



Hackers do Bem – Fundamental
Prof. Fábio Carneiro de Castro
17/02/2026

Atividade Prática – Módulo 4

Aulas 1 e 2

Gabriel dos Santos Schmitz

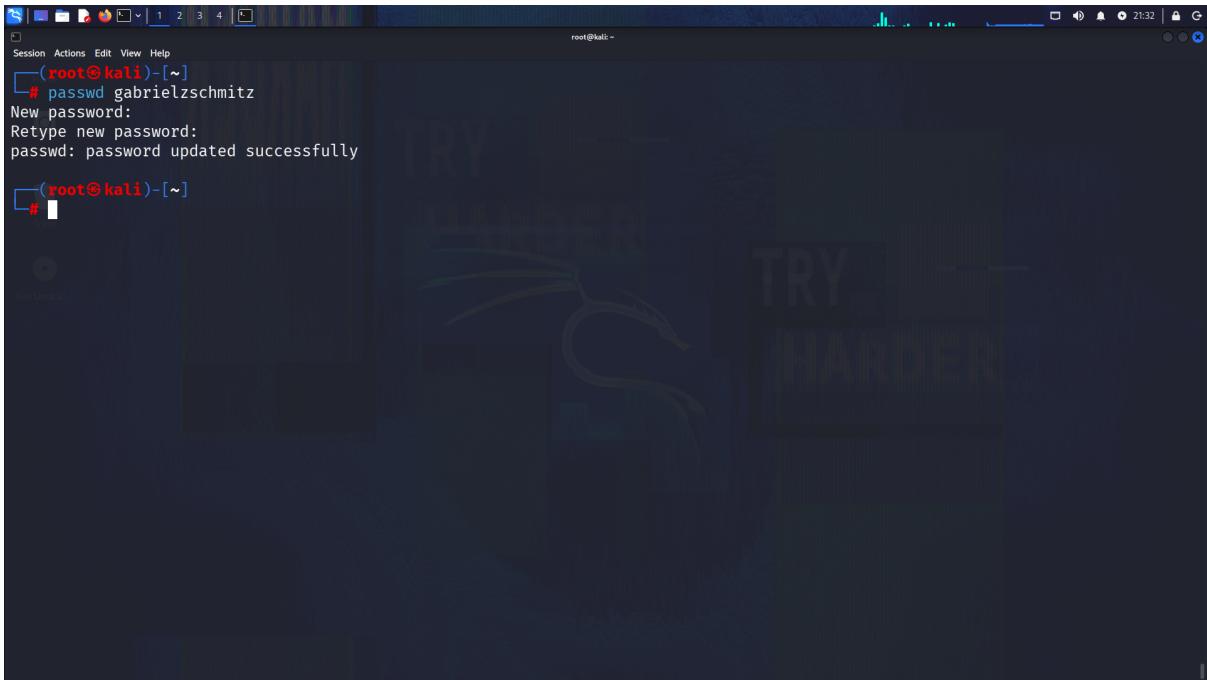
1 Introdução

Este documento apresenta as evidências práticas das atividades do Módulo 4 (Aulas 1 e 2) do Programa Hackers do Bem – Nível Fundamental, por meio dos prints solicitados, demonstrando a correta execução das tarefas propostas.

Conforme as orientações do curso, este documento reúne, em um único arquivo PDF, os seguintes registros obrigatórios: Atividade 4.1 (passo 7), Atividade 4.2 (passo 5), Atividade 4.3 (passo 10), Atividade 4.4 (passo 7) e Atividade 4.5 (passo 11), todos acompanhados de breve descrição explicativa, com o objetivo de facilitar a análise e avaliação por parte do instrutor.

2 Atividades

Atividade 4.1. Modificando os parâmetros de Controle de Autenticação no Kali Linux

A screenshot of a terminal window on Kali Linux. The window title is 'root@kali'. The terminal shows the following session:

```
Session Actions Edit View Help
└(root@kali)-[~]
# passwd gabrielzschmitz
New password:
Retype new password:
passwd: password updated successfully
└(root@kali)-[~]
#
```

The background of the desktop shows a dark image of a person wearing a graduation cap and gown, with the text 'TRY HARDER' visible.

