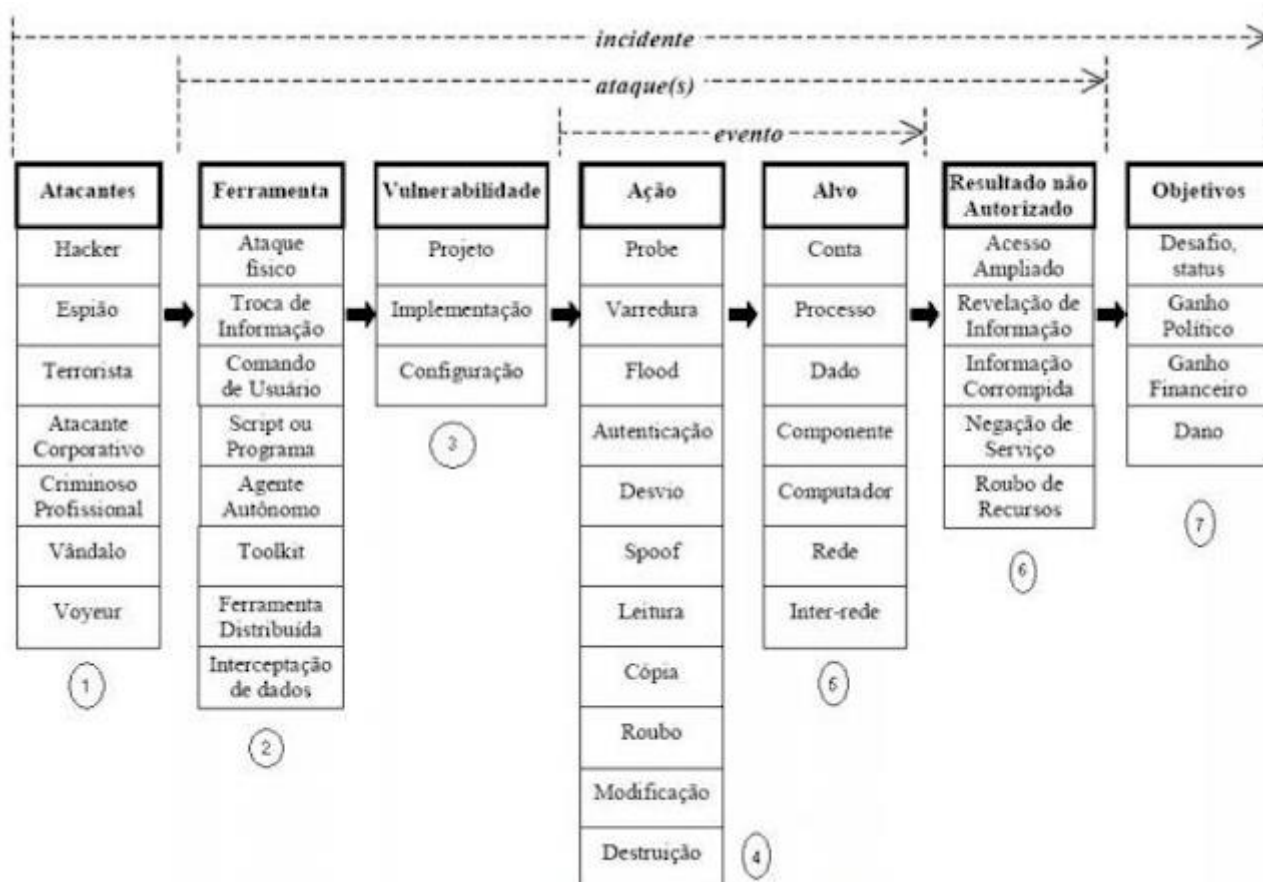
Tecnologias empregadas

- **Linguagem:** Sistema desenvolvido com PHP (versão 7.1.3) orientado a objetos
- **Framework PHP:** Laravel versão 5.8
- **Arquitetura da aplicação:** Padrão MVC (Model-View-Controller).
- **Construção de Formulários:** Utiliza o pacote Laravel Collective versão 5.8.0
- **WYSIWYG HTML editor:** Utiliza o CKEditor 4 para edição de campos textarea.
- **Controle de roles e permissions:** Utiliza o pacote Shinobi versão 4.0
- **Design visual:** Utiliza o framework Bootstrap 4.0. É responsivo.
- **Ícones:** Utiliza o framework Font Awesome Icons

Autor: Roberto Pinheiro

1.2 Gerenciamento de Incidentes de Segurança da Informação

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de Redes de Computadores. Em geral, qualquer situação em que um ou mais ativos da informação está(ão) sob risco, é considerado um incidente de segurança. O propósito do processo de gerenciamento de incidentes é garantir que os incidentes e as fraquezas que são relacionadas aos sistemas de informação sejam conhecidos para que as medidas apropriadas sejam tomadas a tempo. Os funcionários, pessoal temporário e usuários externos, todos devem estar cientes dos procedimentos para relatar os vários tipos de incidentes e falhas que podem ter uma influência sobre a confiabilidade da informação e da segurança dos ativos de negócios.



1.3 Concepção de um incidente e suas estruturas

Deve-se exigir dos funcionários e outros usuários a notificação de todos os incidentes e falhas o mais rapidamente possível pois é do interesse de todos que a organização responda com uma solução rapidamente.

Duas questões são de grande importância e que devem ficar claro à administração:

1. **Relatórios de incidentes de segurança** são usados como uma forma de aprender com eles a fim de evitar que incidentes semelhantes ocorram novamente;

2. A **notificação de incidente** não deve ser utilizada como uma forma de punir o autor do incidente. No entanto, isso não significa que não possa acontecer. Se um funcionário intencionalmente armar uma sabotagem e danificar os dados de um sistema, ou causar o vazamento de informações confidenciais, pode ser severamente punido.

É importante que as pessoas não tenham medo de reportar um incidente ao gestor e muito menos, medo de serem vistos como acusadores injustos. O processo também deve garantir que a pessoa que relatou um incidente de segurança da informação seja informada dos resultados após o seu tratamento. Os relatórios de incidentes também são úteis quando se efetua uma análise de risco, já que as medidas tomadas até então, talvez não sejam suficientes para evitar novos incidentes. O uso de um formulário localizado na intranet para relatar tais incidentes é importante não apenas para dar instruções sobre respostas imediatas diante de um incidente, mas também para coletar detalhes relativos ao incidente.

1.4 Importância da notificação de incidentes de segurança

Parte indispensável do processo de tratamento de incidentes, a notificação é uma atividade de grande importância visto que:

- **Melhora a capacidade de detecção de incidentes.** Muitas instituições descobrem que estão comprometidas apenas quando são notificadas por colaboradores ou por terceiros. Notificar incidentes pode ajudar a identificar problemas e prevenir novas ocorrências;
- **Contribui para a segurança geral da Internet.** Ao notificar uma tentativa de ataque da qual foi vítima, ao invés de apenas mitigá-la, busca-se a solução do problema e demonstra-se comprometimento com questões de segurança;
- **Pode ajudar a conter danos e prejuízos.** Notificações podem ser instrumentos eficazes na mitigação de incidentes e na contenção dos prejuízos, como por exemplo, em casos de fraudes;
- **Permite gerar estatísticas, correlacionar dados e identificar tendências** que ajudarão a elaborar recomendações e materiais de apoio, a orientar campanhas pela adoção de boas práticas e a estabelecer ações em cooperação.

1.5 O que notificar

Devem ser notificados eventos adversos relacionados à segurança dos sistemas de computação ou das redes de computadores, em desrespeito à política de segurança ou à política de uso aceitável da organização, como por exemplo:

- tentativas, com ou sem sucesso, de ganhar acesso não autorizado a um sistema ou a seus dados (ex: varreduras, ataques de força bruta SSH);
- interrupção indesejada de serviço (ex: ataque de negação de serviço);

- uso não autorizado de um sistema (ex: site comprometido hospedando páginas de phishing, propagando malware ou infectado com bot para ataque a terceiros/envio de spam);
- modificações em um sistema sem o conhecimento ou consentimento prévio de seu dono (ex: desfiguração de página);
- sistemas desatualizados ou incorretamente configurados, permitindo abuso (ex: DNS recursivo aberto, NTP permitindo amplificação);
- uso abusivo, em desrespeito à política de uso aceitável do provedor de serviço (ex: contratação de sistema em nuvem para uso malicioso).

1.6 Página Inicial

- Para se logar no sistema, acesse <http://app-incidentes.herokuapp.com> e clique no link "Login", na parte superior direita da tela.

Home Manual Sobre
Login Cadastrar



- SISTEMA DE GERENCIAMENTO DE INCIDENTES DE TI

O SGI é um sistema de gerenciamento de incidentes de TI. Permite o registro de notificações de incidentes por parte dos colaboradores da empresa e o registro das ações corretivas por parte da equipe de TI. Responder rapidamente e de forma adequada a um incidente pode evitar que ativos de informação da empresa corram riscos ou sejam comprometidos. Leia o Manual para saber como o sistema funciona. Cadastre-se e tenha acesso GRATUITO como visitante.









OrionTecInfo - By: Roberto Pinheiro - Copyright © 2021 - Todos os direitos reservados.

1.7 Cadastrando-se como visitante

- Você pode acessar o sistema como [visitante](#). Para isso, no menu superior, clique na opção "[Cadastrar](#)". Na tela que se abrirá, entre com seu nome, email e uma senha de pelo menos 8 caracteres:

CADASTRO



Name

Regina Alves Santos

E-Mail Address

regina_alves_santos@gmail.com

Password

Confirm Password

Cadastrar

- Em seguida, clique no botão "[Cadastrar](#)". Se tudo estiver ok, o cadastro será realizado e automaticamente você será redirecionado para o seu Painel de Controle. Para sair, com segurança, realize o [Logout](#).


1.8 Tela de Login

- Depois de cadastrado, nas próximas vezes que desejar acessar o sistema, clique na opção "[Login](#)" do menu superior. Será aberta a tela de Login. Entre com as informações solicitadas e clique no botão "[Acessar](#)".

