
# PRATI QUE GUIA RGPD

## SEGURANÇA DADOS PESSOAIS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

# TABLE DES MATIÈRES

# PREÂMBULO

A gestão de riscos permite determinar as precauções a serem tomadas *"em relação à **natureza dos dados e aos riscos** apresentados pelo processamento, a fim de preservar a segurança dos dados"* (Artigo 121 da Lei de Proteção de Dados[1]). O Regulamento Geral de Proteção de Dados[2] (GDPR) especifica que a proteção de dados pessoais requer que *"medidas técnicas e organizacionais adequadas* sejam tomadas para *garantir um **nível de segurança adequado ao risco**"*. Esta exigência aplica-se tanto ao controlador dos dados pessoais quanto aos sub-processadores envolvidos (artigo 32 da GDPR).

Tal abordagem permite a tomada de decisões objetivas e a determinação de medidas que são estritamente necessárias e adaptadas ao contexto. Entretanto, às vezes é difícil, quando não se está familiarizado com esses métodos, implementar tal abordagem e garantir que o mínimo tenha sido implementado.

Para ajudá-lo em sua conformidade, **este guia recorda as precauções básicas que devem ser implementadas sistematicamente.** Este guia é destinado em particular aos DPOs (responsáveis pela proteção de dados), CISOs (responsáveis pela segurança dos sistemas de informação) e especialistas em TI. Advogados e usuários também podem achá-lo útil.

**Idealmente, este guia será utilizado como parte do gerenciamento de risco, mesmo que mínimo, que consiste nas três ações a seguir.**

1. **Identificar o processamento** de dados pessoais, automatizados ou não, os dados processados (por exemplo, arquivos de clientes, contratos) e os meios em que este processamento se baseia:

   - hardware (por exemplo, servidores, laptops, discos rígidos);
   - software (por exemplo, sistemas operacionais, software comercial);
   - canais de comunicação lógica ou física (por exemplo, fibra ótica, Wi-Fi, Internet, trocas verbais, mensageiros);
   - mídia impressa (por exemplo, documentos impressos, fotocópias);
   - as instalações físicas e instalações onde estão localizados os elementos acima (por exemplo, salas de informática, escritórios).

2. **Avaliar os riscos** de cada tratamento:

a. **Identificar os impactos potenciais** sobre os direitos e liberdades das pessoas em questão para os três eventos temidos a seguir:
   - **acesso ilegítimo aos dados** (por exemplo, roubo de identidade após a divulgação das folhas de pagamento de todos os funcionários de uma empresa);
   - **Modificação indesejada de dados** (por exemplo, acusar erroneamente uma pessoa de má conduta ou crime como resultado de registros de acesso modificados);
   - **desaparecimento de dados** (por exemplo, falha na detecção de uma interação medicamentosa devido à impossibilidade de acesso ao registro eletrônico do paciente).

1 "La loi Informatique et Libertés", cnil.fr

2 "O Regulamento Geral de Proteção de Dados - RGPD", cnil.fr

b. **Identificar as fontes de risco** (quem ou o que poderia causar cada evento temido?), levando em conta fontes humanas internas e externas (por exemplo, administrador de TI, usuário, atacante externo, concorrente), bem como fontes internas e externas não humanas (por exemplo, água, epidemia, materiais perigosos, vírus de computador não direcionados)

c. **Identificar as ameaças viáveis** (o que poderia fazer acontecer cada evento temido?). Estas ameaças ocorrem na mídia identificada anteriormente (hardware, software, canais de comunicação, mídia em papel, etc.), que podem ser :
- usado inadequadamente (por exemplo, abuso de direitos, erro de manipulação);
- modificado (por exemplo, entalamento de software ou hardware - *keylogger*, instalação de malware);
- perdido (por exemplo, roubo de um laptop, perda de um pen drive);
- observado (por exemplo, observação de uma tela em um trem, geolocalização de equipamentos);
- Deteriorado (por exemplo, vandalismo, deterioração devido ao desgaste natural);
- sobrecarregado (por exemplo, armazenamento completo, ataque de negação de serviço).

d. **Identificar medidas existentes ou planejadas** para enfrentar cada risco (por exemplo, controle de acesso, backups, rastreabilidade, segurança das instalações, criptografia, anonimização).

e. **Estimar a gravidade e a probabilidade dos** riscos, com base no acima exposto (exemplo de uma escala que pode ser usada para a estimativa: insignificante, moderada, significativa, máxima).