Fig. 1: Alteração da senha do usuário no Kali Linux e autenticação com a nova credencial

Sobre:

Nesta atividade, foi realizado o processo de modificação de credenciais de autenticação no sistema Kali Linux, demonstrando o funcionamento do controle de acesso baseado em senha em ambientes Linux.

Inicialmente, foi verificado o usuário logado e o diretório de trabalho atual por meio dos comandos `whoami` e `pwd`, confirmando o contexto de execução do usuário `aluno` no diretório `/home/aluno`.

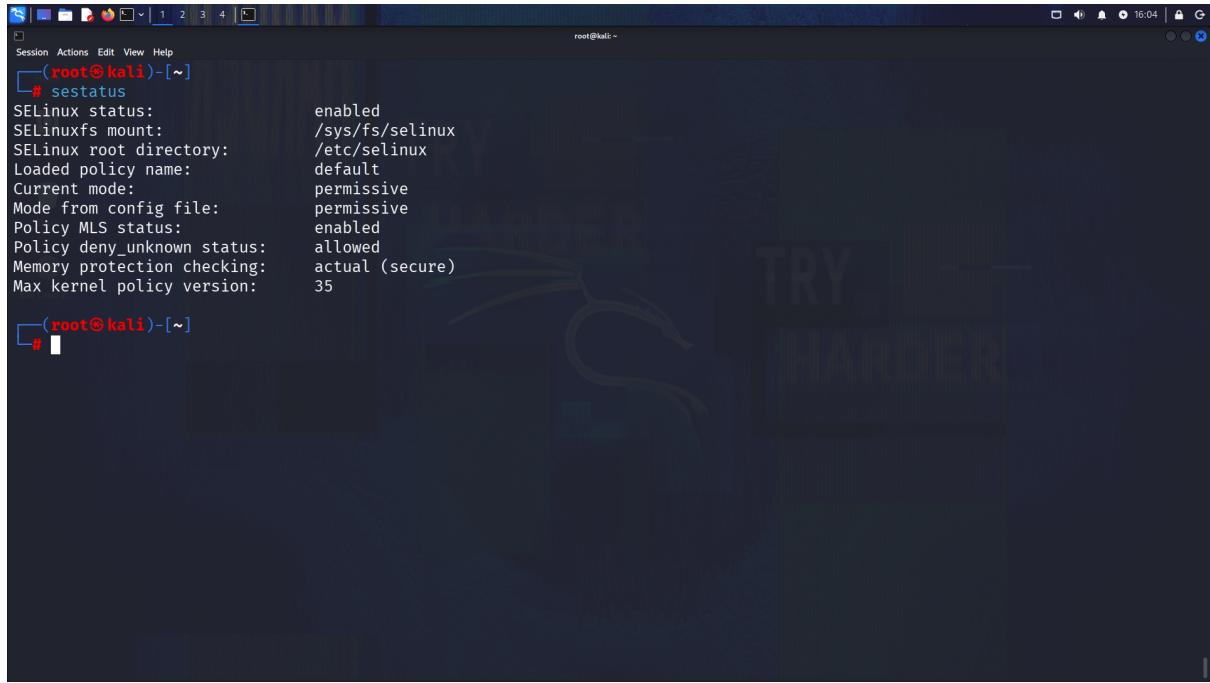
Em seguida, foram analisados os arquivos de configuração `/etc/passwd` e `/etc/group`, responsáveis por armazenar informações sobre usuários e grupos no sistema. Observou-se que o arquivo `/etc/passwd` contém dados estruturados em campos, como nome de usuário, UID, GID, diretório pessoal e shell padrão, enquanto o arquivo `/etc/group` define os grupos existentes e seus respectivos membros.

Posteriormente, foi realizada a alteração da senha do usuário `aluno` por meio da elevação de privilégios com o comando `sudo -i`, seguido do comando `passwd aluno`, definindo uma nova senha de autenticação.

Após a alteração, foi efetuado o encerramento da sessão e realizado novo acesso ao sistema via RDP, utilizando a senha atualizada, validando o sucesso do processo de modificação de credenciais.

Por fim, a senha foi restaurada ao valor original, garantindo a manutenção do ambiente conforme o estado inicial. Este procedimento evidenciou o controle de autenticação baseado em senha no Kali Linux e a importância da gestão segura de credenciais em sistemas operacionais.