Home Manual Sobre

Login Cadastrar

LOGIN



E-Mail Address

Password

Acessar

OrionTecInfo - By: Roberto Pinheiro - Copyright © 2021 - Todos os direitos reservados.

1.9 Acessando o sistema

- Ao realizar o login, você será redirecionado para a página home e no menu superior serão exibidas as opções disponíveis conforme suas permissões (definidas no grupo de usuários do qual você faz parte).



1.10 Base de testes

- Para que o usuário possa conhecer e testar as funcionalidades do sistema é necessário que as tabelas de dados estejam populadas. No sistema são inseridos e exibidos, parcialmente ou integralmente, de acordo com os privilégios do usuário, os seguintes dados:

- 20 usuários;
- 9 grupos de usuários;
- 42 permissões de usuários;
- 16 notificações de incidentes;
- 11 categorias de ataques e ameaças;
- 53 tipos de ameaças e ataques;

2 GRUPOS DE USUÁRIOS

Um grupo de usuários é uma coleção de contas de usuários. A principal função dos grupos de usuários é facilitar a administração e a atribuição de permissões para acesso a recursos ou funcionalidades de um sistema. Uma vez atribuída as permissões ao grupo, todos os membros do grupo, irão herdar estas permissões. Por exemplo, podemos criar um grupo chamado *Colaboradores*, do qual farão parte todos os colaboradores (funcionários) da empresa. Dessa forma, ao invés de darmos permissões individualmente, para cada um dos colaboradores, podemos atribuir permissões para o grupo. Se, por exemplo, um *Colaborador* for designado para também administrar os usuários do sistema, basta também adicioná-lo ao grupo de *Administrador de usuários*. Dessa forma, o usuário terá tanto as permissões do grupo *Colaboradores* como as permissões do grupo *Administrador de usuários*. A utilização de grupos pode facilitar a atribuição e a administração de permissões concedidas aos usuários.

O sistema permite que os administradores (do sistema ou de grupos de usuários) criem e gerenciem grupos de usuários definindo as permissões de cada grupo. Permissões estão relacionadas às funcionalidades disponíveis, seja através do menu principal, de um submenu ou de um botão que cada usuário terá ao acessar o sistema. Os administradores também podem renomear ou excluir grupos, bem como modificar as permissões atribuídas a cada um deles. Também podem listar os usuários de cada grupo. Um usuário pode pertencer a um ou mais grupos de usuários.

Os grupos **padrões** do sistema são os seguintes:

Grupo	Descrição
Administrador do sistema	Gerencia incidentes, categorias e tipos de ameaças, usuários e grupos de usuários
Administradores de usuários	Gerencia usuários
Administradores de grupos de usuários	Gerencia grupos de usuários
Analistas de segurança da informação 1	Atende notificações de incidentes
Analistas de segurança da informação 2	Gerencia as categorias e tipos de ameaças e ataques
Colaboradores	Funcionários da empresa
Convidados	Usuários convidados para conhecer o sistema
Visitantes	Visitante registrado no sistema
Suspensos	Funcionários desligados da empresa, usuários suspensos

Observações:

- Um usuário pode pertencer a um ou mais grupos.
- Grupos podem ser adicionados, excluídos ou modificados, de acordo com os interesses de cada empresa.

Permissões

As permissões do sistema que podem ser aplicadas ou não a cada um dos grupos de usuários são as seguintes:





































- Listagem de usuários (Lista todos os usuários do sistema)
- Exibição de detalhes de um usuário (Exibe detalhes de um usuário do sistema)
- Cadastro de um usuário (Cadastra um usuário no sistema)
- Edição de usuários (Edita dados de um usuário do sistema)
- Exclusão de usuário (Exclui um usuário do sistema)
- Alteração de senha de usuário (Altera a senha do usuário)
- Listagem usuários x grupo de usuários (Lista usuários vinculados a um grupo de usuários)
- Listagem de usuários por ordem alfabética de nomes (Lista usuários em ordem alfabética crescente de nomes)
- Listagem de grupos de usuários (Lista os grupos de usuários do sistema)
- Exibição de detalhes de um grupo de usuários (Exibe detalhes de um grupo de usuário do sistema)
- Criação de um grupo de usuários (Cria um grupo de usuários)
- Edição de um grupo de usuários (Edita dados de um grupo de usuários)
- Exclusão de um grupo de usuários (Exclui um grupo de usuários do sistema)
- Listagem de notificações de incidentes (Lista notificações de incidentes)
- Exibição de detalhes de uma notificação de incidente (Exibe detalhes de uma notificação de incidente)
- Criação de notificação de incidente (Cria uma notificação de incidente)
- Edição de notificação de incidente (Edita uma notificação de incidente)
- Exclusão de notificação de incidente (Exclui uma notificação de incidente)
- Listagem de notificações de incidentes por usuário (Exibe notificações de incidentes por usuário)
- Listagem de notificações de incidentes abertas (Exibe notificações de incidentes abertas)
- Listagem de tipos de ameaças ou ataques (Lista tipos de ameaças ou ataques)
- Exibição de detalhes de um tipo de ameaça ou ataque (Exibe detalhes de um tipo de ameaça ou ataque)
- Cadastro de tipo de ameaça ou ataque (Cadastra um tipo de ameaça ou ataque)
- Edição de tipo de ameaça ou ataque (Edita um tipo de ameaça ou ataque)
- Exclusão de tipo de ameaça ou ataque (Exclui um tipo de ameaça ou ataque)
- Listagem de ameaças em ordem crescente de nomes (Lista ameaças em ordem alfabética crescente de nomes)
- Listagem de ameaças em ordem decrescente de nomes (Lista ameaças em ordem alfabética decrescente de nomes)
- Listagem de ameaças em ordem decrescente de id (Lista ameaças em ordem decrescente de id)
- Listagem de categorias de ameaças ou ataques (Lista categorias de ameaças ou ataques)
- Exibição de detalhes de uma categoria de ameaças ou ataques (Exibe detalhes de uma categoria de ameaças ou ataques)
- Cadastro de categoria de ameaça ou ataque (Cadastra uma categoria de ameaça ou ataque)

- Edição de categoria de ameaça ou ataque (Edita uma categoria de ameaça ou ataque)
- Exclusão de categoria de ameaça ou ataque (Exclui uma categoria de ameaça ou ataque)
- Listagem de ameaças por categoria (Lista as ameaças de uma determinada categoria)
- Listagem de categorias de ameaças em ordem alfabética de nomes (Lista categorias de ameaças em ordem alfabética crescente de nomes)
- Listagem da documentação do sistema (Lista de documentação)
- Visualização da documentação (Visualizar documentação)
- Cadastro de documentação (Cadastra uma documentação)
- Edição de documentação (Edita uma documentação)
- Exclusão de documentação (Exclui uma documentação)
- Listagem de usuários de um grupo específico (Lista usuários de um grupo específico)
- Listagem de usuários por ordem decrescente de acesso (Lista usuários por ordem decrescente de data de acesso)

2.1 Listagem dos grupos de usuários

Home Incidentes Categorias Ameaças Usuários Grupos Documentação Manual Sobre
Roberto Pinheiro

GRUPOS DE USUÁRIOS

Nome	Slug	Descrição	Ações
Administrador do sistema	admin-system	Gerencia incidentes, categorias e tipos de ameaças, usuários e grupos de usuários	   
Administrador de usuários	admin-users	Gerencia usuários	   
Administrador de grupos de usuários	admin-roles	Gerencia grupos de usuários (roles)	   
Analista de Seg. da Informação 1	analyst-si-1	Atende notificações de incidentes	   
Analista de Seg. da Informação 2	analyst-si-2	Gerencia as categorias e tipos de ameaças e ataques	   
Colaborador	colaborator	Funcionário da empresa	   
Suspenso	user-off	Funcionário desligado da empresa ou usuário suspenso	   
Convidado	guest	Convidado	   
Visitante	visitor	Visitante registrado no sistema	   

OrionTechInfo - By: Roberto Pinheiro - Copyright © 2021 - Todos os direitos reservados.

2.2.1 O que é slug?

Normalmente, a primeira coisa que um visitante vê ao acessar uma página web é a sua URL, ou seja, o seu endereço. A URL geralmente está vinculada a algum link. Esse link é a "ligação" direta que acessa o seu conteúdo no local exato onde foi criado. "Slug" é uma expressão para definir um caminho amigável, um link fácil de ler e entender tanto para o visitante e/ou usuário quanto para os mecanismos de busca na Internet.

Convém destacar que slug e URL não são sinônimos. A URL, sigla que significa "Uniform Resource Locator", é o endereço completo do site. O slug é apenas parte da URL, normalmente o final. No entanto, ele pode ser alterado livremente

Para criar um slug é necessário seguir algumas recomendações:

- Não utilizar acentuação ou caracteres especiais;
- Todas as letras minúsculas;
- Substituir o espaço em branco por traços "-".
- Mantenha o slug curto. Um slug longo é complexo demais e desnecessário.

Por exemplo, se você pretende criar um grupo de usuários com o nome de "Clientes e Fornecedores", um possível slug seria:

clientes-e-fornecedores


Observação: Se no campo slug você digitar letras maiúsculas ou utilizar acentuação e/ou espaços em brancos, o sistema automaticamente fará a conversão do texto digitado para o formato slug.

2.3 Exibição dos detalhes de um grupo de usuários

- Para visualizar informações de um determinado grupo de usuários clique no botão verde (**Exibir detalhes**) localizado no campo "**Ações**" do referido grupo.

GRUPO DE USUÁRIOS

INFORMAÇÕES CADASTRADAS:



Id: 2

Grupo de usuários: Administrador do sistema

Slug: admin-system


Descrição: Gerencia incidentes, categorias e tipos de ameaças, usuários e grupos de usuários

Criado em: 13/06/2019 - 17:04:49

2.4 Atualização de dados de um grupo de usuários

- Para atualizar (editar) dados de um determinado grupo de usuários clique no botão amarelo (**Editar**) localizado no campo "**Ações**" do referido grupo.