A tabela a seguir pode ser usada para formalizar este pensamento:

| Riscos | Impactos sobre as pessoas | Principais fontes de risco | Principais ameaças | Medidas existentes ou planejadas | Severidade para os indivíduos | Veracidade |
|---|---|---|---|---|---|---|
| Acesso ilegítimo aos dados | | | | | | |
| Alteração indesejada de dados | | | | | | |
| Desaparecimento de dados | | | | | | |

3. **Implementar e verificar as medidas planejadas.** Se as medidas existentes e planejadas forem consideradas apropriadas, deve ser assegurado que elas sejam implementadas e monitoradas. Caso contrário, medidas adicionais devem ser decididas e implementadas para reduzir a gravidade e/ou probabilidade dos riscos associados.

## PARA IR A MAIS

- A GDPR introduz **avaliações de impacto da proteção de dados** (DPIAs) e especifica que elas devem conter pelo menos *"uma descrição [...] das operações [...] e objetivos do processamento [...], uma avaliação da necessidade e proporcionalidade [...], uma avaliação dos riscos [...] e as medidas previstas para enfrentar os riscos [...] e demonstrar o cumprimento do Regulamento"* (ver artigo 35.7). **A reflexão sobre os riscos nesta ficha fornece informações para a parte da avaliação de risco da avaliação de impacto.**
- Os guias DPIA da CNIL[3] permitem a realização de uma análise de impacto da proteção de dados. A CNIL também publicou software para facilitar a condução e formalização dos DPIAs[4].
- **As auditorias de segurança são um meio essencial para avaliar o nível de segurança de uma operação de processamento de dados pessoais.** Realizadas periodicamente, elas permitem levar em conta as mudanças no processamento e as ameaças. Cada auditoria deve resultar em um plano de ação, cuja implementação deve ser monitorada no nível mais alto da organização.
- **O estudo dos riscos de segurança da informação[5] pode ser realizado ao mesmo tempo que o estudo dos riscos à privacidade**. Estas abordagens são compatíveis.
- O estudo de risco permite determinar as medidas de segurança a serem postas em prática. É necessário **fornecer um orçamento** para sua implementação.

3 "The DPA (Data Protection Impact Assessment) guides", cnil.fr

4 "Ferramenta PIA: baixar e instalar o software CNIL", cnil.fr

5 Por exemplo, usando o método EBIOS RM (ver: "The EBIOS Risk Manager method", ssi.gouv.fr), o método de gerenciamento de risco publicado pela Agência Nacional de Segurança dos Sistemas de Informação (ANSSI) da Secretaria Geral de Defesa e Segurança Nacional (SGDSN). EBIOS é uma marca registrada da SGDSN.

# FOLHA 1 - SENSIBILIZAÇÃO DOS USUÁRIOS

**Conscientizar cada usuário sobre as questões de segurança e privacidade.**

## Precauções básicas

- **Fazer com que os usuários (internos e externos à organização) que trabalham com dados pessoais tomem consciência dos riscos relacionados às liberdades e à privacidade dos indivíduos,** informá-los sobre as medidas tomadas para lidar com esses riscos e sobre as possíveis conseqüências em caso de não conformidade. Em termos concretos, isto pode envolver a organização de uma sessão de conscientização, o envio regular de atualizações dos procedimentos relevantes às pessoas de acordo com suas funções, o envio de lembretes por e-mail, etc.
- **Documentar os procedimentos operacionais,** mantê-los atualizados e disponibilizá-los a todos os usuários envolvidos. Em termos concretos, qualquer ação sobre o processamento de dados pessoais, seja uma operação administrativa ou o simples uso de um aplicativo, deve ser explicada em linguagem clara e adaptada a cada categoria de usuário, em documentos aos quais este último possa se referir.
- **Elaborar uma carta de TI e dar-lhe força vinculativa** (por exemplo, anexada ao regulamento interno). Esta carta deve incluir, pelo menos, os seguintes elementos

