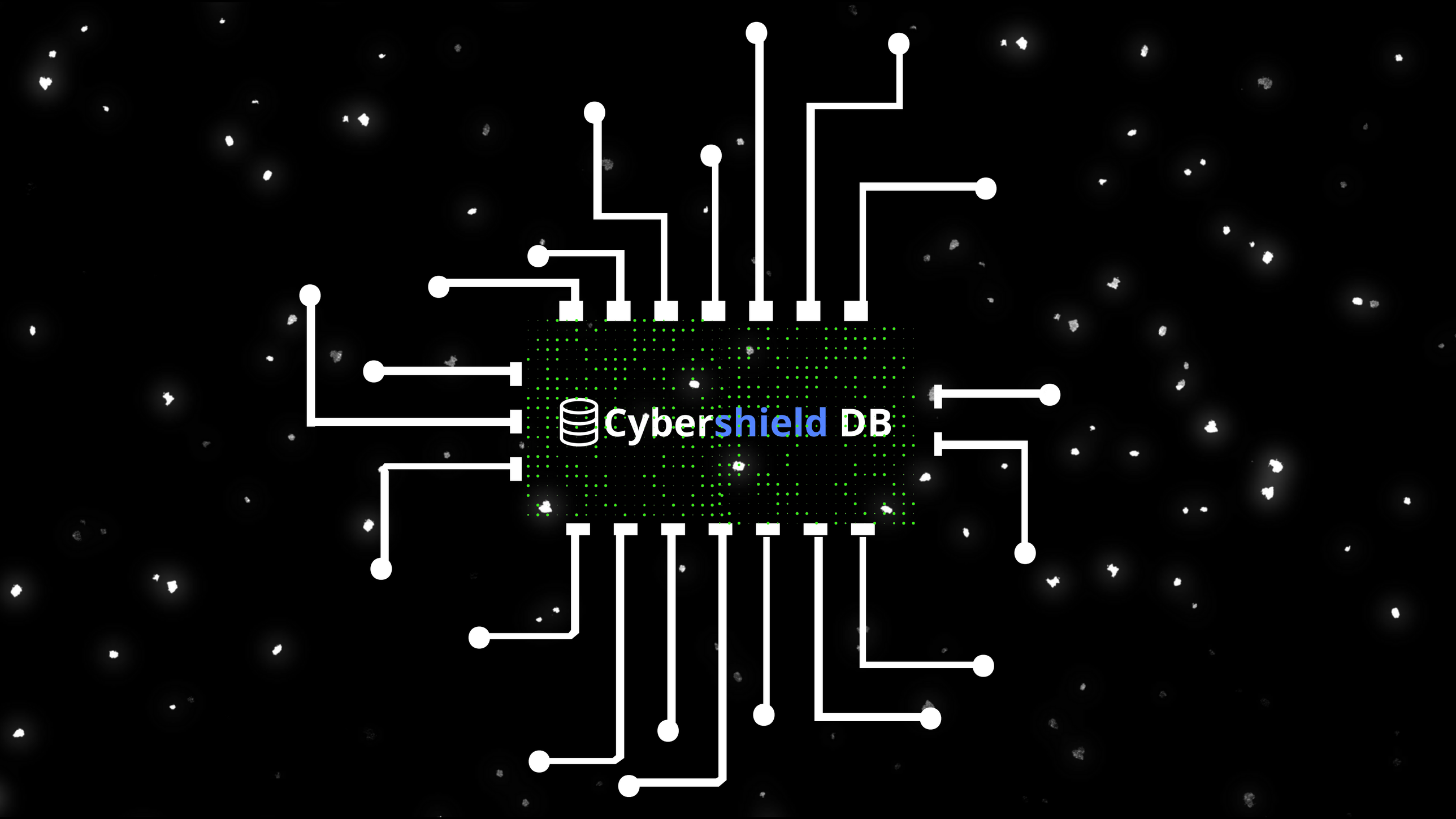

Cybershield DB

Cybershield DB

A cibersegurança é crucial na era digital para proteger dados pessoais e empresariais, prevenir ataques cibernéticos, garantir a continuidade dos negócios e cumprir regulamentações. Além disso, ela aumenta a confiança dos clientes e parceiros, protege infraestruturas críticas e acompanha a evolução das ameaças cibernéticas. Medidas como firewalls, antivírus, criptografia, autenticação de dois fatores, backups regulares e educação dos usuários são essenciais para mitigar riscos e proteger informações sensíveis.

INCIDENTES

Cybershield DB

Os Incidentes são eventos específicos de segurança cibernética que são registrados detalhadamente para análise e resposta adequada. Cada incidente é descrito em termos de sua natureza, gravidade e data de relato, fornecendo uma visão abrangente do cenário de segurança da organização. Além disso, os danos causados aos dispositivos e a natureza específica do dano são documentados para avaliar o impacto e direcionar as medidas de mitigação apropriadas. O registro de incidentes permite uma resposta rápida e eficaz, minimizando os danos e fortalecendo as defesas contra futuras ameaças.

TIPOS DE INCIDENTES

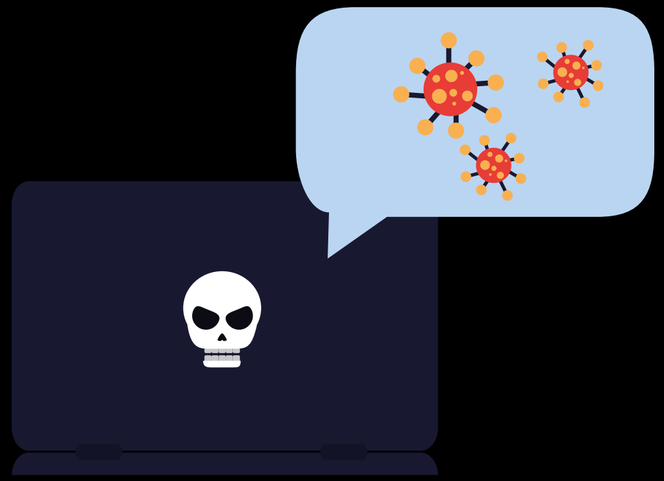
Cybershield DB

Os Tipos de Incidentes são categorizados e registrados para uma compreensão clara das ameaças cibernéticas enfrentadas pela organização. Cada tipo de incidente é identificado, categorizado e priorizado com base em sua gravidade e categoria. Isso permite uma resposta mais eficaz e direcionada a cada incidente, garantindo que os recursos sejam alocados adequadamente para enfrentar as ameaças mais críticas. Além disso, o registro da data de criação e atualização dos tipos de incidentes permite o acompanhamento e a análise ao longo do tempo, fornecendo insights valiosos para aprimorar as medidas de segurança cibernética.

COMENTÁRIOS DE INCIDENTES

Cybershield DB

Os Comentários de Incidentes são registros de comunicações relacionadas a incidentes específicos de segurança cibernética. Cada comentário é associado a um incidente específico e pode ser feito por usuários autorizados. Os comentários fornecem informações adicionais, esclarecimentos e discussões sobre o incidente em questão, permitindo uma colaboração eficaz entre os membros da equipe de resposta a incidentes. O registro dos comentários e suas datas de criação e atualização oferecem um histórico detalhado das ações e discussões realizadas durante a resolução do incidente.



USUARIOS

Cybershield DB

Os Usuários são os indivíduos autorizados a acessar e operar o sistema de gerenciamento de segurança cibernética da organização. Cada usuário é identificado por um nome de usuário exclusivo e possui informações como e-mail, cargo e número de telefone registrados no banco de dados. Além disso, medidas de segurança adicionais, como perguntas e respostas de segurança, são implementadas para proteger o acesso ao sistema contra atividades não autorizadas. O registro detalhado dos usuários permite um gerenciamento eficaz de suas permissões e responsabilidades dentro do contexto da segurança cibernética da organização.