ATUALIZAR GRUPO:
COLABORADOR



* Informação obrigatória

Nome *

Slug *

Exemplos: Para um nome de grupo "Administrador de Usuários" o slug poderia ser "administrador-usuarios". Recomenda-se um slug curto (no máximo 3 palavras separadas por hífen).

Descrição *

Lista de permissões

- ☐ Listagem de usuários (Lista todos os usuários do sistema)
- ☐ Exibição de detalhes de um usuário (Exibe detalhes de um usuário do sistema)
- ☐ Cadastro de um usuário (Cadastra um usuário no sistema)
- ☐ Edição de usuários (Edita dados de um usuário do sistema)
- ☐ Exclusão de usuário (Exclui um usuário do sistema)
- ☐ Alteração de senha de usuário (Altera a senha do usuário)
- ☐ Listagem usuários x grupo de usuários (Lista usuários vinculados a um grupo de usuários)
- ☐ Listagem de usuários por ordem alfabética de nomes (Lista usuários em ordem alfabética crescente de nomes)
- ☐ Listagem de grupos de usuários (Lista os grupos de usuários do sistema)
- ☐ Exibição de detalhes de um grupo de usuários (Exibe detalhes de um grupo de usuário do sistema)
- ☐ Criação de um grupo de usuários (Cria um grupo de usuários)
- ☐ Edição de um grupo de usuários (Edita dados de um grupo de usuários)
- ☐ Exclusão de um grupo de usuários (Exclui um grupo de usuários do sistema)
- ☒ Listagem de notificações de incidentes (Lista notificações de incidentes)
- ☒ Exibição de detalhes de uma notificação de incidente (Exibe detalhes de uma notificação de incidente)
- ☒ Criação de notificação de incidente (Cria uma notificação de incidente)
- ☐ Edição de notificação de incidente (Edita uma notificação de incidente)
- ☐ Exclusão de notificação de incidente (Exclui uma notificação de incidente)
- ☐ Listagem de notificações de incidentes por usuário (Exibe notificações de incidentes por usuário)
- ☐ Listagem de notificações de incidentes abertas (Exibe notificações de incidentes abertas)
- ☒ Listagem de tipos de ameaças ou ataques (Lista tipos de ameaças ou ataques)
- ☒ Exibição de detalhes de um tipo de ameaça ou ataque (Exibe detalhes de um tipo de ameaça ou ataque)
- ☐ Cadastro de tipo de ameaça ou ataque (Cadastra um tipo de ameaça ou ataque)
- ☐ Edição de tipo de ameaça ou ataque (Edita um tipo de ameaça ou ataque)
- ☐ Exclusão de tipo de ameaça ou ataque (Exclui um tipo de ameaça ou ataque)
- ☒ Listagem de ameaças em ordem crescente de nomes (Lista ameaças em ordem alfabética crescente de nomes)
- ☒ Listagem de ameaças em ordem decrescente de nomes (Lista ameaças em ordem alfabética decrescente de nomes)
- ☒ Listagem de ameaças em ordem decrescente de id (Lista ameaças em ordem decrescente de id)
- ☒ Listagem de categorias de ameaças ou ataques (Lista categorias de ameaças ou ataques)
- ☐ Exibição de detalhes de uma categoria de ameaças ou ataques (Exibe detalhes de uma categoria de ameaças ou ataques)
- ☐ Cadastro de categoria de ameaça ou ataque (Cadastra uma categoria de ameaça ou ataque)
- ☐ Edição de categoria de ameaça ou ataque (Edita uma categoria de ameaça ou ataque)
- ☒ Exclusão de categoria de ameaça ou ataque (Exclui uma categoria de ameaça ou ataque)
- ☒ Listagem de ameaças por categoria (Lista as ameaças de uma determinada categoria)
- ☐ Listagem de categorias de ameaças em ordem alfabética de nomes (Lista categorias de ameaças em ordem alfabética crescente de nomes)
- ☒ Listagem da documentação do sistema (Lista de documentação)
- ☒ Visualização da documentação (Visualizar documentação)
- ☐ Cadastro de documentação (Cadastra uma documentação)
- ☐ Edição de documentação (Edita uma documentação)
- ☐ Exclusão de documentação (Exclui uma documentação)
- ☐ Listagem de usuários de um grupo específico (Lista usuários de um grupo específico)

- Faça as alterações que deseja e em seguida clique no botão "**Gravar**".





























































3 USUÁRIOS

O controle de acesso é um exemplo de adoção de mecanismos de autenticação e consiste em verificar, na base de dados, se a pessoa que deseja acessar o sistema tem ou não autorização para isso. Em caso positivo, libera o acesso, caso contrário, não. O acesso é controlado por um procedimento que estabelece a identidade do usuário com algum grau de confiança (autenticação), e só então concede determinados privilégios (permissões) de acordo com sua identidade e grupo de usuários a qual pertence.


Os usuários do sistema podem ser internos como: os colaboradores, profissionais da equipe de TI ou da segurança da informação e administradores. Também podem ser externos como: visitantes, convidados, clientes e fornecedores. Este módulo permite que os administradores (do sistema, ou de usuários) cadastrem e gerenciem usuários. Possui as seguintes funcionalidades:

- 1) listagem de usuários (por ordem crescente de nomes ou decrescente de id);
- 2) cadastro de usuário definindo o grupo no qual ele fará parte;
- 3) exibição de detalhes do usuário;
- 4) atualização dos dados de um usuário;
- 5) exclusão de usuários;
- 6) listagem de incidentes notificados por usuário;
- 7) alteração de senha do usuário;
- 8) listagem de usuários x grupo de usuários.

3.1 Listagem de usuários

USUÁRIOS CADASTRADOS			
<div><div></div><div></div><div></div></div>			
Nome	Email	Último acesso	Ações
Luciano Campos	luciano_campos@hotmail.com	21/01/2021 07:28:44	    
Fabiana Vieira	fabiana_vieira@gmail.com	05/01/2021 09:25:24	    
Helena Romero	helenaromero@ig.com.br	22/12/2020 19:22:32	    
Emília D'ávila	emilia_davila@uol.com.br	18/12/2020 01:57:28	    
Allison de Oliveira	allison_oliveira@yahoo.com	29/12/2020 15:56:35	    
Silvana Lozano	silvana_lozano@gmail.com	10/01/2021 22:38:19	    
Henrique Barreto	henrique_barreto@terra.com.br	25/12/2020 02:27:16	    
Violeta Godói	violeta_godoi@gmail.com	30/12/2020 11:01:24	    
Pablo Domingues	pablo_domingues@ig.com.br	19/01/2021 20:54:44	    
Vitória Grego	vitória_grego@yahoo.com	25/12/2020 23:05:55	    
<div><div></div><div>Total de usuários: 20</div></div>			
<div><div></div></div>			

3.2 Cadastro de usuário

- Clique no botão  (Cadastrar usuário) localizado na parte superior da tela. Será aberto o formulário a seguir:

CADASTRAR USUÁRIO



* Informação obrigatória

Nome *

Email *

Senha *

Confirmar Senha *

Grupo de usuários

☐ Administrador de usuários *(Gerencia usuários)*

☐ Administrador de grupos de usuários *(Gerencia grupos de usuários (roles))*

☐ Analista de Seg. da Informação 1 *(Atende notificações de incidentes)*

☐ Analista de Seg. da Informação 2 *(Gerencia as categorias e tipos de ameaças e ataques)*

☐ Colaborador *(Funcionário da empresa)*

☐ Suspenso *(Funcionário desligado da empresa ou usuário suspenso)*

☐ Convidado *(Convidado)*

☐ Visitante *(Visitante registrado no sistema)*

Cadastrar

- Preencha os campos Nome, Email, Senha e Confirmar Senha.
- Marque o grupo de usuários do qual o usuário fará parte.
- Clique no botão "Cadastrar".

3.3 Exibição de detalhes de um usuário

- Para visualizar informações de um determinado usuário clique no botão verde (**Exibir detalhes**) localizado no campo "Ações" do referido usuário.

ENZO HENRY SOUZA

INFORMAÇÕES CADASTRADAS:

Id: 8

Nome: Enzo Henry Souza

Email: enzo_henry_souza@hotmail.com

Último acesso: 06/02/2021 08:24:49

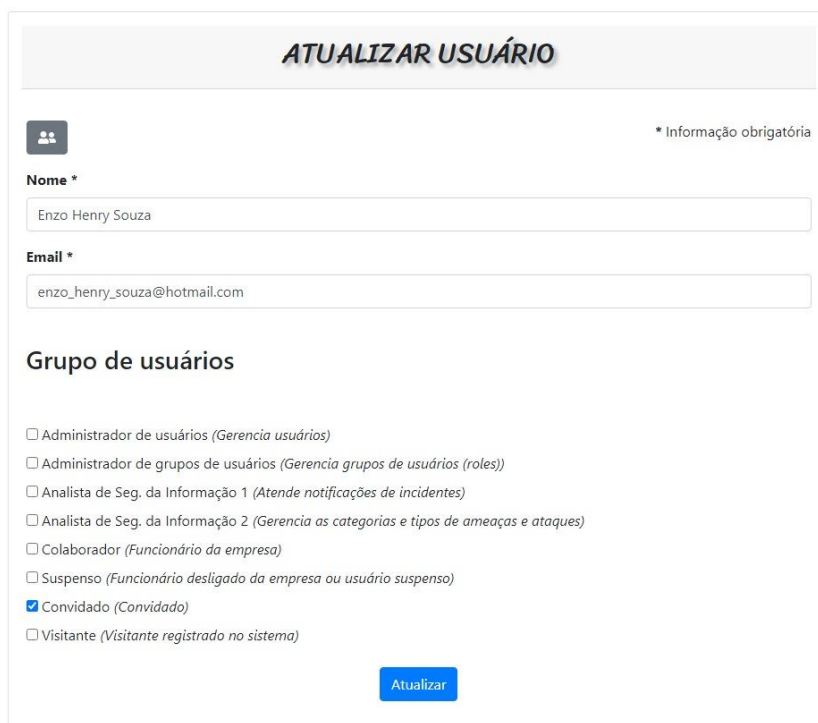
IP: 191.180.30.87

Usuário cadastrado em: 11/02/2021 - 08:24:49

3.4 Atualização de dados de um usuário

- Para atualizar (editar) dados de um determinado usuário clique no botão amarelo (**Editar**) localizado no campo "Ações" do referido usuário.