1. Um lembrete sobre as regras de proteção de dados e as penalidades por não cumprimento.

2. O escopo da carta, que inclui em particular :
   - as modalidades de intervenção das equipes encarregadas de gerenciar os recursos de TI da organização;
   - os meios de autenticação utilizados pela organização e a política de senha a ser seguida pelo usuário;
   - as regras de segurança que os usuários devem cumprir, as quais devem incluir
     - comunicar ao departamento interno de TI qualquer suspeita ou tentativa de violação de sua conta de TI, qualquer perda ou roubo de equipamento e, em geral, qualquer mau funcionamento;
     - nunca dê seu login/password a terceiros;
     - não instalar, copiar, modificar ou destruir o software e suas configurações sem permissão;
     - bloqueie seu computador assim que você sair de sua estação de trabalho;
     - não acessar, tentar acessar ou apagar informações, se isso não fizer parte das obrigações do usuário;
     - Respeitar os procedimentos previamente definidos pela organização a fim de gerenciar as operações de cópia de dados em mídias removíveis, em particular, obtendo o acordo prévio do superior hierárquico e respeitando as regras de segurança.

3. As modalidades de utilização dos meios informáticos e de telecomunicação disponibilizadas, tais como :
   - a estação de trabalho ;
   - equipamento nômade (especialmente no contexto do teletrabalho);
   - espaços de armazenamento individuais ;
   - redes locais ;
   - condições para o uso de dispositivos pessoais ;
   - Acesso à Internet ;
   - e-mail ;
   - Telefonia.

4. As condições de administração do sistema de informação, e a existência, se houver, de :
   - sistemas de filtragem automática ;
   - sistemas automáticos dedicados à rastreabilidade das ações;
   - Sistemas de gerenciamento do local de trabalho.

5. Responsabilidades e sanções em caso de não conformidade com a carta.

**PARA IR A MAIS**

- Implementar uma política de **classificação de informações** que defina vários níveis (por exemplo, público, interno, confidencial) e exija a marcação de documentos, mídia e e-mails contendo dados confidenciais.
- Adicionar uma declaração visível e explícita em cada página de documentos em papel ou eletrônicos que contenham dados sensíveis[6].
- Organizar sessões de treinamento e conscientização sobre segurança da informação. Lembretes periódicos podem ser feitos via e-mail. As campanhas de conscientização também podem tomar a forma de ataques simulados (por exemplo, campanhas de *phishing*).
- Prever a assinatura de um **compromisso de confidencialidade** (ver cláusula modelo ao lado), ou incluir uma **cláusula específica de confidencialidade** relativa a dados pessoais nos contratos de trabalho.

6 Os dados sensíveis são descritos no artigo 6 da Lei francesa de proteção de dados e no artigo 9 da GDPR.

## Exemplo de um compromisso de confidencialidade para aqueles q u e lidam com dados pessoais:

Eu, abaixo assinado Sr./Sra. _____na posição de _____ dentro da empresa _____ (doravante denominada "a Empresa"), tendo acesso aos dados pessoais, declara que reconhece a confidencialidade de tais dados.

Comprometo-me, portanto, em conformidade com o artigo 32 do Regulamento Geral de Proteção de Dados de 27 de abril de 2016, a tomar todas as precauções de acordo com o estado da técnica e as regras internas no âmbito das minhas funções, a fim de proteger a confidencialidade das informações às quais tenho acesso e, em particular, impedir que sejam comunicadas a pessoas não expressamente autorizadas a receber tais informações.