DEPARTAMENTOS

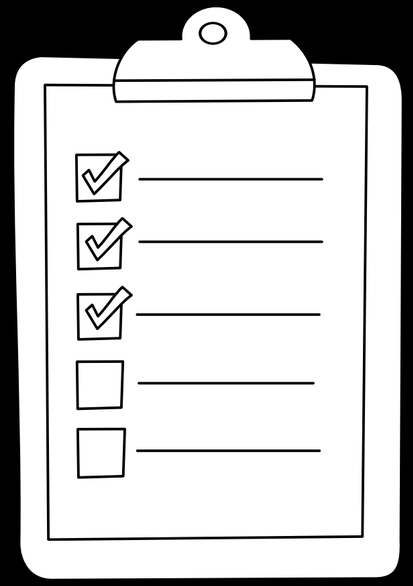
Cybershield DB

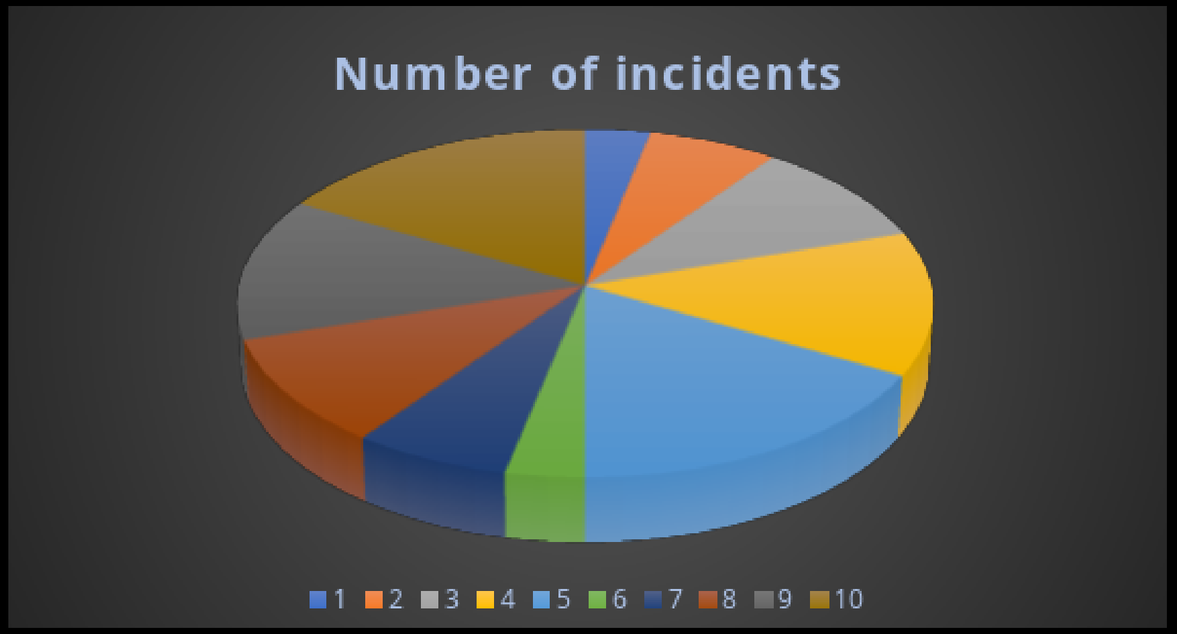
Os Departamentos representam as diferentes unidades organizacionais dentro da empresa, cada uma com suas próprias responsabilidades e funções. Cada departamento é identificado por um código exclusivo e é descrito em termos de seu gerente, número de funcionários e localização. O registro dos departamentos permite uma visão estruturada da organização, facilitando o gerenciamento de recursos humanos e a atribuição de responsabilidades. Além disso, a descrição de cada departamento fornece insights adicionais sobre suas atividades e contribuições para os objetivos gerais da organização.