ATUALIZAR USUÁRIO

 * Informação obrigatória

Nome *

Email *

Grupo de usuários

☐ Administrador de usuários (Gerencia usuários)

☐ Administrador de grupos de usuários (Gerencia grupos de usuários (roles))

☐ Analista de Seg. da Informação 1 (Atende notificações de incidentes)

☐ Analista de Seg. da Informação 2 (Gerencia as categorias e tipos de ameaças e ataques)

☐ Colaborador (Funcionário da empresa)

☐ Suspendo (Funcionário desligado da empresa ou usuário suspenso)

☒ Convidado (Convidado)

☐ Visitante (Visitante registrado no sistema)

Atualizar

- Faça as alterações que deseja e em seguida clique no botão "Gravar".

3.5 Exclusão de um usuário

- Para excluir um usuário do sistema clique no botão vermelho (**Excluir**) do referido usuário. Antes de excluir, o sistema pedirá uma confirmação da exclusão.

The screenshot shows the 'USUÁRIOS CADASTRADOS' (Registered Users) page. A confirmation dialog is displayed over the table, asking: 'app-incidentes.herokuapp.com diz: Tem certeza que deseja excluir Luciano Campos?' with 'OK' and 'Cancelar' buttons. The table below lists three users: Luciano Campos, Fabiana Vieira, and Helena Romero. Each user row has an 'Excluir' button (red icon with a person and a minus sign) in the 'Ações' column.

Nome	Email	Último acesso	Ações
Luciano Campos	luciano_campos@hotmail.com	21/01/2021 07:28:44	[Ver] [Alerta] [Adicionar] [Editar] [Excluir]
Fabiana Vieira	fabiana_vieira@gmail.com	05/01/2021 09:25:24	[Ver] [Alerta] [Adicionar] [Editar] [Excluir]
Helena Romero	helenaromero@ig.com.br	22/12/2020 19:22:32	[Ver] [Alerta] [Adicionar] [Editar] [Excluir]

3.6 Listagem de incidentes notificados por um usuário específico

- Para listar os incidentes notificados por um usuário específico clique no botão preto (**Incidentes notificados**), do referido usuário.

The screenshot shows the 'INCIDENTES NOTIFICADOS POR: EMÍLIO SOARES' page. It displays a list of incidents with columns: Título, Descrição resumida, Critic., Tpo de ameaça, Status, Criada em, and Ações. There are two incidents listed. The total number of incidents is 2.

Título	Descrição resumida	Critic.	Tpo de ameaça	Status	Criada em	Ações
Meu computador faz parte de uma rede de botnets	Executei o anti-vírus da organização que me informou que meu ip consta em uma lista de botnets (c...	Não avaliada	Bot e botnet	Aberto	31/01/2021 - 08:24:50	[Ver] [Alerta] [Adicionar]
Computador com processamento lento	Computador repentinamente passou a ter comportamento estranho e processamento muito lento....	Média	Vírus	Fechado	06/02/2021 - 08:24:50	[Ver] [Alerta] [Adicionar]

3.7 Alteração de senha do usuário

- Para alterar a senha, clique no botão cinza (**Alterar senha**) localizado no campo "Ações", do usuário desejado.




The form is titled "ALTERAR SENHA: EMÍLIO SOARES" in bold, italicized black text. Below the title is a dark gray icon of two people. To the right of the icon is the text "* Informação obrigatória". The form contains two input fields: "Senha *" with the placeholder "Digite a senha" and "Confirmar Senha *" with the placeholder "Redigite a senha". Below these fields is a red note: "Observação: A senha não deve conter caracteres especiais, não pode iniciar por números e deve ter entre 6 e 20 caracteres". At the bottom center is a green button labeled "Alterar".

- Digite a nova senha. A senha não deve conter caracteres especiais, não pode iniciar por números e deve ter o mínimo de 6 caracteres e o máximo de 20 caracteres;
- Confirme a senha;
- Clique no botão "Gravar".

3.8 Listagem de usuários X grupo de usuários

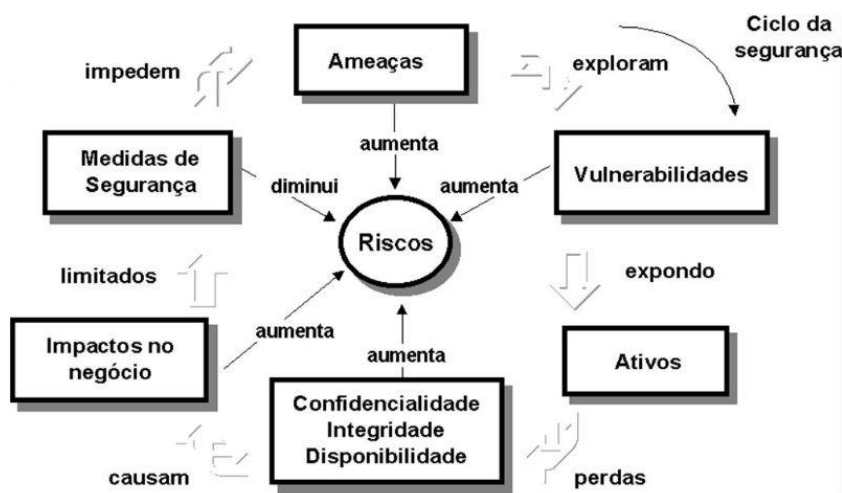
- Para listar, em ordem crescente de nomes, cada usuário e o grupo a qual pertence, clique no botão azul localizado na parte superior esquerda da tela (**Listar usuários x grupo de usuários**)..

USUÁRIOS X GRUPO DE USUÁRIOS			
			
Nome do Usuário	Email	Slug	Nome do grupo
Allison de Oliveira	allison_oliveira@yahoo.com	colaborator	Colaborador
Daniel Souza Araujo	daniel_souza_araujo@oriontecinfo.com.br	analyst-si-1	Analista de Seg. da Informação 1
Daniel Souza Araujo	daniel_souza_araujo@oriontecinfo.com.br	analyst-si-2	Analista de Seg. da Informação 2
Douglas Lima Silva	douglas_lima_silva@oriontecinfo.com.br	analyst-si-1	Analista de Seg. da Informação 1
Emília D'ávila	emilia_davila@uol.com.br	colaborator	Colaborador
Emílio Soares	emilio_soares@hotmail.com	colaborator	Colaborador
Enzo Henry Souza	enzo_henry_souza@hotmail.com	guest	Convidado
Fabiana Vieira	fabiana_vieira@gmail.com	colaborator	Colaborador
Fábio Kevin Bernardes	fabio_kevin_bernardes@oriontecinfo.com.br	admin-system	Administrador do sistema
Helena Romero	helenaromero@ig.com.br	colaborator	Colaborador
Henrique Barreto	henrique_barreto@terra.com.br	colaborator	Colaborador
Larissa Cunha Barbosa	larissa_cunha_barbosa@oriontecinfo.com.br	admin-users	Administrador de usuários
Larissa Cunha Barbosa	larissa_cunha_barbosa@oriontecinfo.com.br	admin-roles	Administrador de grupos de usuários
Luciano Campos	luciano_campos@hotmail.com	colaborator	Colaborador
Malena Casanova	malena_casanova@r7.com	colaborator	Colaborador
Nicole Isabelle Teixeira	nicole_isabelle_teixeira@gmail.com	guest	Convidado
Pablo Domingues	pablo_domingues@ig.com.br	colaborator	Colaborador
Regina Alves Santos	regina_alves_santos@gmail.com	visitor	Visitante
Silvana Lozano	silvana_lozano@gmail.com	colaborator	Colaborador
Thiago Martins Melo	thiago_martins_melo@oriontecinfo.com.br	admin-users	Administrador de usuários
Violeta Godói	violeta_godoi@gmail.com	colaborator	Colaborador
Vitória Grego	vitoria_grego@yahoo.com	colaborator	Colaborador

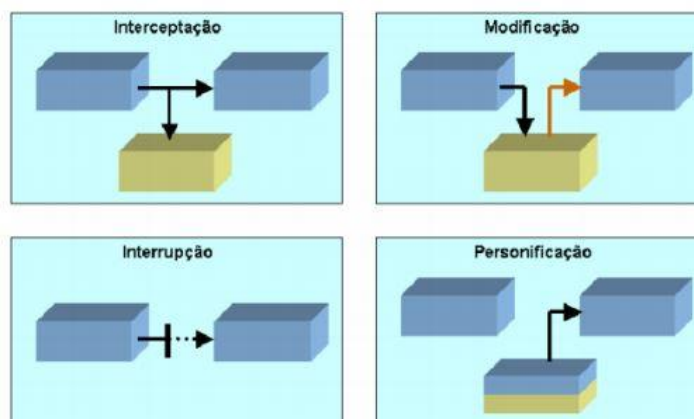
4 CATEGORIAS DE AMEAÇAS E ATAQUES

Ameaças à segurança da informação são situações ou condições que por meio da exploração de vulnerabilidades (falhas em projetos, implementações ou configurações de um software ou sistema operacional) podem causar incidentes que afetam as informações e seus ativos, provocando perda de confidencialidade, integridade ou disponibilidade e resultando em prejuízos financeiros ou de comprometimento de imagem da organização. Ao identificar vulnerabilidades é possível dimensionar os riscos aos quais o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção.

Ataques são ações intencionais de agentes maliciosos ao explorar ameaças com o objetivo de conseguir acesso não autorizado, espionagem ou roubo de informações (perda de confidencialidade), destruição ou alteração de dados (perda de integridade), ou para tornar um sistema indisponível (perda de disponibilidade). Após realizar suas ações o atacante pode cobrir seus rastros para dificultar o trabalho do profissional da segurança da informação, que tem a função de descobrir o que foi realizado indevidamente pelo atacante. O fato de um ataque estar acontecendo não significa necessariamente que o atacante terá sucesso.






