Em particular, eu me comprometo a :
- não utilizar os dados aos quais tenho acesso para outros fins que não aqueles pelos quais sou responsável;
- divulgar tais dados somente a pessoas devidamente autorizadas, em virtude de suas funções, a receber tais dados, sejam elas pessoas privadas, públicas, físicas ou jurídicas;
- não fazer qualquer cópia destes dados, exceto quando necessário para o desempenho de minhas funções;
- tomar todas as medidas de acordo com o estado da técnica e as regras internas no âmbito das minhas funções, a fim de evitar o uso indevido ou fraudulento desses dados;
- tomar todas as precauções de acordo com o estado da técnica e as regras internas para preservar a segurança física e lógica destes dados;
- assegurar, dentro dos limites dos meus poderes, que somente meios seguros de comunicação sejam utilizados para transferir tais dados;
- caso eu deixe de exercer meu cargo, para devolver todos os dados, arquivos de computador e qualquer suporte de informação relacionada a esses dados.

Este compromisso de confidencialidade, que está em vigor durante todo o meu mandato, permanecerá em vigor, sem qualquer limite de tempo, depois que eu deixar de exercer o cargo, seja qual for a causa, na medida em que este compromisso diz respeito ao uso e à comunicação de dados pessoais.

Fui informado de que qualquer violação deste compromisso me exporá a sanções disciplinares e penais de acordo com os regulamentos em vigor, em particular no que diz respeito aos artigos 226-13 e 226-16 a 226-24 do código penal.

Feito em xxx, em xxx, em xxx, em xxx cópias

Nome:
Assinatura :

# FOLHA 2 - AUTENTICAÇÃO DE USUÁRIOS

## Reconhecer seus usuários e, em seguida, dar-lhes o acesso necessário.

Para garantir que um usuário só acesse os dados de que necessita, ele deve ter um
**O usuário tem** que se **identificar** e se **autenticar** antes de qualquer uso das instalações de TI.

Os mecanismos para a autenticação de pessoas são categorizados de acordo com se envolvem :

- **um fator de conhecimento** (o que é conhecido), por exemplo, uma senha;
- **um fator de posse** (o que você tem), por exemplo, um cartão inteligente;
- **um fator inerente** (quem você é) que pode ser biométrico, por exemplo uma impressão digital, ou comportamental[7] , por exemplo, o teclado. Como lembrete, o processamento de dados biométricos com o objetivo de identificar automática e unicamente um indivíduo com base em suas características físicas, fisiológicas ou comportamentais é um processamento de dados sensíveis que dá origem à aplicação do artigo 9 do GDPR[8].

Diz-se que a autenticação de um usuário é multifator quando ele usa uma combinação d e pelo menos duas dessas categorias e é dito que é forte se pelo menos um fator for baseado em um mecanismo criptográfico robusto (por exemplo, chave criptográfica).

## Precauções básicas

- **Definir um identificador único para cada usuário e proibir contas compartilhadas** entre vários usuários. Caso o uso de identificadores genéricos ou compartilhados seja inevitável, exigir a validação da hierarquia, implementar meios para rastrear as ações associadas a esses identificadores e renovar a senha assim que uma pessoa não precisar mais acessar a conta.
- **Cumprir a** recomendação CNIL[9] **no caso de autenticação de usuário baseada em senha,** em particular, aplicando as seguintes regras
  - **manter as senhas seguras** ;
  - não exigindo renovação periódica de senha para usuários simples (ao contrário dos administradores);
  - exigir que o usuário **altere qualquer senha atribuída automaticamente ou por um administrador** quando a conta é criada ou quando a senha é renovada no primeiro login;
  - impor complexidade de acordo com os casos de uso:
    - **por padrão, entropia mínima** (imprevisibilidade teórica) **de 80 bits** (que corresponde, por exemplo, a um mínimo de 12 caracteres com letras maiúsculas e minúsculas, dígitos e caracteres especiais, ou um mínimo de 14 caracteres com letras maiúsculas e minúsculas e dígitos, sem um caráter especial obrigatório);