Atividade 4.2. Explorando a ferramenta SELinux no Kali Linux



```
root@kali: ~] # sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                  permissive
Mode from config file:         permissive
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    35
root@kali: ~] #
```

Fig. 2: Verificação do status do SELinux no Kali Linux

Sobre:

Nesta atividade, foi realizada a exploração do SELinux (Security-Enhanced Linux), um mecanismo de segurança que implementa controle de acesso obrigatório (MAC) em sistemas Linux, permitindo a definição de políticas de segurança mais granulares sobre processos, arquivos e recursos do sistema.

Inicialmente, foi efetuada a elevação de privilégios utilizando o comando `sudo -i`, possibilitando a execução de tarefas administrativas. Em seguida, procedeu-se com a ativação do SELinux por meio do comando `selinux-activate`, que realizou a geração do arquivo de configuração do GRUB, responsável pelo carregamento do kernel com suporte às políticas de segurança do SELinux.

Após a ativação, o sistema foi reiniciado para aplicação das alterações. Durante o processo de inicialização, ocorre a etapa de *relabeling*, na qual os arquivos do sistema recebem rótulos de segurança apropriados, permitindo a aplicação correta das políticas definidas.

Com o sistema em execução, foi verificado o estado do SELinux utilizando o comando `sestatus`, confirmando que o mecanismo estava habilitado e operando em modo *permissive*, no qual as violações de política são registradas em log, sem bloqueio efetivo das ações.

Em seguida, foram analisadas as configurações de usuários do SELinux por meio do comando `semanage user -l`, que apresenta os rótulos de segurança, funções e níveis associados a cada usuário. Também foram verificadas as associações de login com o comando `semanage login -l`, evidenciando o mapeamento entre usuários do sistema e identidades do SELinux.

Posteriormente, foi examinada a lista de variáveis booleanas do SELinux com `semanage boolean -l`, permitindo identificar parâmetros que controlam o comportamento de diferentes serviços e aplicações. Além disso, foram listadas as definições de portas com o comando `semanage port -l`, relacionando tipos de políticas, protocolos e números de portas.

Por fim, foi realizada a desativação do SELinux por meio da edição do arquivo de configuração `/etc/selinux/config`, alterando o modo para `disabled`, seguida de reinicialização do sistema. A verificação final com o comando `sestatus` confirmou a desativação do mecanismo.

Esta atividade demonstrou o funcionamento do SELinux, suas configurações principais e a importância do controle de acesso baseado em políticas para o aumento da segurança em sistemas Linux.