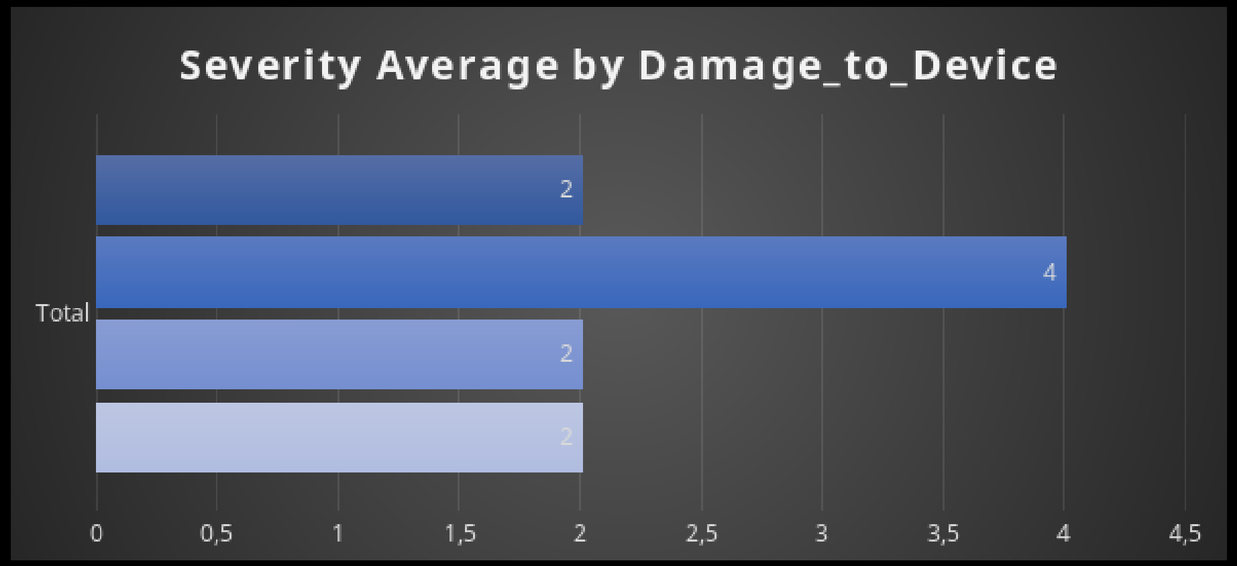
AÇÕES DE MITIGAÇÃO

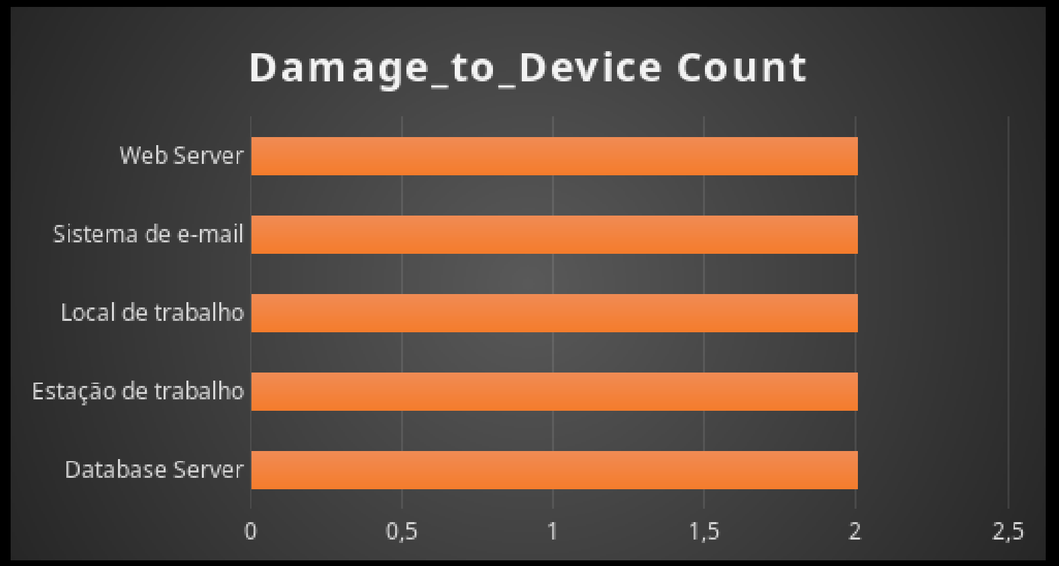
Cybershield DB

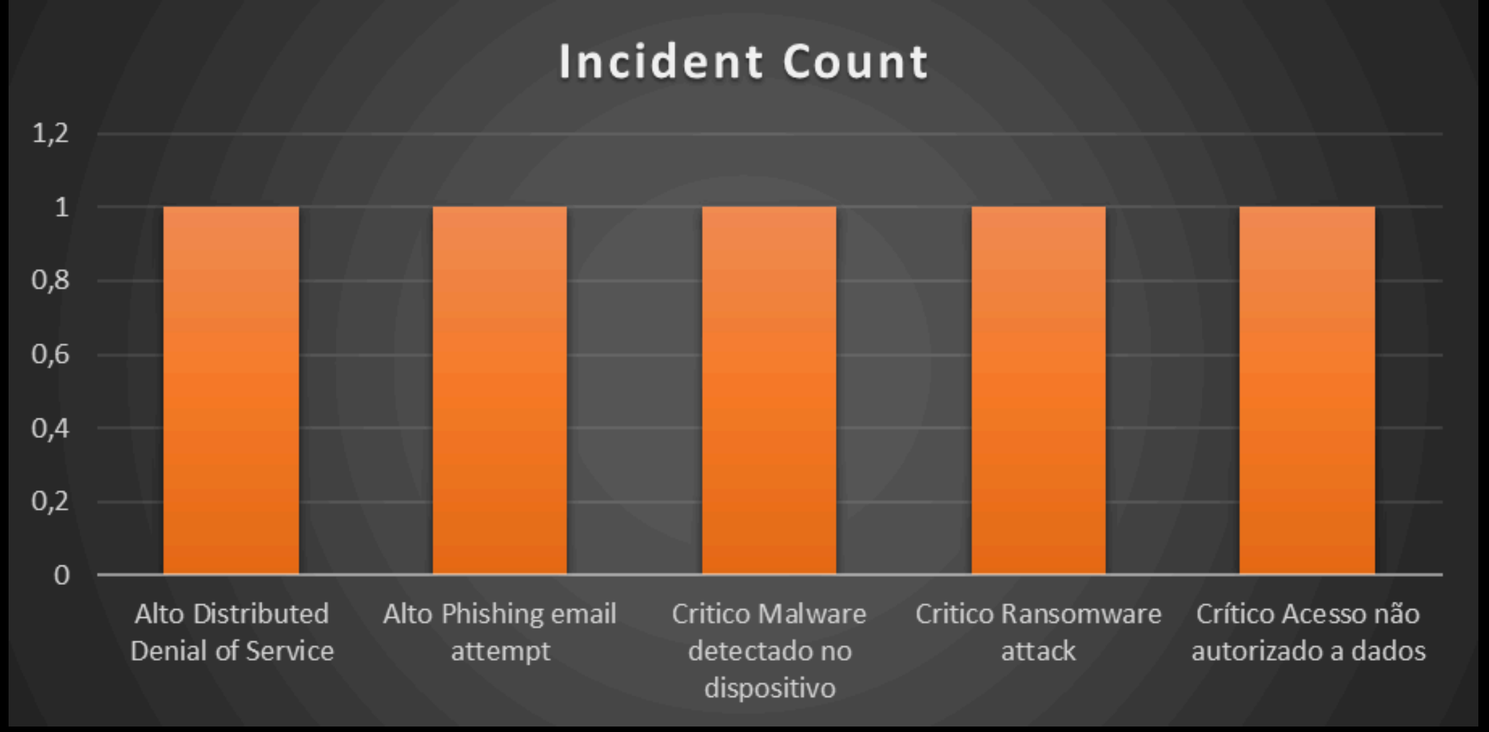
As Ações de Mitigação representam as medidas tomadas para minimizar o impacto e prevenir a recorrência de incidentes de segurança cibernética. Cada ação é registrada juntamente com a data em que foi realizada e sua eficácia em reduzir o risco associado ao incidente. Além disso, as ações são atribuídas a usuários específicos para garantir responsabilidade e acompanhamento adequado. O registro detalhado das ações de mitigação permite uma análise posterior para avaliar sua eficácia e identificar áreas de melhoria na resposta a incidentes e na segurança geral do sistema.