7 A autenticação comportamental é uma tecnologia menos madura do que a biométrica, por exemplo.

8 Em termos de autenticação no local de trabalho, isto significa que qualquer controlador de dados que deseje implementar tal processamento deve cumprir com as disposições do regulamento padrão sobre acesso por autenticação biométrica no local de trabalho (ver: "Controle de acesso biométrico no local de trabalho", cnil.fr).

9 "Senhas: uma nova recomendação para controlar sua segurança", cnil.fr

- entropia de 50 bits caso existam medidas adicionais (restrição de acesso à conta, como um timeout após várias falhas, a implementação do "Captcha" ou o bloqueio da conta após 10 falhas);
- Entropia de 13 bits no caso de hardware de propriedade do usuário (por exemplo, cartão SIM, dispositivo contendo um certificado) com bloqueio após 3 falhas.

**Verifique a robustez de sua política de senhas.**
A CNIL fornece em seu site uma ferramenta[10] para calcular a complexidade das senhas solicitadas aos usuários, de acordo com cada caso de uso (somente senha, com acesso restrito ou com material em poder da pessoa).

A fim de criar senhas complexas, é possível contar com um dos dois meios a seguir:

- **Mnemônica,** por exemplo, por :
  - mantendo apenas as primeiras letras das palavras de uma frase criada para a ocasião;
  - capitalizar a palavra se for um substantivo (por exemplo, Chefe);
  - manter sinais tipográficos e de pontuação (por exemplo, ');
  - expressando números usando dígitos de 0 a 9 (por exemplo, um→ 1);
  - usando abreviações fonéticas (por exemplo, comprado em→ ht).

Por exemplo, a frase "*um empresário bem informado vale por dois*" poderia ser a senha **1Cd'Eaev2**.

- Os gerentes de senhas[11], que :
  - permitir que você armazene com segurança tantas senhas quantas forem necessárias enquanto requer apenas uma senha mestra para ser armazenada;
  - oferecer para gerar senhas aleatórias e, para alguns deles, ter uma estimativa de sua entropia;
  - pode preencher automaticamente os campos de autenticação.

## O que não fazer

- Dê uma senha pessoal para outra pessoa.
- Armazenamento de senhas em um arquivo não criptografado, em papel ou em um local de fácil acesso por outros.
- Salvar senhas em um navegador sem uma senha mestra.
- Use senhas relacionadas a você (por exemplo, nome, data de nascimento).
- Use a mesma senha para acessos diferentes.
- Mantenha as senhas padrão.
- Enviar suas próprias senhas por e-mail.
- Usar uma função criptográfica projetada internamente que, portanto, não é reconhecida ou comprovada.
- Usando uma função criptográfica obsoleta, como MD5 ou SHA-1, para armazenar senhas.