Os diversos tipos de ameaças e ataques podem ser separados em categorias, de acordo com as características comuns que possuem. A seguir estão ilustradas as principais categorias de ataques.



- **Interceptação:** Ataque que tem como objetivo interceptar e registrar tráfego que passa sobre uma rede digital ou parte dela com diversos objetivos, dentre os quais, obter cópias de arquivos de seu interesse durante sua transmissão, e obter senhas pessoais, informações bancárias ou ver as conversações em tempo real.
- **Modificação:** O ataque de modificação é quando existe alteração da informação que está sendo transmitida, ou seja, ataca-se a integridade da mesma. Um exemplo de ataque desta categoria é o Replay, onde parte de uma transmissão de rede é copiada e reproduzida posteriormente, simulando um usuário autorizado.
- **Interrupção:** Tais ataques têm como objetivo tornar inacessíveis os serviços providos pela vítima a usuários legítimos. Nenhum dado é roubado, nada é alterado e não ocorre nenhum acesso não autorizado ao computador da vítima.
- **Personificação:** É um ataque de falsificação ou disfarce de identidade que ocorre quando uma pessoa se faz passar por outra pessoa de forma a enganar o seu alvo induzindo-o a informar os seus dados pessoais, ou a executar alguma ação em benefício do atacante.


Este módulo permite o gerenciamento de categorias de ameaças e ataques. Possui as seguintes funcionalidades, listagem, cadastro, exibição de detalhes, atualização de dados e exclusão de categorias de ameaças e ataques. Também permite a listagem dos tipos de ameaças por categoria,

4.1 Listagem das categorias de ameaças e ataques

CATEGORIAS DE AMEAÇAS E ATAQUES		
		
Nome	Descrição resumida	Ações
Não identificado	Ameaça ou ataque não identificado.	   
Envio de mensagens eletrônicas em massa	O SPAM é uma mensagem eletrônica que chega ao usuário sem a sua permissão ou sem seu desejo em recebê-lo. Geralmente são recebidas por e-mail, mas também podem circular pelas redes sociais ou comentários de blogs. O SPAM tem um fundo geralmente comercial, mas também pode assumir um viés criminoso.	   
Ameaças internas	Embora os hackers modernos possam usar malware sob medida e técnicas de alta tecnologia para planejar um roubo, é provável que comecem explorando o ponto de entrada mais frágil: a natureza humana. Para evitar riscos de incidentes, os funcionários devem cumprir a política de segurança da informação da empresa. Há também os chamados "ataques internos" que ocorrem quando funcionários da empresa comportam-se de modo não autorizado, por exemplo, executando softwares inadequados com o objetivo de burlar a segurança para obter algum tipo de lucro ou vantagem, ou quando ocorre a tentativa de efetuar acesso em que o mesmo não tenha permissão.	   
Ataques de modificação de dados	Nesse procedimento o invasor, visando obter algum benefício, não apenas escuta o tráfego da rede, como também altera a informação capturada (ataque a integridade) e a envia ao destinatário. Por exemplo, um cliente envia uma mensagem para um banco para iniciar alguma transação. O atacante intercepta a mensagem e modifica o tipo de transação para tirar algum proveito. Um exemplo deste ataque é o Replay, onde parte de uma transmissão de rede é copiada e reproduzida posteriormente, simulando um usuário autorizado.	   
Tentativa de acesso não autorizado	Autenticação é um processo utilizado para verificar se a pessoa que solicita o acesso a um sistema ou serviço é uma pessoa cadastrada e autorizada. Normalmente a autenticação é feita por meio da solicitação do nome de usuário (ou seu email) e senha. Um ataque de autenticação é uma das formas de explorar falhas de segurança em aplicações web, em um processo de login de uma página web para conseguir acesso ao sistema. Mecanismos de autenticação contêm uma riqueza de diferentes vulnerabilidades, tanto de projeto quanto de implementação. Um atacante pode se aproveitar disso para obter acesso não autorizado.	   
Interceptação de tráfego de rede (Sniffing)	Sniff, em inglês, quer dizer, entre outros significados, farejar. Sniffing é a prática que utiliza uma ferramenta genericamente chamada sniffer. Essa ferramenta é um programa de computador ou hardware que pode interceptar e registrar tráfego que passa sobre uma rede digital ou parte de uma rede.	   
Ataques de falsificação (Spoofing)	É um ataque de falsificação ou disfarce de identidade que ocorre quando uma pessoa se faz passar por outra pessoa de forma a enganar o seu alvo e levá-lo a partilhar os seus dados pessoais, ou a executar alguma ação para benefício do spoofer. Muitas vezes, o infrator toma o seu tempo e faz um esforço para ganhar a confiança da sua vítima, certificando-se assim que este partilha mais facilmente informação sensível.	   
Exploração de vulnerabilidades de segurança	O termo exploração é geralmente usado para descrever um programa de software desenvolvido para atacar um ativo tirando proveito de vulnerabilidades em um sistema. Vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. Uma vulnerabilidade é como um buraco no software ou sistema que permite a um atacante executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.	   
Engenharia social	Engenharia social é qualquer estratégia não-técnica usada pelos hackers que, em grande parte, dependem da interação humana e geralmente envolvem iludir o usuário para desrespeitar práticas de segurança padrão, como abrir links maliciosos, baixar arquivos suspeitos ou compartilhar informações confidenciais que permitam ao hacker atingir seus objetivos.	   
Ataques de negação de serviço	Diferentemente da maioria dos ataques da Internet, um ataque de negação de serviço não visa invadir um computador para extrair informações confidenciais, como números de cartões de crédito e senhas bancárias, e nem para modificar o conteúdo armazenado neste computador, como sites da Internet. Tais ataques têm como objetivo tornar inacessíveis os serviços providos pela vítima a usuários legítimos. Nenhum dado é roubado, nada é alterado e não ocorre nenhum acesso não autorizado ao computador da vítima. A vítima simplesmente para de oferecer o seu serviço aos clientes legítimos, enquanto tenta lidar com o tráfego gerado pelo ataque. Um serviço pode ser o uso de um buscador de páginas, a compra de um determinado produto ou simplesmente a troca de mensagens entre duas entidades. O resultado de um ataque de negação de serviço pode ser o congelamento ou a reinicialização do programa da vítima que presta o serviço, ou ainda o esgotamento completo de recursos necessários para prover o seu serviço.	   
Malware (Códigos maliciosos)	A expressão malware provém do termo malicious software (do inglês software malicioso), que são programas desenvolvidos para executarem ações danosas e ilícitas em um sistema. Entre os danos mais conhecidos, podem ser destacados a perda de dados e o roubo de informações sigilosas. Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.	   

Total de categorias: 11

4.2 Cadastro de categoria de ameaças e ataques

- Clique no botão  (**Cadastrar categoria**) localizado na parte superior da tela. Será aberto o formulário a seguir:

CADASTRAR **CATEGORIA DE AMEAÇA OU ATAQUE**



* Informação obrigatória

Nome *

Descrição *

Cadastrar

- Preencha os campos: Nome e Descrição.;
- Clique no botão "Cadastrar".

4.3. Exibição dos detalhes de uma categoria de ameaças e ataques

- Para visualizar informações de uma determinada categoria de ameaças e ataques clique no botão verde (**Exibir detalhes**) localizado no campo "Ações" da referida categoria.

CATEGORIA DE AMEAÇA OU ATAQUE
Ataques de falsificação (Spoofing)



Id: 5

Título: Ataques de falsificação (Spoofing)

Descrição:

É um ataque de falsificação ou disfarce de identidade que ocorre quando uma pessoa se faz passar por outra pessoa de forma a enganar o seu alvo e levá-lo a partilhar os seus dados pessoais, ou a executar alguma ação para benefício do spoofer. Muitas vezes, o infrator toma o seu tempo e faz um esforço para ganhar a confiança da sua vítima, certificando-se assim que este partilha mais facilmente informação sensível.



```
graph LR
    A[Attacker A] -- "Impersonates U" --> V[Victim V]
    U[User U] -- "Sends message" --> R[Router]
    R -- "Sends message" --> V
    V -- "Responds to A" --> R
    R -- "Sends message" --> A
```

Visto que é uma personificação efetuada por meios tecnológicos, o spoofing pode assumir várias formas. As formas mais sofisticadas de spoofing passam-se todas online. Na maioria dos casos, estas implicam o envio de e-mails fraudulentos para alvos desprevenidos, mas podem também incluir spoofing de dispositivos e endereços. Independentemente do seu tipo, a maioria dos ataques de spoofing é maliciosa. Os infratores por detrás destes ataques tentam normalmente adquirir o acesso aos dados pessoais da vítima, distribuir malware, aceder a redes privadas, criar botnets com o propósito de lançar ciberataques, ou causar prejuízos à vítima.

O spoofing em si não é ilegal, dado que qualquer pessoa pode precisar de falsificar o seu número de telefone, endereço IP, ou mesmo o nome para proteger a sua identidade, ou para poder aceder a certos serviços indisponíveis para a sua região. Todavia, é ilegal usar o spoofing para defraudar outra pessoa e incorrer em práticas criminais. Dependendo da gravidade do ataque, os spoofers podem ser multados ou mesmo sentenciados a pena de prisão. Podem também ter de compensar a sua vítima pelos danos sofridos na consequência do ataque.

Pilares da segurança afetados: confidencialidade, integridade.

Cadastrado em: 11/02/2021 - 08:24:50

4.4 Atualização de dados de uma categoria de ameaças e ataques

- Para atualizar (editar) dados de uma determinada categoria de ameaças ou ataques clique no botão amarelo (**Editar**) localizado no campo "Ações" do referido grupo.

ATUALIZAR - CATEGORIA DE AMEAÇAS OU ATAQUES

* Informação obrigatória

Nome *

Ataques de falsificação (Spoofing)

Descrição *

É um ataque de falsificação ou disfarce de identidade que ocorre quando uma pessoa se faz passar por outra pessoa de forma a enganar o seu alvo e levá-lo a partilhar os seus dados pessoais, ou a executar alguma ação para benefício do spoofer. Muitas vezes, o infrator toma o seu tempo e faz um esforço para ganhar a confiança da sua vítima, certificando-se assim que este partilha mais facilmente informação sensível.