Atividade 4.3. Criando um cofre de senhas com o KeePassXC no Kali Linux

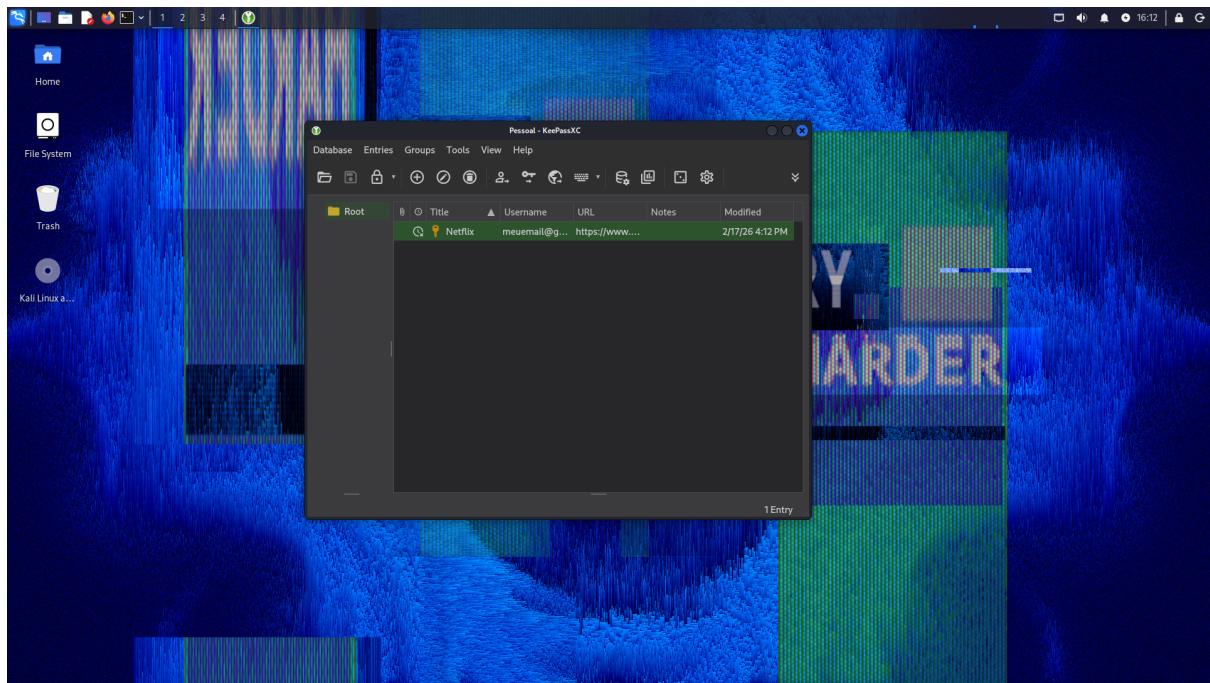


Fig. 3: Criação e gerenciamento de credenciais no KeePassXC

Sobre:

Nesta atividade, foi realizada a criação e manipulação de um cofre de senhas utilizando o KeePassXC, um gerenciador de senhas de código aberto que permite armazenar credenciais de forma segura por meio de criptografia avançada.

Inicialmente, o aplicativo foi executado no Kali Linux por meio do comando `keepassxc`, utilizando o usuário padrão do sistema, conforme recomendado. Em seguida, foi criado um novo banco de dados, denominado *Pessoal*, destinado ao armazenamento de credenciais.

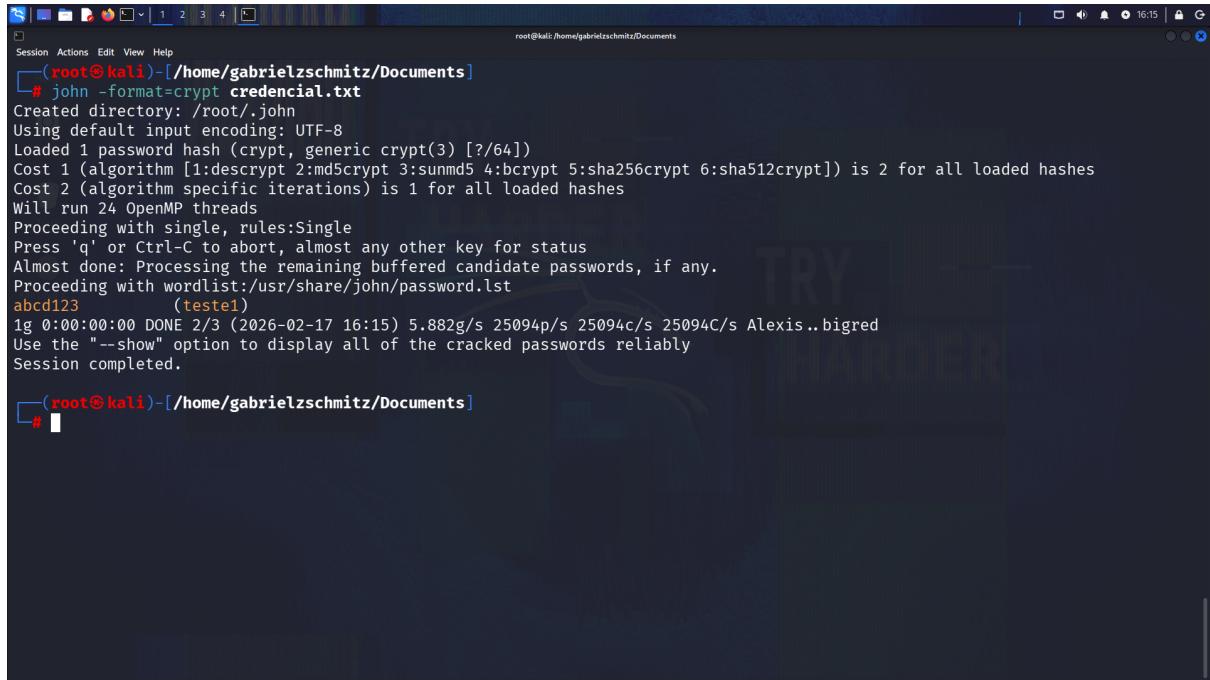
Durante a configuração do banco de dados, foi verificado o uso do algoritmo de criptografia AES de 256 bits, reconhecido por oferecer alto nível de segurança na proteção dos dados armazenados. Foi então definida uma senha mestra para o cofre, responsável por controlar o acesso às informações armazenadas.

