UNIVERSIDADE FEDERAL DE SANTA CATARINA · SeTIC

CARTILHA DE

SEGURANÇA DA INFORMAÇÃO

Boas práticas para servidores e professores da UFSC

Do curso “Segurança da Informação e Certificação Digital”

Henrique Ribeiro

Gestor de Segurança da Informação · SeTIC/UFSC

Cartilha de Segurança da Informação

Boas práticas para servidores e professores da UFSC

Realização

SeTIC, Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação · UFSC

Autoria e conteúdo

Henrique Ribeiro, Analista de Tecnologia da Informação (CSS/SeTIC/SEPLAN) · Gestor de Segurança da Informação da UFSC (Portaria nº 1799/2025/GR)

Origem

Material derivado do curso de capacitação “Segurança da Informação e Certificação Digital” (20h, CCP/DDP/PRODEGESP, 2026), Aulas 1–5 (Certificação Digital, com Fernando Lauro Pereira) e Aulas 6–10 (Segurança da Informação).

Base normativa

LGPD (Lei nº 13.709/2018) · LAI (Lei nº 12.527/2011) · Lei nº 8.112/1990 · IN GSI/PR nº 01/2020 e nº 03/2021 · Decretos nº 12.572/2025 (PNSI) e nº 12.573/2025 (E-Ciber) · Portaria SGD/MGI nº 9.511/2025 (PPSI) · Resolução CD/ANPD nº 15/2024.

Apresentação

Esta cartilha nasceu de uma constatação simples, repetida ao longo de dez encontros de capacitação: a segurança da informação da Universidade não mora nos servidores de rede da SeTIC, mora na mesa de cada servidor e de cada professor. O firewall protege o perímetro técnico; quem protege o restante é você.

O material resume, em linguagem direta e sem tecniquês, as melhores práticas trabalhadas na segunda metade do curso “Segurança da Informação e Certificação Digital”: senhas e identidade digital, golpes por e-mail, redes e dispositivos, proteção de dados pessoais (LGPD) e resposta a incidentes.

Use-a como material de consulta rápida: cada seção fecha com o essencial em uma caixa, e a última página traz os 12 hábitos do servidor seguro, para imprimir e colar ao lado do monitor.

> **COMO LER ESTA CARTILHA**
>
> **Caixas laranja** trazem a regra de ouro de cada tema.
>
> **Caixas vermelhas** são alertas: o que nunca fazer.
>
> **Caixas azuis** indicam o caminho institucional: quem acionar e como.

1 Você é o perímetro

Por que segurança da informação é assunto seu, e não só da TI.

Durante décadas, proteger informação era proteger um prédio: firewall, antivírus, sala trancada. Esse mundo acabou. Hoje o trabalho viaja com você, no notebook, no celular, no e-mail aberto no ônibus. O perímetro de segurança da UFSC deixou de ser um muro técnico e passou a ser o comportamento de cada pessoa que manipula informação institucional.

E há quem se interesse por essa informação: em 2025, o custo médio de uma violação de dados no Brasil chegou a R$ 7,19 milhões (IBM/Ponemon), o país está entre os mais atacados do mundo e os ataques à rede acadêmica cresceram 56% em um ano (RNP). Universidades guardam um pacote raro: dados pessoais em massa, pesquisa inédita, folha de pagamento e visibilidade pública.

O que estamos protegendo

- **Dados pessoais de estudantes e servidores**, matrículas, históricos, folha, saúde.
- **Processos administrativos, contratos e licitações**, inclusive disciplinares e judiciais.
- **Pesquisa em andamento**, dados não publicados valem ouro (e espionagem existe).
- **Credenciais e acessos**, a senha que abre tudo isso.

Os três pilares: C · I · D

Toda decisão de segurança protege um destes três princípios, que já existiam no tempo do telégrafo, quando alguém podia grampear, adulterar ou cortar o fio:

> **A REGRA DE OURO DA SEÇÃO**
> O ser humano não é o elo mais fraco, é o elo mais consciente. Um software não desconfia de um e-mail estranho. Você desconfia. Esta cartilha existe para fortalecer essa intuição.