Attacker A

Atualizar

- Faça as alterações que deseja e em seguida clique no botão "Gravar".

4.5 Exclusão de uma categoria de ameaças e ataques

- Para excluir uma categoria de ameaças ou ataques clique no botão vermelho (**Excluir**) do referido grupo. Antes de excluir, o sistema pedirá uma confirmação da exclusão.

localhost/sgi30-prod/public/categories

Gerador de Formul... Formulário com vali... Gerador de...

Home Incidents Categories Types Users



localhost diz

Tem certeza que deseja excluir a categoria de ameaça ou ataque?

OK Cancelar

CATEGORIAS DE AMEAÇAS E ATAQUES

Nome Descrição resumida Ações

Não identificado	Ameaça ou ataque não identificado	   
Envio de spam	O SPAM é uma mensagem eletrônica que chega ao usuário sem a sua permissão ou sem seu desejo em recebê-lo. Geralmente são recebidas por e-mail, mas também podem circular pelas redes sociais ou comentários de blogs. O SPAM tem um fundo geralmente comercial, mas também pode assumir um viés criminoso.	   

4.6 Listagem de tipos de ameaças por categoria

- Para listar as ameaças e ataques de uma categoria específica clique no botão cinza (**Ameaças cadastradas**), da referida categoria.

AMEAÇAS POR CATEGORIA: Ataques de falsificação (Spoofing)		
		Total de ameaças: 5
Id	Nome	Descrição resumida
46	ARP Spoofing	O ARP – Address Resolution Protocol, é um protocolo utilizado para encontrar um endereço ethernet (MAC) a partir do endereço IP. O host que está procurando um MAC envia através de broadcast um pacote ARP contendo o endereço IP do host desejado e espera uma resposta com seu endereço MAC, que será mapeado para o respectivo endereço IP. Esta técnica é aplicada apenas em redes Ethernet.
44	DNS Spoofing	Todos os computadores e websites na Internet têm o seu próprio endereço IP único. Quando um usuário escreve um endereço no seu browser e pressiona Enter, o sistema de nomes de domínios (Domain Name System, ou DNS) procura rapidamente o endereço IP que corresponde ao nome do domínio que foi inserido, e redireciona o usuário para esse endereço. Os hackers encontraram maneiras de manipular este sistema e redirecionar o tráfego para websites maliciosos. Este tipo de manipulação é chamado DNS spoofing.
43	Email Spoofing	O envio de e-mails é baseado no protocolo SMTP, que não exige senha ou autenticação do remetente. Por conta disto um servidor de transporte de e-mail (MTA do inglês Mail Transfer Agent) pode identificar-se como sendo do domínio A, mesmo não o sendo. Os spammers utilizam esta flexibilidade do protocolo para, dentre outros exemplos, se fazer passar por uma instituição financeira e mandar um e-mail em nome do banco solicitando a senha ou outros dados do correntista (prática conhecida por Phishing).
25	IP Spoofing	Todo computador em uma rede é identificado com um endereço IP (Internet Protocol), usado para se comunicar com outros dispositivos na mesma rede. Os endereços IP vêm em diferentes formas, a forma mais comum, conhecida como IPv4, fornece a cada computador um identificador de 32 bits (por exemplo, 192.168.34.12). Em algumas redes, a segurança de ativos e aplicativos digitais é mantida especificando quais endereços IP podem acessar quais recursos. Porém, devido às características do protocolo IP, o reencaminhamento de pacotes é feito com base numa premissa muito simples: o pacote deverá ir para o destinatário (endereço-destino) e não há verificação do remetente — não há validação do endereço IP nem relação deste com o router anterior (que encaminhou o pacote). Aproveita-se, sobretudo, da noção de confiabilidade que existe dentro das organizações: que supostamente não deveria temer uma máquina de dentro da empresa, se ela é da empresa.. Assim, é possível falsificar o endereço de origem através de uma manipulação simples do cabeçalho IP.
32	Pharming	Ao digitar a URL (endereço) do site que deseja acessar, um banco por exemplo, o servidor DNS converte o endereço em um número IP, correspondente ao do servidor do banco. Se o endereço procurado estiver armazenado no cache do servidor do provedor local, então ele mesmo direciona o programa de navegação para o endereço almejado (esse banco de dados de cache é usado para otimização de desempenho, para que o IP do servidor destino seja resolvido mais rapidamente), caso contrário, a requisição é transferida para um servidor de um provedor maior, e assim por diante, até encontrar aquele que reconheça o endereço procurado e faça a correspondência.

5 TIPOS DE AMEAÇAS E ATAQUES


Com a popularização dos recursos de informática, os problemas relacionados a ameaças, tentativas de ataques e invasões, tornam-se a principal preocupação das organizações, pois afetam os requisitos básicos dos sistemas computacionais. Segundo a norma ABNT NBR ISO/IEC 17799:2005, diversos tipos de ameaças à segurança da informação estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. O foco para o ataque é a obtenção de informações sobre o sistema, que pode ser feito por meio de diversas técnicas, sejam: monitorando a rede; penetrando no sistema; inserindo códigos prejudiciais ou informações falsas no sistema; enviando uma grande quantidade de informações desnecessárias ao sistema comprometendo a disponibilidade do mesmo. Nos ambientes organizacionais os sistemas de informação e redes de computadores estão cada vez mais expostos a essas ameaças. As consequências destes ataques são sempre negativas e podem ser variadas: monitoramento não autorizado; descoberta e vazamento de informações confidenciais; modificação não autorizada de servidores e da base de dados da organização; negação ou corrupção de serviços; fraude ou perdas financeiras; perda de confiança e de reputação da empresa; trabalho extra para a recuperação do sistema e dados; perda de negócios, clientes e oportunidades. Devido aos riscos gerados por ataques e pelos números de incidentes com segurança da informação, dar a devida atenção a esse tema deve fazer parte da estratégia dos gestores e responsáveis por setores de tecnologia nas empresas.

Este módulo permite o gerenciamento dos tipos de ameaças e ataques. Já vem instalado com uma base dos principais tipos de ameaças e ataques. Esta base pode ser modificada através de exclusão ou edição das ameaças cadastradas, além da inclusão de outras ameaças. O módulo possui as seguintes funcionalidades: listagem (em ordem crescente ou decrescente de nomes ou de id), cadastro, exibição de detalhes (texto descritivo sobre a ameaça), atualização (edição) e exclusão de tipos de ameaças ou ataques.


5.1 Listagem dos tipos de ameaças e ataques

TIPOS DE AMEAÇAS E ATAQUES			
Id		Nome	Descrição resumida
			Ações
53	Advanced Persistent Threat	Ameaças persistentes avançadas (APT – Advanced Persistent Threats) constituem um determinado tipo de ameaça cibernética, especialmente focado em espionagem via internet. São descritos como persistentes, pois na maioria das vezes são invasores contratados para atacar determinada organização e as tentativas de invasão só irão cessar após o objetivo final ser atingido, o que pode às vezes demorar meses.	  
52	Defacement	Defacement ou, como é conhecido de maneira popular, deface, é uma técnica que consiste na realização de modificações de conteúdo e estética de uma página da web. A palavra de origem inglesa é utilizada na segurança da informação para categorizar ataques realizados por defacers, que são usuários de computador que na maioria das vezes possuem pouco conhecimento técnico e, por isso, precisam de várias horas para explorar vulnerabilidades de um site a fim de alterar sua página principal através de um servidor.	  
51	Man-in-the-Browser	É um tipo de ataque similar ao Man In The Middle, porém, ao contrário deste ataque, onde um terceiro está situado entre dois pontos finais, ouvindo pacotes para obter informações que lhe sejam úteis, o ataque Man in the Browser ocorre especificamente em navegadores web. O método emprega o uso de um Cavalo de Tróia ou malware similar para obter informações confidenciais dos usuários de sites, especialmente informações bancárias e de cartão de crédito. É uma parte de um código que altera e adiciona campos de entrada diferentes para uma página da web que você está visitando. Como a URL não é alterada, você acredita que o site precisa dessa informação, basta preenchê-la.	  
50	Bolware	O bolware é um malware que infecta computadores e realiza a falsificação de dados de boletos bancários, realizando determinadas mudanças no documento, alterando muitas vezes a conta em que o valor será depositado, criando problemas para o usuário que - sem saber - perde o valor do pagamento realizado, como também para as empresas que irão receber o pagamento.	  
49	CamuBot	O CamuBot se apresenta para a vítima como um módulo de segurança gerado pela instituição financeira e a engana para roubar suas credenciais bancárias. Módulo de segurança é um programa que o banco possui para tornar as suas transações de internet banking mais seguras. Ele é tão sofisticado que inclui o logotipo do banco, fazendo com que o visual e a sensação sejam de que ele realmente faz parte da segurança da aplicação. O golpe envolve ferramentas de engenharia social bastante complexas. Em alguns casos, o malware chega a ter acesso a senhas de uso único empregadas nas autenticações biométricas.	  
48	Vazamento de informações	Vazamento de Informação é um incidente de Segurança da Informação que consiste na liberação indevida (seja proposital ou não intencional) de dados considerados sensíveis ou confidenciais. Como forma de Vazamento de Informação, as possibilidades se estendem desde técnicas que se utilizam de ameaças cibernéticas e técnicas de espionagem via internet – também conhecidas como APT (Advanced Persistent Threat ou “ameaça persistente avançada”) –, até práticas que envolvem engenharia social e a exploração de vulnerabilidades humanas – e-mails de phishing, mídias removíveis infectadas com malware ou interceptação de dados em conexões de wi-fi público.	  
47	Replay Attack	No ataque de repetição, os pacotes são capturados usando um sniffer de pacote. Depois que as informações relevantes são capturadas e extraídas, os pacotes podem ser colocados de volta na rede. A intenção é injetar as informações capturadas – como uma senha – de volta para a rede e direcioná-las para um recurso como um servidor, com o objetivo de obter acesso. Uma vez que os pacotes são reproduzidos, as credenciais válidas fornecem acesso a um sistema, dando a um invasor a capacidade de alterar informações ou obter dados confidenciais.	  
46	ARP Spoofing	O ARP – Address Resolution Protocol, é um protocolo utilizado para encontrar um endereço ethernet (MAC) a partir do endereço IP. O host que está procurando um MAC envia através de broadcast um pacote ARP contendo o endereço IP do host desejado e espera uma resposta com seu endereço MAC, que será mapeado para o respectivo endereço IP. Esta técnica é aplicada apenas em redes Ethernet.	  
45	Browser Hijacking	Os hijackers são programas ou extensões que fazem alterações no navegador da Internet, seja na sua totalidade ou em características específicas (por exemplo: alteram a página inicial do navegador, abrem pop-ups de publicidade, instalam barras de ferramentas, alteram o mecanismo de busca padrão, redirecionam a página visitada para uma outra página escolhida pelo programador da praga digital, entre outros). A concepção dos criadores de hijackers é vender os cliques que o usuário faz nessas páginas, circunstância que lhe gera lucro.	  
44	DNS Spoofing	Todos os computadores e websites na Internet têm o seu próprio endereço IP único. Quando um usuário escreve um endereço no seu browser e pressiona Enter, o sistema de nomes de domínios (Domain Name System, ou DNS) procura rapidamente o endereço IP que corresponde ao nome do domínio que foi inserido, e redireciona o usuário para esse endereço. Os hackers encontraram maneiras de manipular este sistema e redirecionar o tráfego para websites maliciosos. Este tipo de manipulação é chamado DNS spoofing.	  
Total de ameaças: 53			