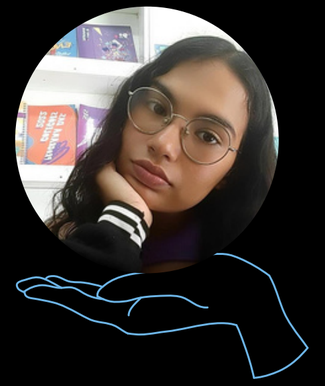


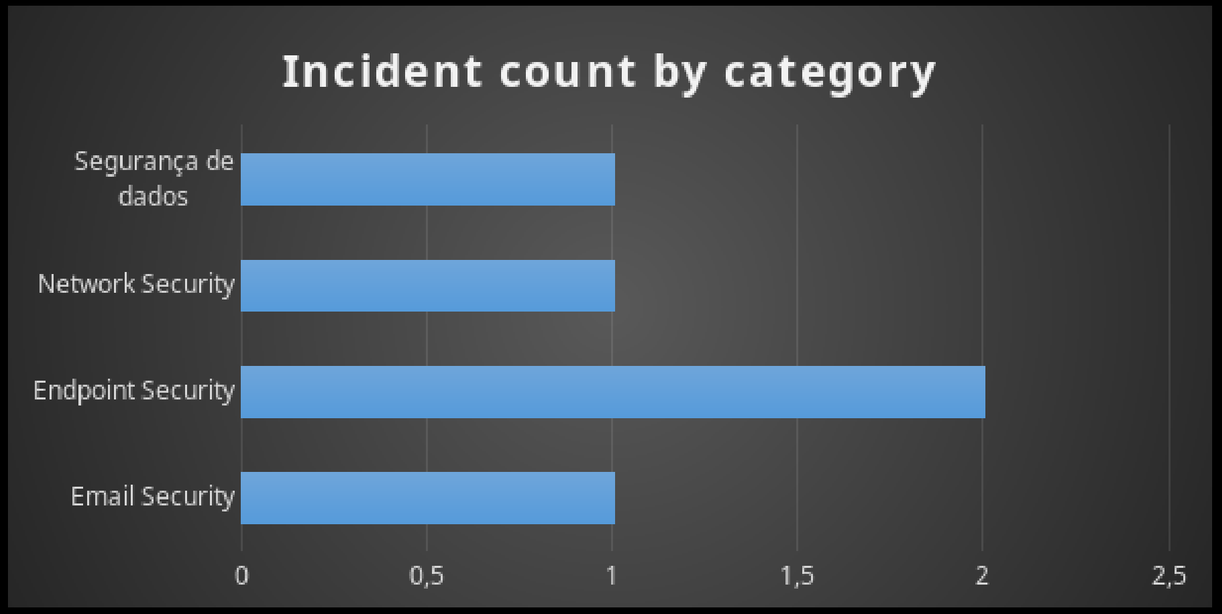

Number of incidents
1
2
3
4
5
6
7
8
9
10

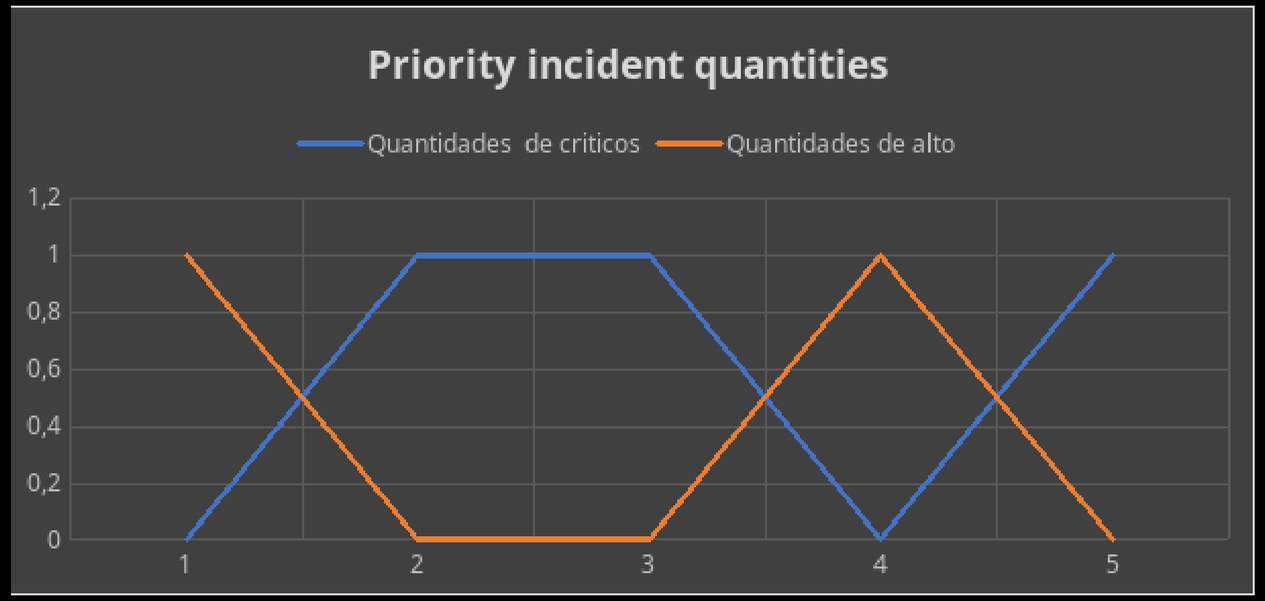

Severity Average by Damage_to_Device
Total
2
4
2
2
0
0,5
1
1,5
2
2,5
3
3,5
4
4,5


Damage_to_Device Count
Web Server
Sistema de e-mail
Local de trabalho
Estação de trabalho
Database Server
0
0,5
1
1,5
2
2,5

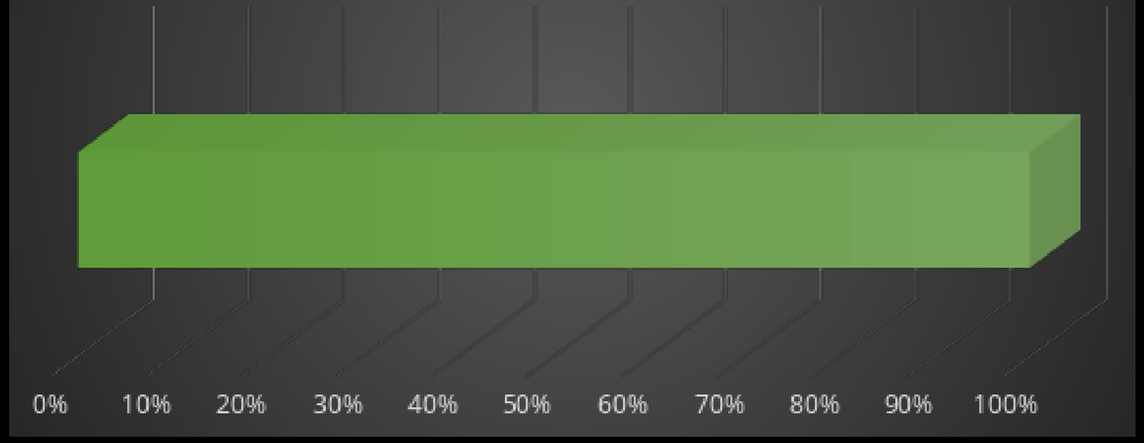

Incident Count
1,2
1
0,8
0,6
0,4
0,2
0
Alto Distributed Denial of Service
Alto Phishing email attempt
Critico Malware detectado no dispositivo
Critico Ransomware attack
Crítico Acesso não autorizado a dados




Incident count by category
Segurança de dados
Network Security
Endpoint Security
Email Security
0
0,5
1
1,5
2
2,5


Priority incident quantities
Quantidades de criticos
Quantidades de alto
1,2
1
0,8
0,6
0,4
0,2
0
1
2
3
4
5