2 Senhas: a chave da sua identidade digital

Uma credencial abre dezenas de portas. Trate cada senha como uma chave, e a idUFSC como a chave-mestra.

Senha forte: comprimento vence complexidade

FAÇA ASSIM (passphrase)

- Frase longa de palavras simples: “três cabras subiram morro azul”
- Mais de 5 palavras, fácil de lembrar, séculos para quebrar
- Única para cada serviço importante
- Padrão NIST, adotado por bancos e governos

NUNCA FAÇA

- P@ss0rd! e variações “complexas” curtas, caem em segundos
- Nome + ano (Henrique69), time + número (Avaí1923)
- “ufsc” + qualquer coisa; 123456, qwerty
- Nome de filho, pet, cônjuge ou datas pessoais

O cofre digital (gerenciador de senhas)

Ninguém decora 90 senhas, e é por isso que a maioria repete. A solução é decorar UMA: a senha-mestra de um cofre digital, que guarda todas as outras. Atenção para não confundir:

COFRE DIGITAL, abre portas

- Guarda credenciais: senhas, códigos, passkeys
- Nativos: Gerenciador do Google, Senhas (Apple), Samsung Pass
- Dedicados: Bitwarden (nuvem, gratuito, código aberto) e KeePassXC (local)
- Uma chave-mestra protege todas as outras

CARTEIRA DIGITAL, paga e comprova

- Guarda valores e documentos: cartões, ingressos, CNH Digital, e-Título
- Google/Apple/Samsung Wallet, gov.br
- Não é lugar de senha
- O celular virou chaveiro E carteira: proteja o aparelho

> **A SENHA-MESTRA**
> É a única que realmente importa, e não tem “esqueci minha senha”. Use uma frase-senha longa (5+ palavras), ative a recuperação por e-mail quando existir e anote em papel guardado em local fisicamente seguro (gaveta com chave). O próprio fabricante recomenda.

MFA: a segunda fechadura

Múltiplo Fator de Autenticação (MFA) é exigir duas provas: a senha (algo que você sabe) e um código no celular (algo que você tem). Google e Microsoft estimam que o MFA bloqueia 99% dos ataques de uso indevido de credenciais, é a ação isolada de maior impacto na sua segurança.

- **Comece pelo e-mail pessoal**, é ele que recebe os “esqueci minha senha” de todo o resto.
- **Prefira app autenticador (TOTP)**, Google/Microsoft Authenticator, Aegis (Android), Raivo (iOS). SMS é melhor que nada, mas vulnerável ao golpe do chip clonado.
- **Na UFSC AINDA não há MFA corporativo**, o hábito formado agora nas contas pessoais estará pronto quando a Universidade adotar.

A idUFSC é a chave-mestra institucional

E-mail, sistemas administrativos, Moodle, CAGR, eduroam, VPN, periódicos CAPES, Assin@UFSC: uma credencial, dezenas de portas. Por isso ela merece tratamento especial: única (não repetida em nenhum outro serviço), longa e guardada no cofre.

ALERTA MÁXIMO

Ninguém da SeTIC pede a sua senha. Nunca. Quem pedir está te enganando.

Compartilhar conta institucional, mesmo com colega de confiança, destrói a rastreabilidade que a LGPD exige da Universidade.

HÁBITO DE UM SEGUNDO

Levantou, bloqueou: Win + L (Windows) · Control + Command + Q (Mac). Em computador compartilhado: nunca "lembrar senha" no navegador e logout completo a cada turno.