5.2 Cadastro de tipo de ameaça ou ataque

- Clique no botão  (**Cadastrar ameaça**) localizado na parte superior da tela. Será aberto o formulário a seguir:

CADASTRAR TIPO DE AMEAÇA OU ATAQUE

* Informação obrigatória

Nome *

Descrição *

Categoria de Ameaças *

Cadastrar

- Preencha os campos: Nome e Descrição,;
- Selecione a categoria da ameaça ou ataque;
- Clique no botão "Cadastrar".

5.3 Exibição dos detalhes de uma ameaça ou ataque

- Para visualizar informações de uma determinada ameaça ou ataque clique no botão verde (**Exibir detalhes**) localizado no campo "Ações" da referida ameaça.

TIPO DE AMEAÇA OU ATAQUE
Buffer overflow



Id: 11

Título: Buffer overflow

Descrição:

Os buffers são áreas de memória criadas pelos programas para armazenar dados que estão sendo processados. Cada buffer tem um certo tamanho, dependendo do tipo e quantidade de dados que ele irá armazenar. Um buffer overflow (ou transbordamento de dados) acontece quando o programa excede o uso de memória assignado a ele pelo sistema operacional, ou seja, recebe mais dados do que está preparado para armazenar no buffer. Este excesso de dados será armazenado em áreas de memória próximas (contíguas) e sua aplicação pode ficar instável, parar ou ainda retornar com algumas informações do erro. Já em outros casos, os dados que foram gravados fora do espaço reservado podem conter comandos maliciosos, e quando estes não são devidamente tratados, serão executados. Essa execução pode trazer uma infinidade de problemas para a segurança de sua aplicação. Normalmente, o código malicioso irá garantir ao atacante acesso a um terminal com o mesmo nível de privilégios do programa através do qual a falha foi explorada.

Exemplo de um buffer overflow com strcpy

```
void main()
{
    char source[] = "username12"; // username12 to source[]
    char destination[7]; // Destination is 8 bytes
    strcpy(destination, source); // Copy source to destination

    return 0;
}
```

Buffer (8 bytes)								Overflow	
U	S	E	R	N	A	M	E	1	2
0	1	2	3	4	5	6	7	8	9

Ou seja, quando um atacante consegue enviar códigos maliciosos para explorar uma vulnerabilidade de buffer overflow e é bem sucedido, ele pode tomar o controle de uma aplicação, enviando comandos a serem executados. Esse envio de comando é chamado "execução arbitrária de código", e acontece quando se injeta código dentro de um buffer e este é executado. Quando a aplicação está sendo executada em um sistema operacional com privilégios de sistema, esta vulnerabilidade pode ser explorada para que o atacante realize uma ação chamada "elevação de privilégios". E, caso o ataque seja bem sucedido, o atacante receberá uma shellcode do sistema com os privilégios do usuário que esteja executando a aplicação. Se este for o administrador ou o root, os privilégios destes usuários serão transferidos para o atacante.

Categoria: Exploração de vulnerabilidades de segurança

Cadastrado em: 28/11/2021 - 13:11:00

5.4 Atualização de dados de uma ameaça ou ataque

- Para atualizar (editar) dados de um determinada de ameaças ou ataques clique no botão amarelo (**Editar**) localizado no campo "Ações" da referida ameaça.

ATUALIZAR - TIPO DE AMEAÇA OU ATAQUE

* Informação obrigatória

Nome *

Buffer overflow

Descrição *

Os buffers são áreas de memória criadas pelos programas para armazenar dados que estão sendo processados. Cada buffer tem um certo tamanho, dependendo do tipo e quantidade de dados que ele irá armazenar. Um buffer overflow (ou transbordamento de dados) acontece quando o programa excede o uso de memória assignado a ele pelo sistema operacional, ou seja, recebe mais dados do que está preparado para armazenar no buffer. Este excesso de dados será armazenado em áreas de memória próximas (contíguas) e sua aplicação pode ficar instável, parar ou ainda retornar com algumas informações do erro. Já em outros casos, os dados que foram gravados fora do espaço reservado podem conter comandos maliciosos, e quando estes não são devidamente tratados, serão executados. Esta execução pode trazer uma infinidade de problemas para a segurança de sua aplicação. Normalmente, o código malicioso irá garantir ao atacante acesso a um terminal com o mesmo nível de privilégios do programa através do qual a falha foi explorada.

Exemplo de um buffer overflow com strcpy

Categoria de Ameaças *

Exploração de vulnerabilidades de segurança

Atualizar

- Faça as alterações que deseja e em seguida clique no botão "Gravar".

5.5 Exclusão de um tipo de ameaça ou ataque

- Para excluir uma ameaça ou ataque clique no botão vermelho (**Excluir**) da referida ameaça. Antes de excluir, o sistema pedirá uma confirmação da exclusão.

Home Incidentes Categorias Ameaças app-incidentes.herokuapp.com diz Fábio Kevin Bernardes

Tem certeza que deseja excluir o tipo de ameaça ou ataque?

OK Cancelar

TIPOS DE AMEAÇAS E ATAQUES

Id	Nome	Descrição resumida	Ações
53	Advanced Persistent Threat	Ameaças persistentes avançadas (APT – Advanced Persistent Threats) constituem um determinado tipo de ameaça cibernética, especialmente focado em espionagem via internet. São descritos como persistentes, pois na maioria das vezes são invasores contratados para atacar determinada organização e as tentativas de invasão só irão cessar após o objetivo final ser atingido, o que pode às vezes demorar meses.	Ver Excluir
52	Defacement	Defacement ou, como é conhecido de maneira popular, deface, é uma técnica que consiste na alteração de modificações de conteúdo a partir de uma página de	Ver Excluir

6 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Não importa o quanto você prepara e protege seus ativos, os incidentes ainda assim acontecerão. A gravidade de um incidente de segurança é medida de acordo com o impacto que ele causa no processo de negócio de uma empresa. Sua capacidade de antecipar possíveis ataques e responder adequadamente a incidentes é que faz a diferença entre resolvê-los de forma eficaz ou incorrer em grande dano à sua empresa e à sua reputação. Qualquer incidente que não seja propriamente contido ou solucionado pode – e provavelmente vai – se tornar um problema muito maior que em última instância pode levar ao colapso da rede corporativa ou a danos significativos. Responder rapidamente a um incidente vai fazer com que a empresa minimize as perdas, mitigue as vulnerabilidades exploradas, restaure serviços e processos e reduza o risco de futuros incidentes. Incidentes podem ser tratados através de uma metodologia, conhecida como **Resposta a Incidentes** de Segurança, que procura minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível.



O módulo de incidentes basicamente permite o gerenciamento e registro das notificações de incidentes feitas por usuários e das ações corretivas tomadas pela equipe de TI ou de segurança da informação. Possui as seguintes funcionalidades: listagem geral,, listagem por ameaças, listagem das notificações que estão abertas, cadastro, exibição de detalhes, atualização e exclusão de notificações de incidentes.

6.1 Funcionamento do módulo de incidentes

Em caso de um eventual incidente de segurança da informação, o usuário registra a notificação. Fornece um título para o mesmo, e no campo descrição detalha ao máximo o ocorrido. Na seleção do tipo de ameaça, a escolha padrão é “**Não sabe identificar**”. Caso o usuário tenha uma ideia do que seja, ele pode selecionar a opção mais provável. Ao cadastrar o incidente, automaticamente o status do mesmo será definido como **aberto**, indicando que o incidente ainda não recebeu um tratamento.

6.3 Listagem de notificações de incidentes por ameaça ou ataque

NOTIFICAÇÕES DE INCIDENTES

Todas as ameaças

Não sabe identificar

Vírus










Worm

Trojan


Título	Descrição resumida	Tipo de ameaça	Status	Notificado por	Ações
Vírus detectado, porém não eliminado	Ao executar o anti-vírus foi detectado um vírus que o anti-vírus não consegue eliminar...	Vírus	Fechado	Fabiana Vieira	  
Computador com processamento lento	Computador repentinamente passou a ter comportamento estranho e processamento muito lento....	Vírus	Fechado	Emílio Soares	  

Total de incidentes: 2

6.4 Listagem das notificações de incidentes com status aberto

NOTIFICAÇÕES DE INCIDENTES COM STATUS ABERTO						
<div> <div>Todas as ameaças</div> </div>						
Título	Descrição resumida	Tipo de ameaça	Status	Notificado por	Ações	
Meu computador faz parte de uma rede de botnets	Executei o anti-vírus da organização que me informou que meu ip consta em uma lista de ...	Bot e botnet	Aberto	Emílio Soares	  	
Saque ilegal em minha conta bancária	Recebi telefonema de uma pessoa que se identificou como funcionário de minha agência ban...	Não sabe identificar	Aberto	Henrique Barreto	  	
Atividade elevada do disco rígido	HD está registrando atividade elevada mesmo com o computador em "descanso" e sem realizar...	Não sabe identificar	Aberto	Allison de Oliveira	  	

6.5 Cadastro de notificação de incidente

- Clique no botão  (**Cadastrar notificação de incidente**) localizado na parte superior da tela. Será aberto o formulário a seguir:

CADASTRAR NOTIFICAÇÃO DE INCIDENTE

 * Informação obrigatória

Título *

Descrição *

Tipo de Ameaça *

Cadastrar

- Preencha os campos: Título e Descrição.;
- Selecione a categoria da ameaça ou ataque;
- Clique no botão "Cadastrar".