Após a criação do banco de dados, o arquivo foi salvo no diretório **Documentos** com o nome **Senhas.kdbx**. Na interface do KeePassXC, foi adicionada uma nova entrada contendo informações de acesso, como título, nome de usuário, senha e URL, demonstrando o processo de armazenamento de credenciais.

Posteriormente, foi realizada a exclusão da entrada criada, evidenciando a capacidade de gerenciamento dos dados armazenados no cofre. Ao final, o arquivo do banco de dados foi removido do sistema por meio do comando `rm`, garantindo a limpeza do ambiente de testes.

Esta atividade demonstrou a utilização do KeePassXC para criação de cofres de senhas seguros, destacando a importância do uso de gerenciadores de credenciais para a proteção de informações sensíveis em ambientes digitais.

Atividade 4.4. Ataque de Dicionário Off-line contra credenciais no Kali Linux



The screenshot shows a terminal window titled '(root@kali)-[/home/gabrielzschmitz/Documents]'. The user has run the command 'john -format=crypt credencial.txt'. The output indicates that a directory '/root/.john' was created, using UTF-8 encoding, and loaded one password hash (crypt, generic crypt(3)). It shows the cost for different algorithms (md5crypt, sunmd5, bcrypt, sha256crypt, sha512crypt) and specifies 24 OpenMP threads. The process is almost done, processing buffered candidate passwords. A password 'abcd123' is found, corresponding to the user 'teste1'. The session completed successfully.

```
root@kali:/home/gabrielzschmitz/Documents
# john -format=crypt credencial.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 2 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 24 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
abcd123      (teste1)
1g 0:00:00:00 DONE 2/3 (2026-02-17 16:15) 5.882g/s 25094p/s 25094c/s 25094C/s Alexis..bigred
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

#
```

Fig. 4: Execução do ataque de dicionário com John the Ripper

Sobre:

Nesta atividade, foi realizada a exploração da ferramenta John the Ripper no Kali Linux, com o objetivo de demonstrar a execução de um ataque de dicionário off-line para descoberta de senhas a partir de hashes.

Inicialmente, foi obtido acesso privilegiado ao sistema utilizando o comando `sudo -i`. Em seguida, foi realizada a leitura do arquivo `/etc/shadow`, que armazena os hashes das senhas dos usuários do sistema, evidenciando a importância do controle de acesso a este arquivo por conter informações sensíveis.

Posteriormente, foi criado um novo usuário denominado `teste1`, com a senha previamente definida, utilizando o comando `useradd` associado à geração de hash por meio do `openssl`. Após a criação, foi possível visualizar o hash correspondente ao usuário no arquivo `/etc/shadow`.

O hash do usuário criado foi então copiado e armazenado em um arquivo `credencial.txt`, localizado no diretório `Documentos`, com o objetivo de utilizá-lo como entrada para o processo de quebra de senha.

Na etapa seguinte, foi executada a ferramenta John the Ripper com o comando `john -format=crypt credencial.txt`, que realizou um ataque de dicionário utilizando listas de palavras para tentar descobrir a senha correspondente ao hash informado.

Ao final da execução, a ferramenta foi capaz de identificar corretamente a senha associada ao usuário `teste1`, demonstrando a eficácia de ataques de dicionário contra senhas fracas ou previsíveis.

Por fim, o arquivo `credencial.txt` foi removido do sistema, finalizando o experimento. Esta atividade evidenciou a importância da adoção de senhas fortes e do uso de boas práticas de segurança para evitar a exposição de credenciais a ataques de quebra de senha.