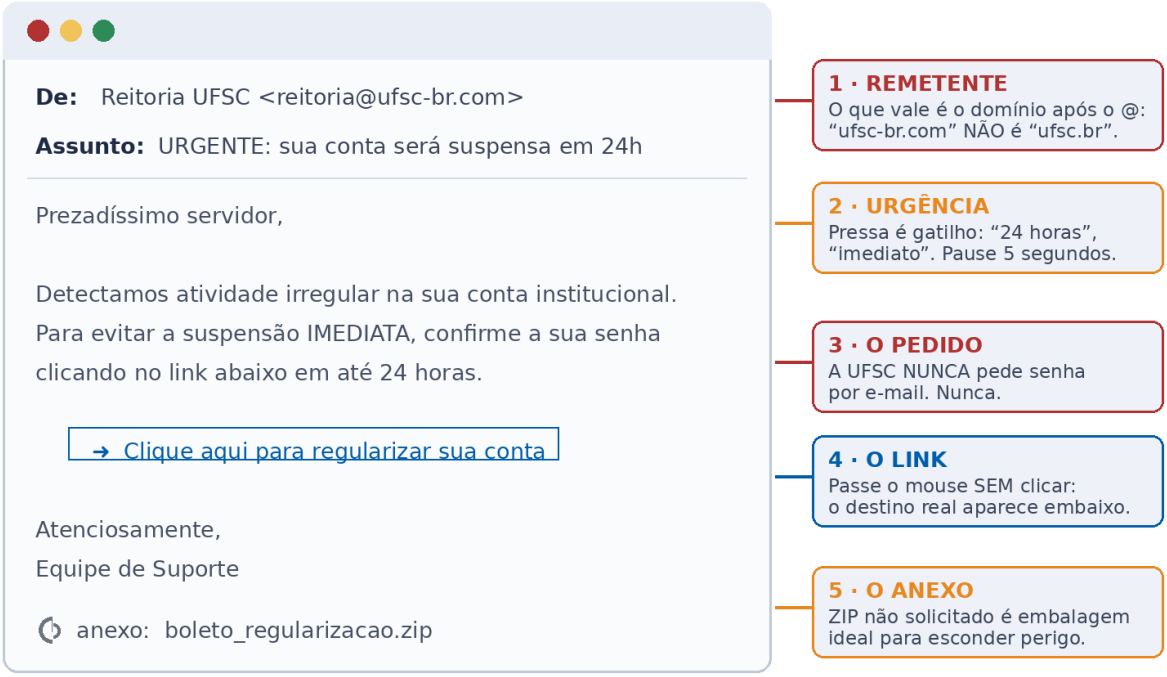
3 Phishing: o golpe que chega educado

A imensa maioria das invasões começa com uma mensagem bem-educada. Vítima de phishing não é gente desatenta, é gente com pressa.

Os 4 gatilhos psicológicos

- **Autoridade,** "o reitor mandou": hierarquia para curto-circuitar seu julgamento.
- **Urgência,** "em 24 horas": quando o e-mail diz AGORA, você age sem pensar. E-mail urgente é, por definição, suspeito.
- **Escassez,** "últimas 3 vagas": medo de perder a oportunidade.
- **Reciprocidade,** "oferta exclusiva para você": o favor que pede retorno.

Anatomia de um e-mail malicioso



O QUE A UFSC NUNCA PEDE POR E-MAIL

Confirmar ou “validar” a sua senha em um link.

Transferência urgente para “liberar pagamento”.

Abrir boleto ou comprovante em anexo não solicitado.

Recebeu um pedido desses? É golpe. Reporte e apague.

O golpe também liga e manda mensagem

- **Vishing (voz):** “aqui é da SeTIC, preciso da sua senha para manutenção”, com IA, clonam até voz de chefia.
- **Smishing (SMS/WhatsApp):** “Receita Federal: CPF irregular”, “oi mãe, troquei de número”.
- **Quishing (QR code):** adesivo falso por cima do QR original em balcões e eventos.
- **Fraude do fornecedor:** “segue nova conta para depósito”, toda mudança bancária exige confirmação por canal independente (telefone conhecido, não o do e-mail).

Caí no golpe. E agora?