Number of comments about the incident

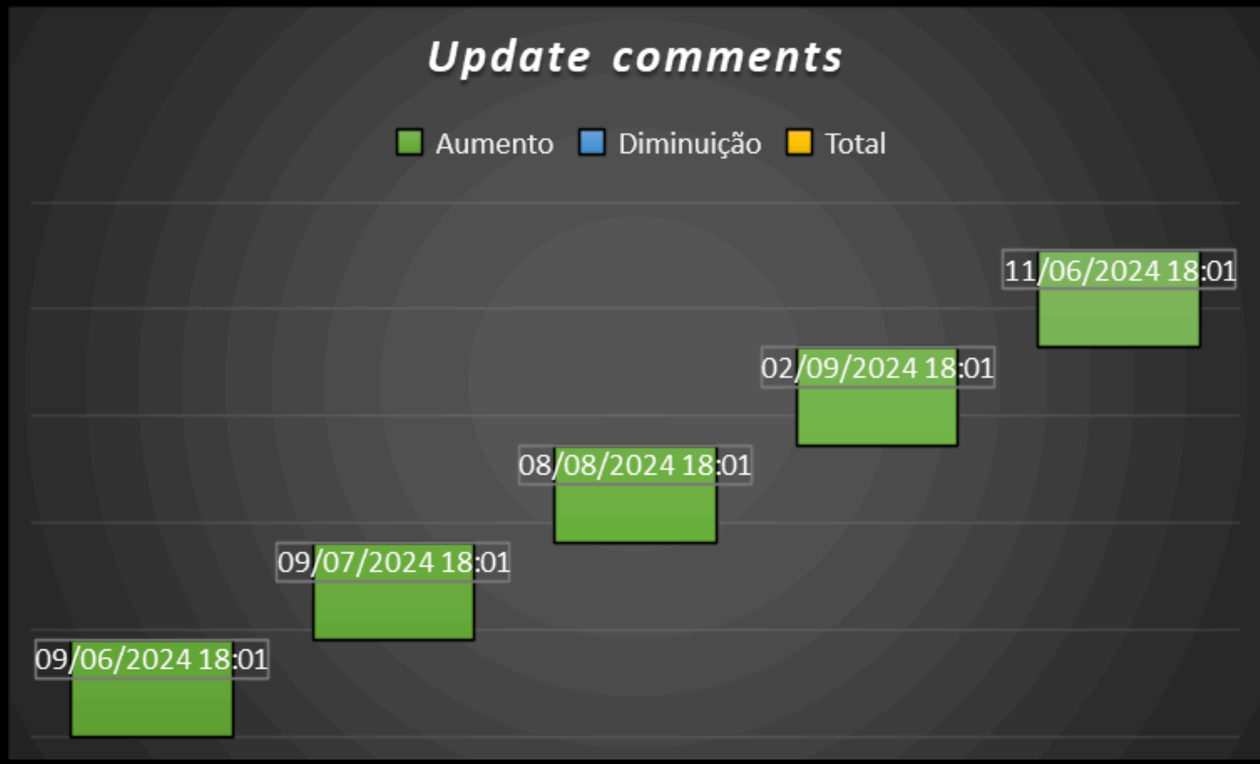


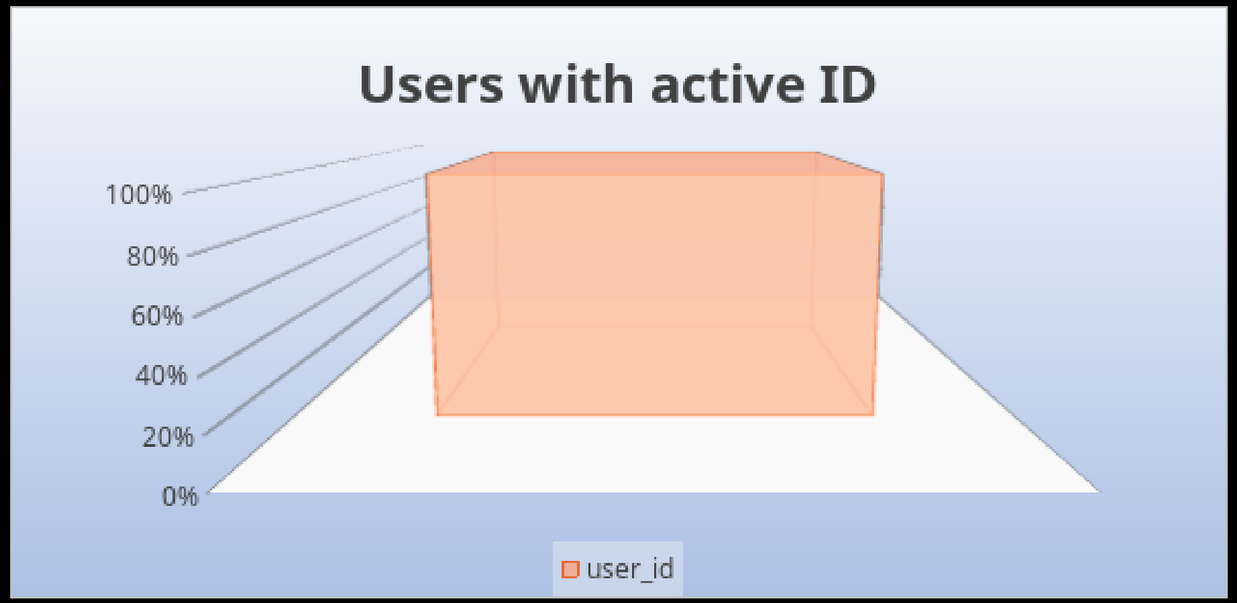
Creation data for create comment

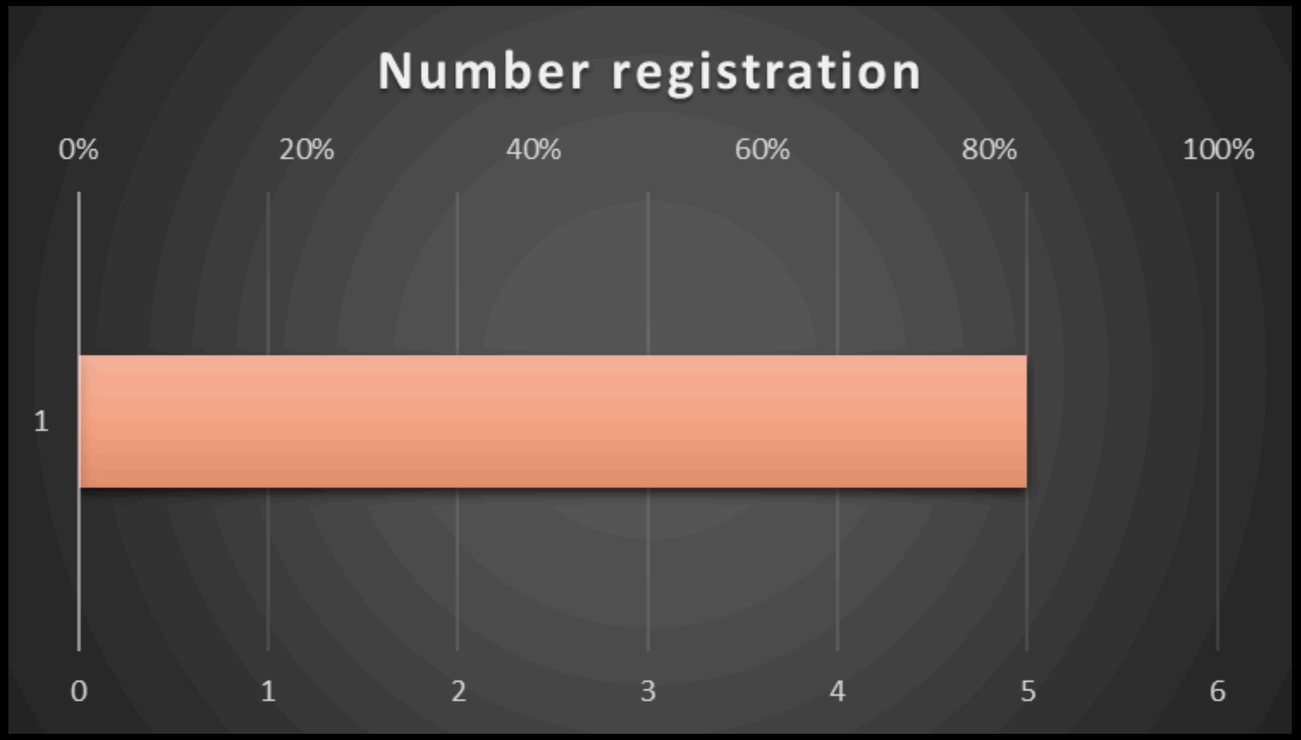
Createe

Investigando a origem do e-m...	09/05/2024 18:01
Verificação de malware no...	10/06/2024 18:01
Notificar as partes afetadas...	20/06/2024 19:01
Mitigação de ataques DDoS	17/06/2024 17:01
Restauração de arquivos a...	27/07/2024 18:01