10 "Verifique sua política de senha", cnil.fr

11 "5 argumentos para adotar o gerenciador de senhas", cnil.fr

PARA IR A MAIS

- **Usar autenticação multi-fator** sempre que possível.
- **Limitar o número de tentativas de acesso às** contas de usuário nas estações de trabalho e bloquear temporariamente a conta quando seu limite for atingido.
- **Impor uma renovação de senha** com uma freqüência relevante e razoável para os administradores (somente).
- Implementar meios técnicos para **impor regras de autenticação** (por exemplo, bloquear a conta se a senha de um administrador não for renovada).
- Se possível, evite que os *logins de* usuário e administrador sejam as contas padrão definidas pelos fornecedores de software e desabilite as contas padrão.
- **Armazenar as senhas com segurança**, com um hash mínimo com uma função criptográfica de hash usando um sal ou uma chave, e na melhor das hipóteses transformadas com uma função especificamente projetada para este fim, sempre usando um sal ou uma chave[12] (ver Ficha 17: Hash, Hash ou Sinal). Uma chave não deve ser armazenada no mesmo banco de dados que as impressões digitais geradas.
- A ANSSI publicou, com a colaboração da CNIL[13], recomendações sobre autenticação multi-fator e senhas. Consulte também os guias[14] publicados pela ANSSI para ajudar os desenvolvedores e administradores na escolha de algoritmos criptográficos, dimensionamento e implementação.
- Para as autoridades administrativas, aplicam-se os anexos do Sistema Geral de Referência de Segurança (RGS)[15], em particular os anexos B1 e B2 relativos aos mecanismos criptográficos e à gestão das chaves utilizadas, respectivamente.

12 A aleatoriedade utilizada é chamada "sal" quando é diferente para cada senha armazenada e "chave" quando a aleatoriedade utilizada é comum à transformação de um conjunto de senhas (por exemplo, uma base de dados completa).

13 "Recomendações sobre autenticação multi-fator e senhas", ssi.gouv.fr

14 "Mecanismos criptográficos", ssi.gouv.fr

15 "Lista de documentos constituintes do RGS v.2.0", ssi.gouv.fr

# FOLHA 3 - GERENCIAMENTO DAS AUTORIZAÇÕES

**Limitar o acesso somente aos dados que um usuário necessita.**

## Precauções básicas

- **Definir perfis de liberação** nos sistemas, separando tarefas e áreas de responsabilidade, a fim de limitar o acesso dos usuários apenas aos dados estritamente necessários para o desempenho de suas tarefas.
- **Ter qualquer pedido de liberação validado** por um gerente (por exemplo, gerente de linha, gerente de projeto).
- **Eliminar as permissões de acesso dos usuários assim que eles não estiverem mais autorizados a acessar uma sala ou um recurso de TI** (por exemplo, mudança de missão ou posição), e **no final de seu contrato.**
- **Realizar uma revisão regular, pelo menos anual, das autorizações a** fim de identificar e excluir contas não utilizadas e realinhar os direitos concedidos às funções de cada usuário.

## O que não fazer

- Criar ou utilizar contas compartilhadas por várias pessoas.
- Dando direitos de administrador aos usuários que não precisam deles.
- Concedendo a um usuário mais privilégios do que o necessário.
- Esquecimento de retirar autorizações temporárias concedidas a um usuário (para um substituto, por exemplo).
- Esquecer de apagar as contas de usuários de pessoas que deixaram a organização ou mudaram de emprego.

**PARA IR A MAIS**

- Estabelecer, documentar e rever regularmente **uma política de controle de acesso** em relação às operações de processamento da organização, que deve incluir
  - os procedimentos a serem aplicados sistematicamente na chegada, partida ou mudança de atribuição de uma pessoa com acesso aos dados pessoais;
  - as conseqüências para aqueles com acesso legítimo aos dados no caso de não cumprimento das medidas de segurança;
  - as medidas planejadas para restringir e controlar a alocação e o uso do acesso à operação de processamento (ver Folha Nº 4: Rastreamento de operações e gerenciamento de incidentes).

# FOLHA 4 - RASTREAMENTO DE OPERAÇÕES E GERENCIAMENTO DE INCIDENTES

## Rastrear operações e fornecer procedimentos para a gestão de incidentes para responder a violações de dados (quebra de confidencialidade) confidencialidade, integridade ou disponibilidade).