Cair no golpe não é o fim, esconder que caiu é. Calma e velocidade, simultaneamente:

- Troque IMEDIATAMENTE a senha do serviço afetado, e de onde ela se repetia.
- Se envolveu conta institucional, avise a SeTIC na hora (https://chamados.setic.ufsc.br).
- Encaminhe o e-mail suspeito como ANEXO (preserva o cabeçalho técnico).
- Não apague as evidências: prints e mensagens ajudam a triagem.

A REGRA DE OURO DA SEÇÃO

Pause antes de clicar. O atacante depende da sua pressa, cinco segundos de dúvida derrubam a maioria dos golpes. Se o e-mail é urgente, geralmente é golpe.

4 Redes e dispositivos: o caminho e a bagagem

A informação viaja, pelo Wi-Fi, pela VPN, no notebook e no celular. Proteja o caminho e a bagagem.

Em qual rede confiar?

PODE USAR COM TRANQUILIDADE	TRATE COMO HOSTIL
• Rede cabeada/Wi-Fi da UFSC no campus • eduroam, em qualquer instituição do mundo, com a credencial idUFSC • Sua rede doméstica com senha forte no roteador • Confie na rede, mas desconfie dos links	• “Free Wi-Fi” de café, hotel, aeroporto, evento • Você não sabe QUEM opera o roteador • Evil twin: rede falsa com nome idêntico à legítima • Sem VPN, é como ler seus documentos em voz alta num bar

VPN UFSC, O TÚNEL CIFRADO

Use sempre que: estiver fora do campus E acessando sistemas administrativos, periódicos CAPES ou qualquer dado institucional.

Pode dispensar: dentro do campus, ou em uso estritamente pessoal.

Como saber se está ativa: o seu IP passa a ser da faixa da UFSC (guia completo no portal da SeTIC).

Checklist do dispositivo (uma vez por aparelho)

- **Atualizações automáticas ligadas**, a diferença entre invadido e não invadido costuma ser UMA atualização atrasada.
- **Antivírus ativo**, no Windows, o Defender basta.
- **Disco criptografado**, BitLocker (Windows), FileVault (Mac), LUKS (Linux).
- **Bloqueio automático de tela**, e senha de tela forte no celular (nada de 0000).
- **Conta separada para o trabalho**, família e filhos não usam o perfil funcional. Não é desconfiança: é dever institucional.
- **Localização e apagamento remoto habilitados**, para o caso de perda ou furto.

Backup: a regra 3-2-1

Sistemas institucionais, e-mail UFSC e nuvem corporativa são responsabilidade da SeTIC. O que vive só no SEU computador é responsabilidade sua:

Para o que é importante na vida — fotos de família, documentos digitalizados, a tese.

PERDEU OU FURTARAM O DISPOSITIVO?

É incidente, não azar: reporte na hora à SeTIC, troque as senhas das contas que estavam ativas nele e acione a localização/apagamento remoto.

5 LGPD: o dado é das pessoas

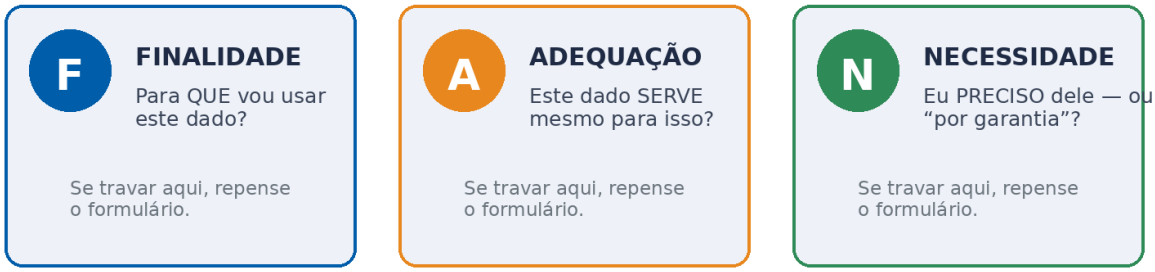
Dados pessoais não são da Universidade. São das pessoas, a Universidade é depositária, e guarda o dado como quem guarda um bem que não é seu.