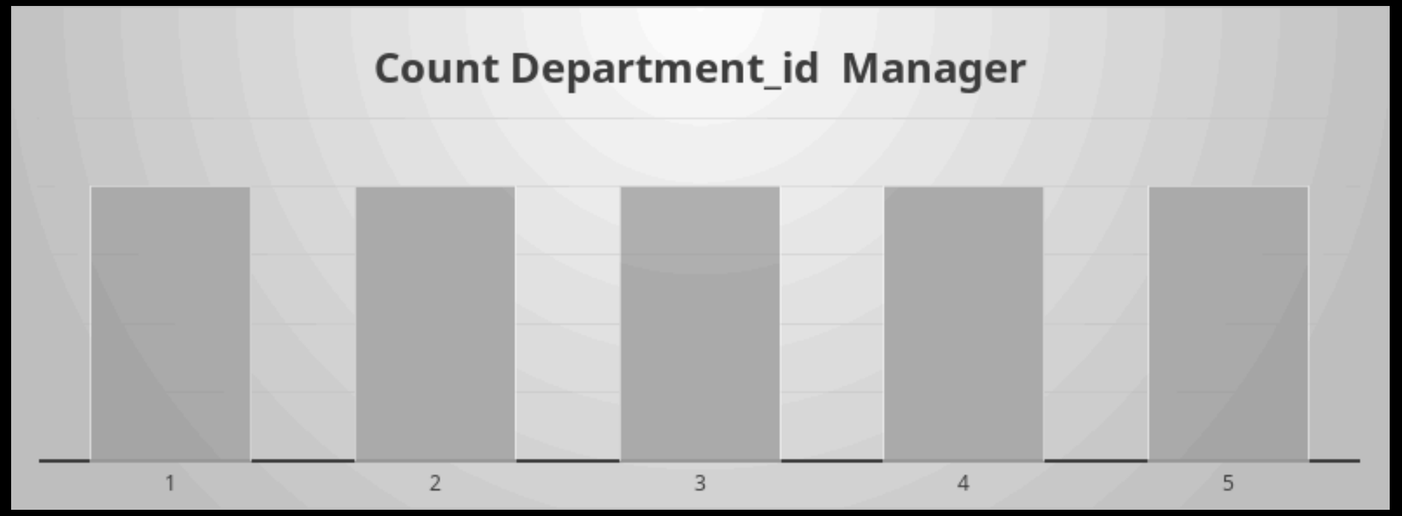
Update comments

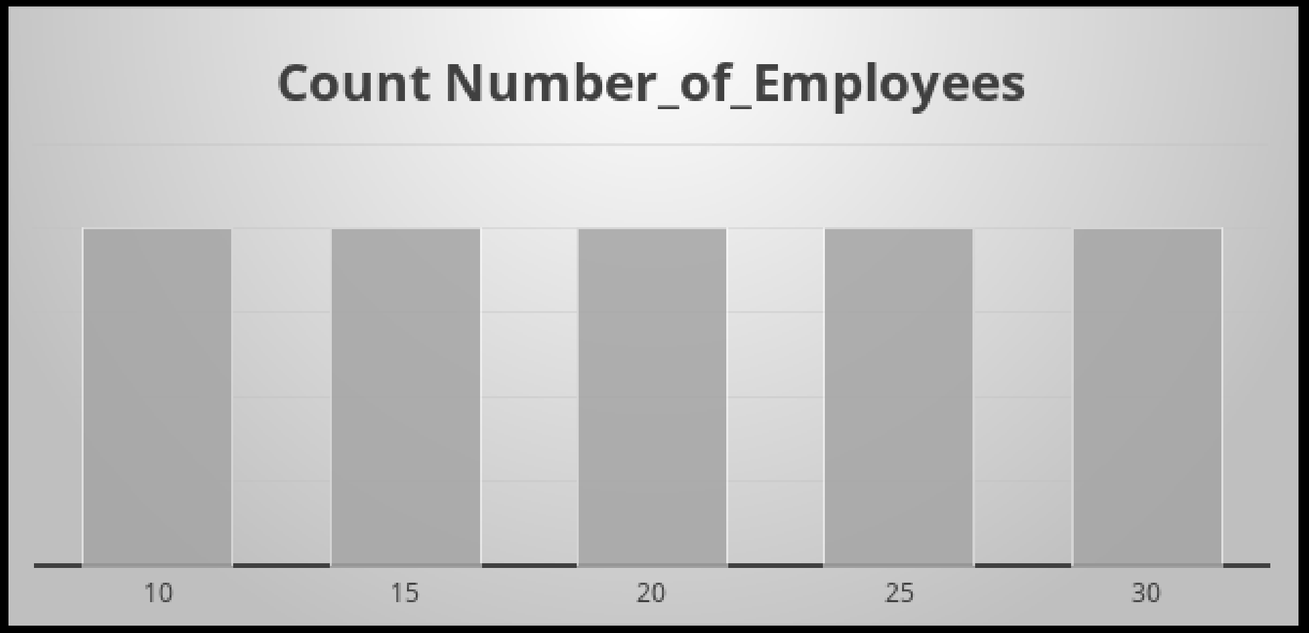


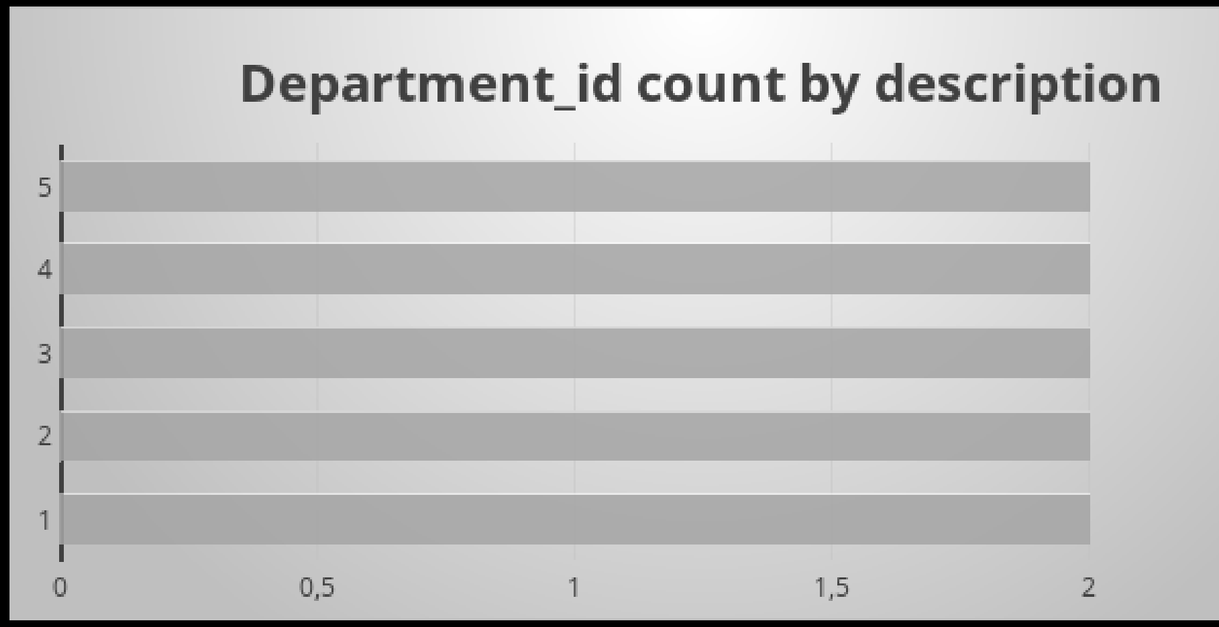

Users with active ID
100%
80%
60%
40%
20%
0%
user_id

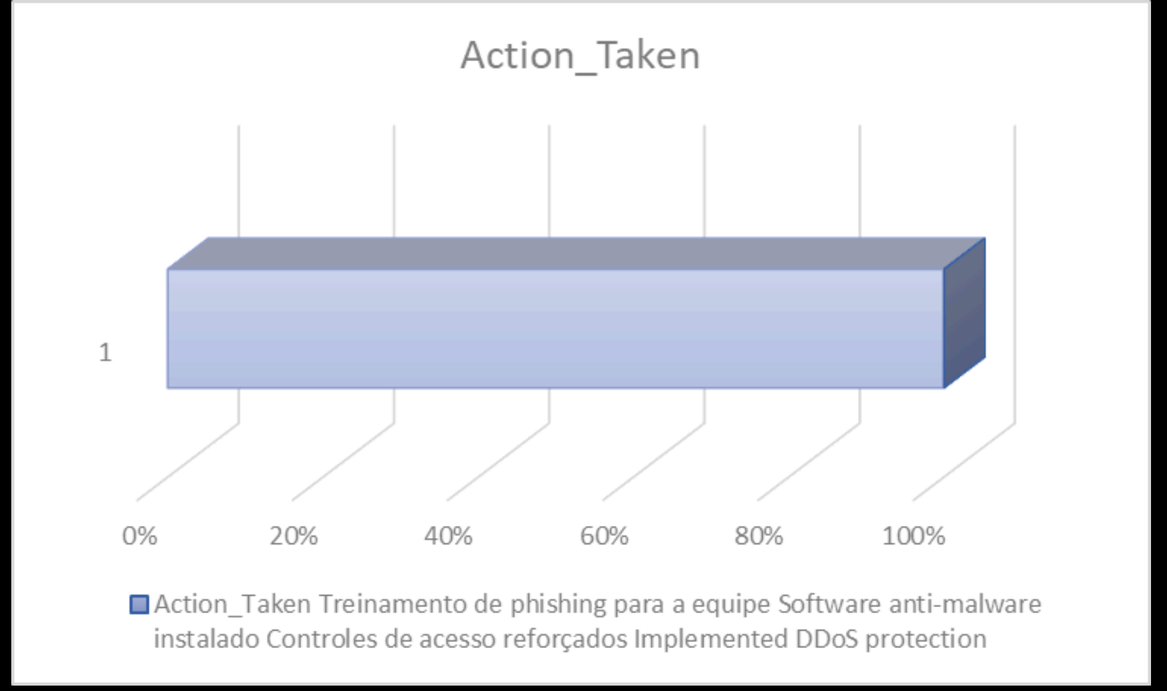

Number registration
0%
20%
40%
60%
80%
100%
1
0
1
2
3
4
5
6

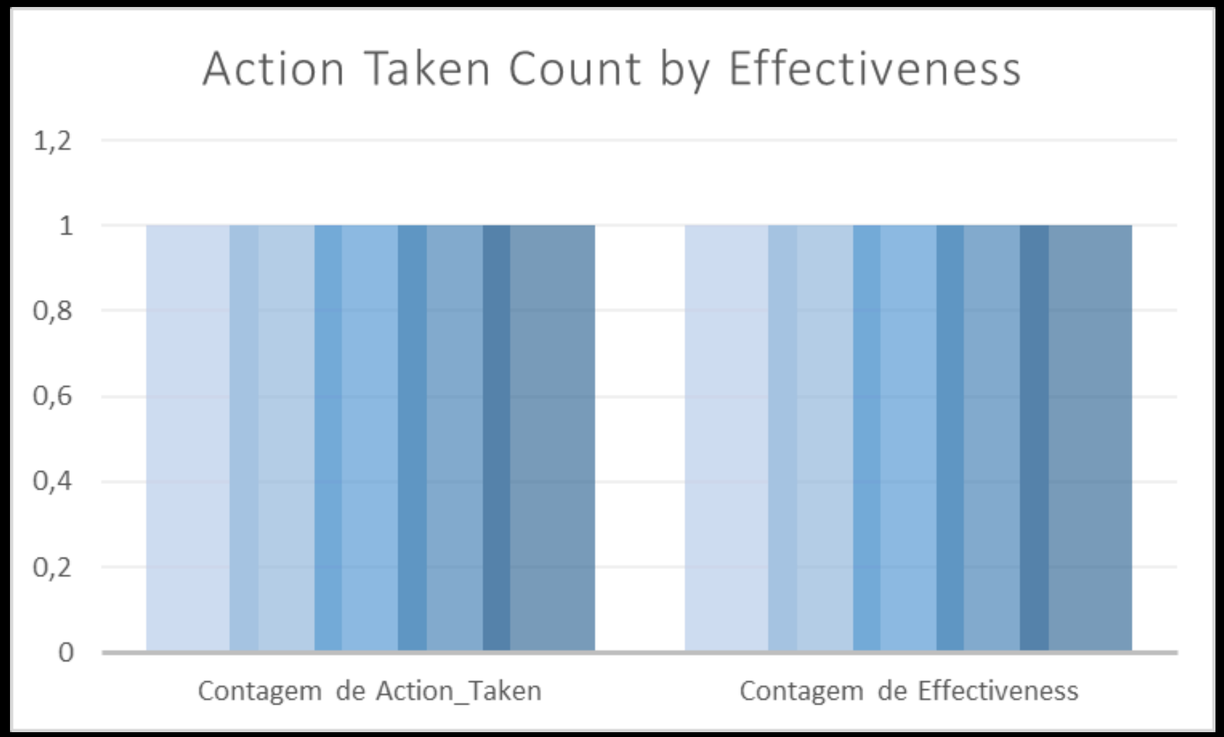

Email registration
5
4
3
2
1
0
1
2
3
4
5
Email

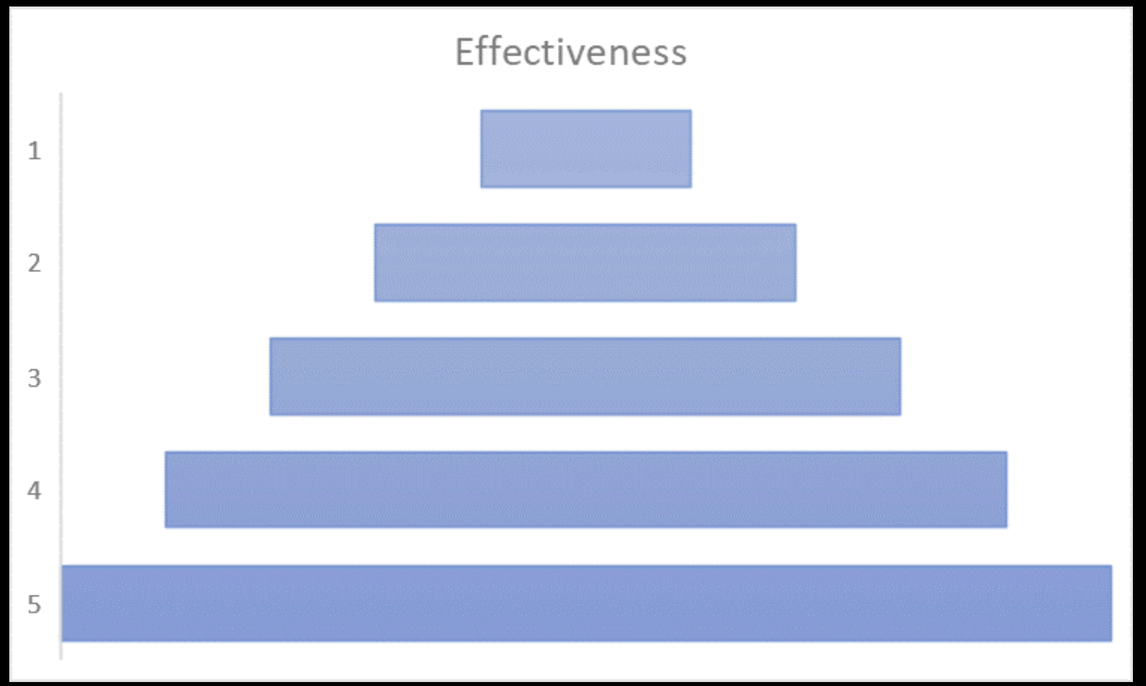

Count Department_id Manager
1
2
3
4
5


Count Number_of_Employees
10
15
20
25
30


Department_id count by description
5
4
3
2
1
0
0,5
1
1,5
2


Action_Taken
1
0%
20%
40%
60%
80%
100%
Action_Taken Treinamento de phishing para a equipe Software anti-malware instalado Controles de acesso reforçados Implemented DDoS protection


Action Taken Count by Effectiveness
1,2
1
0,8
0,6
0,4
0,2
0
Contagem de Action_Taken
Contagem de Effectiveness