Atividade 4.5. Gerenciando credenciais no Windows Server 2022

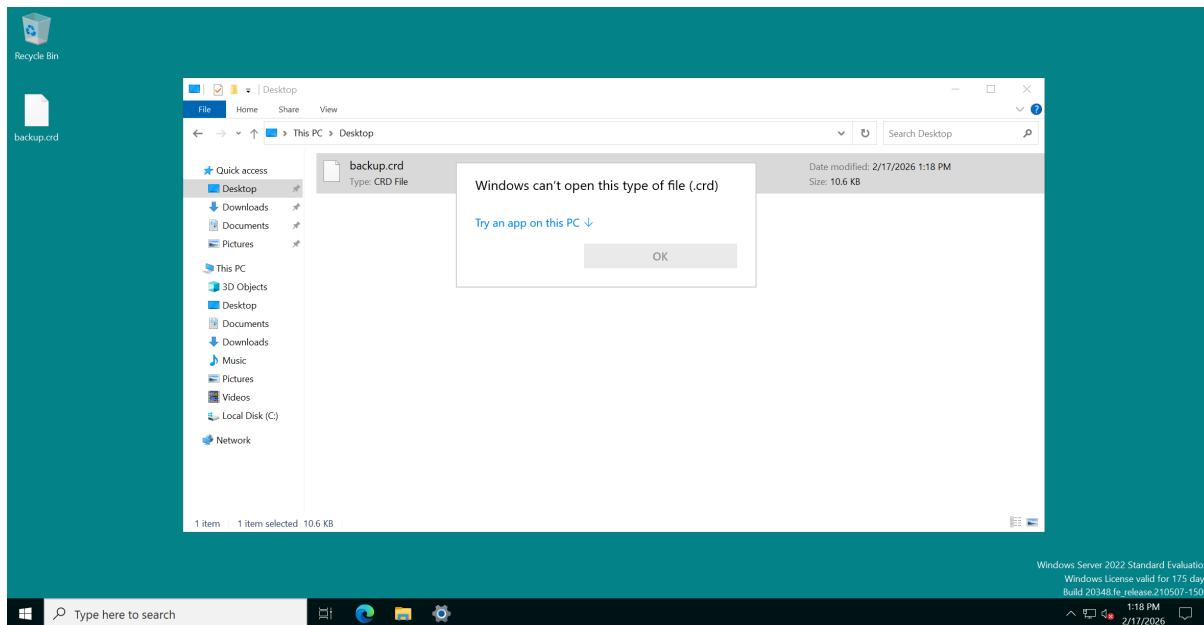


Fig. 5: Backup das credenciais realizado no Credential Manager

Sobre:

Nesta atividade, foi explorada a ferramenta Credential Manager do Windows Server 2022, utilizada para o gerenciamento seguro de credenciais armazenadas no sistema operacional.

Inicialmente, o acesso ao sistema foi realizado via RDP com as credenciais fornecidas. Em seguida, a ferramenta Credential Manager foi acessada por meio da barra de pesquisa do sistema.

Dentro da interface da ferramenta, foram analisadas as seções de credenciais disponíveis. Na aba *Web Credentials*, foi possível visualizar as credenciais relacionadas a acessos em páginas web, que podem incluir usuários e senhas salvos no sistema. Já na aba *Windows Credentials*, foram observadas diferentes categorias de credenciais, como credenciais do Windows, baseadas em certificado e genéricas, utilizadas para autenticação em serviços, aplicações e redes.

Posteriormente, foi realizado o processo de backup das credenciais armazenadas. Para isso, utilizou-se a opção *Back up Credentials*, definindo o diretório Desktop como local de destino e atribuindo o nome *backup* ao arquivo gerado.

Durante o procedimento, foi necessário confirmar a operação utilizando a sequência de segurança *Ctrl + Alt + Delete*, além de definir uma senha de proteção para o arquivo de backup. Após a confirmação, o sistema indicou que o backup foi concluído com sucesso.

Ao final, verificou-se a criação do arquivo *backup.crd* na área de trabalho, evidenciando a conclusão do processo. Por questões de segurança, o arquivo foi removido do sistema, finalizando a atividade.