O elenco da lei

- **Titular**, a pessoa dona do dado: estudante, servidor, candidato, fornecedor.
- **Controlador**, quem decide como tratar: a UFSC. No balcão, você age em nome dela.
- **Operador**, quem trata em nome do controlador: sistemas e empresas contratadas.
- **Encarregado (DPO)**, a ponte: recebe pedidos de titulares, orienta as áreas e dialoga com a ANPD.

Base legal, não consentimento

No setor público, a LGPD raramente depende de consentimento: tratamos dados por obrigação legal e para executar políticas públicas, matrícula, folha, concurso. A contrapartida é o dever de transparência e de coletar apenas o necessário. Antes de qualquer coleta, aplique o filtro:



Três perguntas antes de QUALQUER coleta de dado pessoal.

Exemplo clássico: formulário de presença em evento pedindo CPF, RG, raça e religião. Para confirmar presença bastam nome e e-mail; para emitir certificado, nome e CPF. Cada campo a mais é risco a mais, e a LGPD chama isso de minimização.

Na universidade pública

- **LAI convive com LGPD**, a transparência ativa continua; publica-se o necessário sem expor dado pessoal além da finalidade.
- **Pesquisa acadêmica tem base própria**, a universidade é órgão de pesquisa (art. 5º, XVIII), com anonimização sempre que possível.
- **Papel também é dado pessoal**, armário com chave, descarte na fragmentadora (nunca lixo comum), mesa limpa no fim do expediente.
- **Órgão público não paga multa**, mas sofre advertência e publicização, o agente responde (Lei nº 8.112/1990) e CGU/TCU entram na sequência. Para uma universidade, a pior multa é a manchete.

Dois casos de balcão

"QUERO O HISTÓRICO DO MEU FILHO"

Pai pede o histórico do filho MAIOR de idade. O vínculo é real, mas o titular é o filho, sem autorização expressa dele, o documento não sai. Resposta gentil: oriente o pai a pedir ao próprio filho, ou trazer autorização por escrito.

"POSSO MANDAR A LISTA DE SALÁRIOS POR E-MAIL INTERNO?"

E-mail se encaminha, fica anos na caixa e abre na tela errada. O caminho certo: pasta institucional com permissão POR USUÁRIO, configurada ANTES de salvar o arquivo. Uma planilha controlada vale mais que dez cópias espalhadas.

PEDIDO DE TITULAR NÃO SE IGNORA

"Quero saber o que vocês têm sobre mim" é um direito, não um incômodo. Não resolva no achismo: encaminhe ao Encarregado (DPO) da UFSC.

6 Incidentes: reporte sem medo

Aconteceu algo que não devia com informação institucional? Reporte. A dúvida já merece o e-mail.

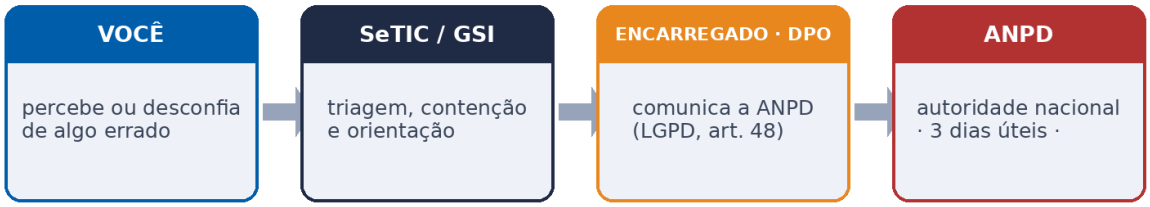
O que é um incidente

É o CID sob ataque: um dado que vazou (confidencialidade), foi alterado sem autorização (integridade) ou um sistema que saiu do ar (disponibilidade). Na prática: vazamento, ransomware, phishing bem-sucedido, uso indevido de credencial, indisponibilidade prolongada, perda ou furto de equipamento.