Effectiveness
1
2
3
4
5

DBDIAGRAMA

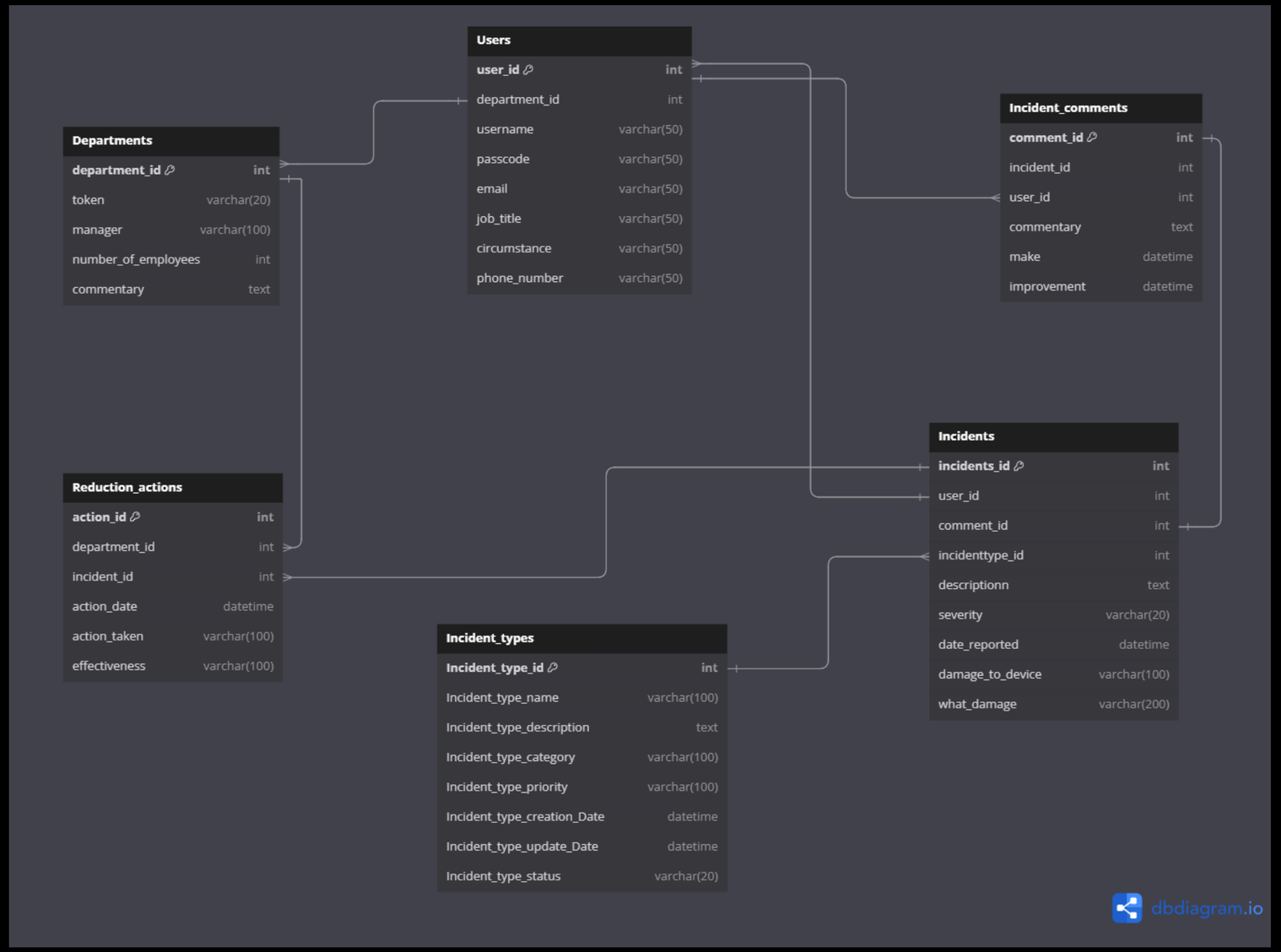
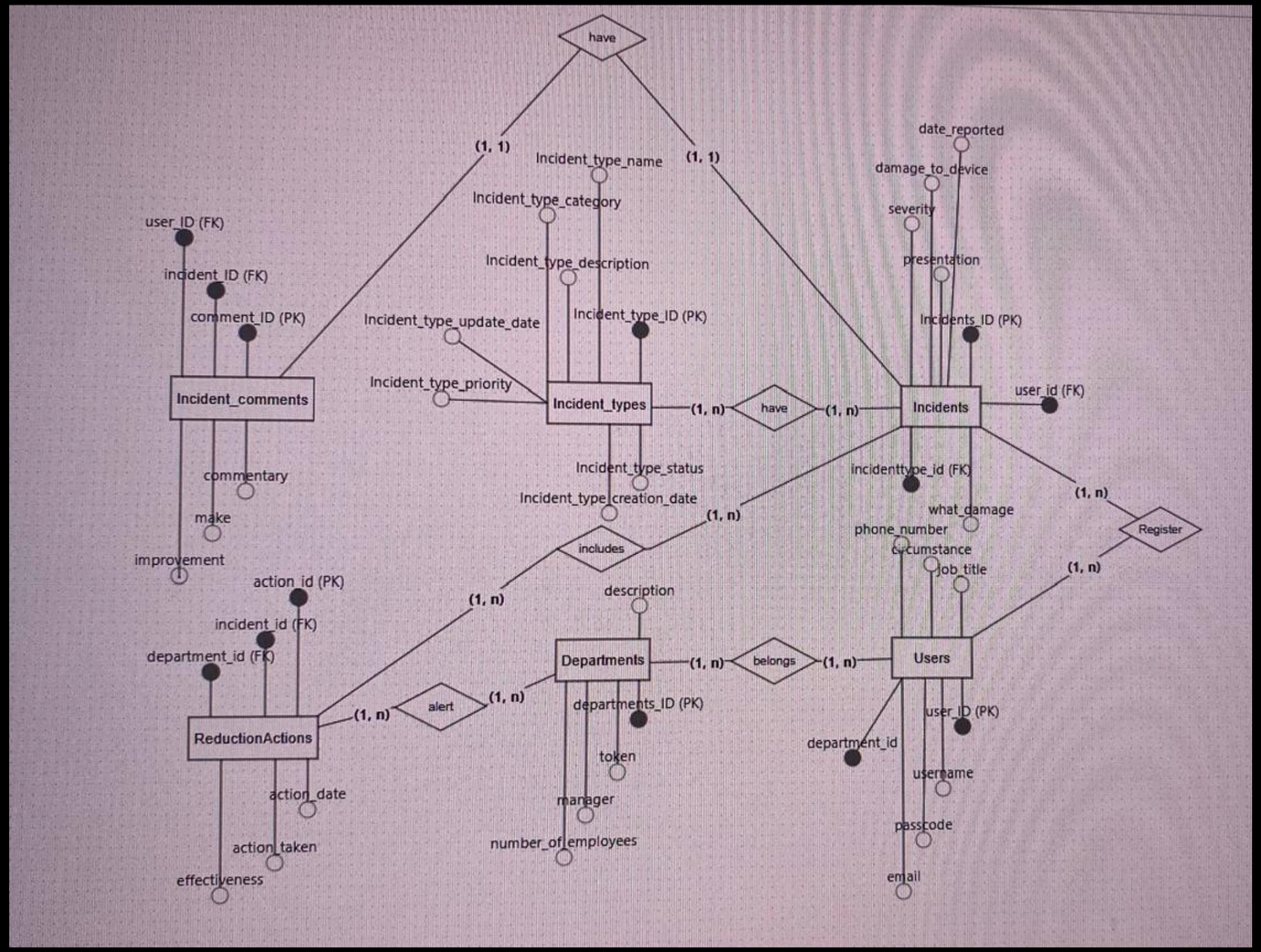

Users
user_id int
department_id int
username varchar(50)
passcode varchar(50)
email varchar(50)
job_title varchar(50)
circumstance varchar(50)
phone_number varchar(50)
Departments
department_id int
token varchar(20)
manager varchar(100)
number_of_employees int
commentary text
Incident_comments
comment_id int
incident_id int
user_id int
commentary text
make datetime
improvement datetime
Reduction_actions
action_id int
department_id int
incident_id int
action_date datetime
action_taken varchar(100)
effectiveness varchar(100)
Incidents
incidents_id int
user_id int
comment_id int
incidenttype_id int
descriptionn text
severity varchar(20)
date_reported datetime
damage_to_device varchar(100)
what_damage varchar(200)
Incident_types
Incident_type_id int
Incident_type_name varchar(100)
Incident_type_description text
Incident_type_category varchar(100)
Incident_type_priority varchar(100)
Incident_type_creation_Date datetime
Incident_type_update_Date datetime
Incident_type_status varchar(20)
dbdiagram.io

DIAGRAMA CONCEITUAL



Cybershield DB

DEMONSTRAÇÃO DO NOSSO BANCO DE DADOS