6.6 Exibição dos detalhes de uma notificação de incidente

- Para visualizar informações de uma determinada notificação de incidente clique no botão verde (**Exibir detalhes**) localizado no campo "**Ações**" da referida notificação.

NOTIFICAÇÃO DE INCIDENTE
Alterações no browser sem meu consentimento



Id: 13

Título: Alterações no browser sem meu consentimento

Descrição: Em meu navegador foram feitas automaticamente, sem que eu tenha configurado ou permitido, alteração da página inicial padrão e do motor de buscas, além de ser exibida uma barra de ferramentas indesejada. Estou tentando, mas não está sendo possível reconfigurar o browser para voltar ao estado anterior.

Tipo de ameaça: Browser Hijacking

Categoria da ameaça: Malware (Códigos maliciosos)

Criticidade: Baixa

Status: Fechado

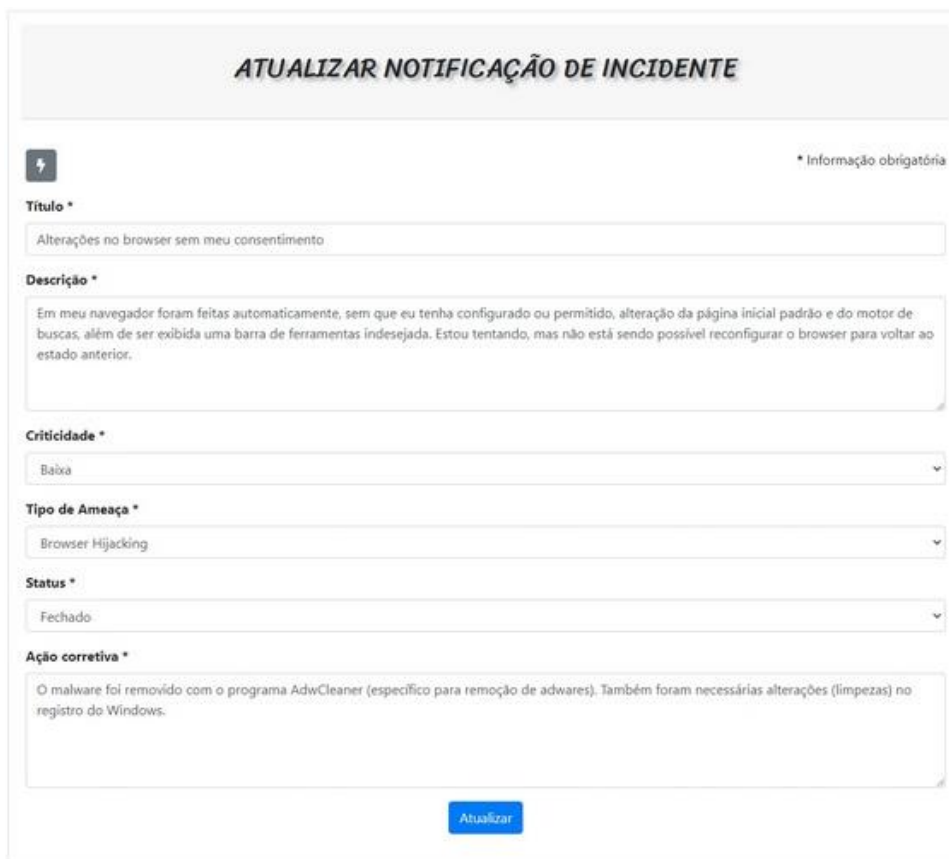
Notificação aberta por: Malena Casanova - **Data:** 05/02/2021 - 08:24:50

Ação corretiva: O malware foi removido com o programa AdwCleaner (específico para remoção de adwares). Também foram necessárias alterações (limpezas) no registro do Windows.

Notificação atendida por: Douglas Lima Silva - **Data:** 06/02/2021 - 08:24:50

6.7 Atualização de dados de uma notificação de incidente

- Para atualizar (editar) dados de uma determinada notificação de incidente clique no botão amarelo (**Editar**) localizado no campo "**Ações**" da referida notificação.



ATUALIZAR NOTIFICAÇÃO DE INCIDENTE

* Informação obrigatória

Título *

Alterações no browser sem meu consentimento

Descrição *

Em meu navegador foram feitas automaticamente, sem que eu tenha configurado ou permitido, alteração da página inicial padrão e do motor de buscas, além de ser exibida uma barra de ferramentas indesejada. Estou tentando, mas não está sendo possível reconfigurar o browser para voltar ao estado anterior.

Criticidade *

Baixa

Tipo de Ameaça *

Browser Hijacking

Status *

Fechado

Ação corretiva *

O malware foi removido com o programa AdwCleaner (específico para remoção de adwares). Também foram necessárias alterações (limpezas) no registro do Windows.

Atualizar

- Faça as alterações que deseja e em seguida clique no botão "Gravar".

6.7.1 Criticidade e graus de prioridade

No momento em que a equipe de TI é acionada, cada requisitante entende sua demanda como prioritária. Porém, a realidade é que atender a todos ao mesmo tempo não é possível — e nem sempre a ordem cronológica é a mais adequada para a organização como um todo. A TI precisa, então, estabelecer critérios para a prioridade de atendimento. Por isso, um item importantíssimo no registro de incidentes é justamente a classificação. Ela estabelece níveis de criticidade que serão observados ao determinar a ordem de solução.

1. **Baixa:** É quando a ameaça não é motivada ou não é capaz de explorar uma vulnerabilidade, ou ainda há controles que podem prevenir ou impedir que a mesma seja explorada.
2. **Média:** É quando a ameaça é motivada o suficiente para explorar uma vulnerabilidade, mas os controles podem prevenir que a mesma seja explorada.
3. **Alta:** É quando a ameaça é altamente motivada, podendo de fato explorar a vulnerabilidade e cujos controles não forem eficazes.

Um procedimento que pode ser feito é o estabelecimento de graus de prioridade em espécies de tabelas, que deve estar disponível para todos os colaboradores, não somente para os responsáveis pelo gerenciamento de incidentes, de modo que todos os envolvidos possam acompanhar o fluxo de atendimento do chamado. Exemplo:

Prioridade	Descrição	Exemplo de Incidente	Resposta Esperada
Baixa	Um evento de baixo impacto com pouco ou nenhum efeito operacional e que requer pouco esforço para gerenciar e resolver	<ul style="list-style-type: none"> Incidente de vírus em um único computador ou dispositivo Diversas tentativas mal sucedidas de obter acesso não autorizado 	Resolvido por agentes da equipe de resposta com ações já mapeadas.
Média	Possível brecha de segurança que requer investigação e envolvimento do Comitê de Segurança para resolução	<ul style="list-style-type: none"> Acesso não autorizado a uma conta de serviço Tentativa de acesso à sala de servidores Escaneamento de portas em rede interna ou externa Múltiplos incidentes de vírus 	Precisa ser escalado para o Comitê de Segurança e Risco para coordenação, investigação e resolução
Alta	Evento com impacto significativo a serviços críticos de TI ou informações, dano a equipamento físico ou à pessoas	<ul style="list-style-type: none"> Violação em larga escala de dados sensíveis a pesquisa, dados financeiros ou pessoais Pichação do website da instituição Acesso não autorizado à sala de servidores Comprometimento de dados de pagamento 	<p>Precisar ser escalado ao Diretor e ao Comitê de Segurança Imediatamente</p> <p>Todos os envolvidos precisam ser notificados Uma revisão pós-incidente precisa ser realizada</p>

Fonte: Adaptado de *Incident Management Procedure, Flinders University*

6.8 Exclusão de uma notificação de incidente

- Para excluir uma notificação de incidente clique no botão vermelho (**Excluir**) da referida notificação. Antes de excluir, o sistema pedirá uma confirmação da exclusão.

The screenshot shows a web application interface for incident management. At the top, there is a navigation bar with links: Home, Incidentes, Categorias, Ameaças. A user profile dropdown shows 'Fábio Kevin Bernardes'. A modal dialog is open in the center, asking 'Tem certeza que deseja excluir a notificação de incidente?' with 'OK' and 'Cancelar' buttons. Below the dialog, the main section is titled 'NOTIFICAÇÕES DE INCIDENTES'. On the left, there is a sidebar with 'Tipos de ameaças' (Types of threats) including 'Todas as ameaças', 'Não sabe identificar', 'Vírus', and 'Worm'. The main table lists notifications with columns: Título, Descrição resumida, Tipo de ameaça, Status, Notificado por, and Ações. The first row shows a Ransomware incident with status 'Fechado' and a notification by Daniel Souza Araujo. The second row shows an activity on a hard drive with status 'Aberto' and a notification by Allison de Oliveira. The third row shows a computer virus with status 'Fechado' and a notification by Emilio Soares. Each row has an 'Excluir' (Delete) button in the actions column.

7 COMO ADQUIRIR O APLICATIVO

As funcionalidades do usuário cadastrado como visitante são limitadas. Se você tiver interesse em implantar o sistema com todas as funcionalidades em sua empresa (conforme descrito neste manual) envie um email para Roberto Pinheiro - pinheiroberto61@gmail.com e faça a solicitação.