A matemática do reporte

- **Custo de reportar:** zero, um e-mail, alguns minutos.
- **Custo do silêncio:** enorme, para você, para o setor, para a Universidade inteira.
- **O que descrever:** o que aconteceu, quando você percebeu, dados/sistemas envolvidos, o que já fez para conter. Anexe prints.
- **Não espere certeza:** a triagem é trabalho da SeTIC, não seu. Reportou em minutos, virou estatística; escondeu por semanas, virou incidente.

Quando envolve dado pessoal: a cadeia até a ANPD



O relógio dos 3 dias úteis da ANPD começa a contar do SEU reporte interno — o primeiro elo é você.

Desde a Resolução CD/ANPD nº 15/2024, a comunicação de incidentes com dados pessoais tem relógio: 3 dias úteis para o controlador comunicar a ANPD (e os titulares, quando houver risco relevante), 20 dias úteis para complementar e registro obrigatório de todos os incidentes por 5 anos. O dia UM é a hora em que você aperta “enviar” no reporte interno.

> **Tá. Mas COMO??**
>
> **Entendi que tem que reportar, mas como eu faço isso? E Pra quem?**
>
> Se tiver relação com dados pessoais, para o encarregado de dados (DPO), hoje é o Rodrigo de Rezende.
>
> Mande um e-mail para gt.lgpd@contato.ufsc.br. Tem um site também https://lgpd.ufsc.br
>
> Se for um incidente de segurança (sem envolvimento de dados pessoais) https://chamados.setic.ufsc.br

Simulação de 30 segundos

Você recebe por engano uma planilha com dados de servidores de outra unidade. Abre por curiosidade? Não, curiosidade também é acesso indevido. Apaga e finge que nada houve? Não, o problema continua existindo. O caminho: não abrir além do necessário, avisar o remetente e a SeTIC, e documentar o ocorrido. Pronto: você acabou de ser o primeiro elo da corrente.

7 Os 12 hábitos do servidor seguro

O curso inteiro em uma página. Marque o que você já pratica, e eleja UM hábito novo para começar amanhã.

- ☐ **01** · Senhas únicas guardadas em um gerenciador (cofre digital)
- ☐ **02** · MFA ativo nos serviços pessoais que oferecem
- ☐ **03** · idUFSC com senha exclusiva, longa e forte
- ☐ **04** · Bloqueio de tela automático, e Win + L ao levantar
- ☐ **05** · Olhar o link antes de clicar (passe o mouse, confira o destino)
- ☐ **06** · Conferir o domínio do remetente (o que vem depois do @)
- ☐ **07** · VPN UFSC ligada fora do campus para acessar sistemas
- ☐ **08** · eduroam configurado no celular e no notebook
- ☐ **09** · Atualizações automáticas ligadas em todos os dispositivos
- ☐ **10** · Backup 3-2-1 do que é importante
- ☐ **11** · Saber QUANDO e COMO reportar um incidente
- ☐ **12** · Saber quem é o Encarregado (DPO) e quando acioná-lo

> **A MATEMÁTICA DA CULTURA**
> Um servidor consciente conversa com 2 colegas. Cada um, com mais 2. Em poucas semanas, um setor inteiro muda de patamar, sem portaria e sem reunião. Cultura não se decreta: se contagia. Seja um ponto de partida.

Canais permanentes

- **Dúvidas e suporte:** chamados.setic.ufsc.br
- **Incidentes de segurança e suspeitas:** chamados.setic.ufsc.br
- **Dados pessoais e direitos de titulares:** Encarregado (DPO) da UFSC gt.lgpd@contato.ufsc.br
- **Boletim de Segurança da Informação:** (em breve).
- **Autor:** Henrique Ribeiro · henrique.r@ufsc.br

“

A segurança da Universidade começa em cada mesa, em cada clique, em cada bom hábito.

cenário → chave → golpe → caminho → dados → CULTURA

SeTIC — Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação · UFSC

chamados.setic.ufsc.br · henrique.r@ufsc.br

Florianópolis · 2026