A fim de **identificar acesso fraudulento** ou **uso indevido** de dados pessoais, ou para determinar a origem de um incidente, é necessário registrar algumas das ações realizadas nos sistemas de informática. Para isso, deve ser implantado um sistema de gerenciamento de traços e incidentes. Isto deve **registrar eventos relevantes** e **garantir que estes registros não possam ser alterados.** Em qualquer caso, **estes registros não devem ser mantidos por um período excessivo de tempo.**

## Precauções básicas

- **Quanto ao monitoramento das operações :**
  - **prever** um **sistema de registro** (isto é, registro em "arquivos *de registro*") das atividades comerciais dos usuários, intervenções técnicas (inclusive por administradores), anomalias e eventos relacionados à segurança:
  - **reter esses eventos por um período rolante entre seis meses e um ano** (exceto, por exemplo, quando existe uma obrigação legal, uma necessidade de gerenciamento de litígios, controle interno ou uma necessidade de análise pós-incidente);
  - **fazer um registro das operações de criação, consulta, modificação e exclusão de** dados, mantendo o identificador do autor, a data, hora e natureza da operação, bem como a referência dos dados em questão (para evitar duplicação);
  - **informar os usuários**, por exemplo no momento da autenticação ou acesso ao sistema, sobre a implementação do sistema de registro, após informar e consultar os órgãos representativos do pessoal;
  - **proteger o equipamento de registro e as informações registradas** contra operações não autorizadas (por exemplo, tornando-as inacessíveis a pessoas cuja atividade é registrada), contra o uso indevido por contas autorizadas (por exemplo, estabelecendo uma carta de usuário ou alertas específicos) e contra a sobregravação de dados escritos pelas aplicações em questão;
  - **garantir que os subcontratados estejam contratualmente obrigados** a implementar o registro de acordo com estas recomendações.
- **Sobre a gestão de incidentes :**
  - Estabelecer procedimentos para a análise dos dados coletados e **para a geração de alertas e seu tratamento em caso de suspeita de comportamento anormal**;
  - garantir que **os gerentes do sistema de gerenciamento de rastreamento notifiquem o controlador sobre qualquer anomalia ou incidente de segurança o mais rápido possível**;
  - prever a comunicação de incidentes pelos usuários e aumentar a conscientização da importância de **relatar eventos suspeitos**;

- Disseminar a todos os usuários **o que fazer e quem contatar no caso de um incidente de segurança ou evento incomum** que afete os sistemas de informação e comunicação da organização;
- **manter um registro interno de todas as violações de dados pessoais**;
- notificar[16] **a CNIL, dentro de 72 horas, de violações que representem um risco para os direitos e liberdades das pessoas e,** em caso de alto risco e salvo disposição em contrário do RGPD[17], **informar as pessoas envolvidas** para que possam limitar as conseqüências[18].

## O que não fazer

- Duplicar e armazenar excessivamente os dados pessoais envolvidos no processamento dentro dos logs (por exemplo, armazenar senhas ou seu resumo (ou (por exemplo, "*hash*") ao autenticar os usuários).
- Usar informações de dispositivos de registro para outros fins que não o de assegurar o uso adequado do sistema de computador (por exemplo, usar os registros para contar as horas trabalhadas é um mau uso do propósito, punível por lei).

**PARA IR A MAIS**

- Ver a recomendação da CNIL sobre a exploração madeireira[19].
- Veja as recomendações de segurança da ANSSI sobre o assunto[20].
- Envolver o usuário no monitoramento das operações realizadas em sua conta e dados (por exemplo, um resumo das três últimas conexões).
- Favorece o monitoramento automático dos logs, juntamente com uma configuração apropriada de alertas.
- No caso de um incidente ou para se preparar para um, consulte o site de assistência e prevenção de segurança digital[21].

16 O procedimento de notificação é detalhado no site da CNIL (ver: "Notificar uma violação de dados pessoais", cnil.fr).

17 Artigos 33 e 34 do RGPD.

18 A obrigação de notificar uma violação de dados pessoais não absolve o controlador de dados de nenhuma outra obrigação potencial de notificar um incidente (ver: "Notificações de incidentes de segurança às autoridades reguladoras: como organizar e quem contatar", cnil.fr).

19 "A CNIL publica uma recomendação sobre medidas de exploração madeireira", cnil.fr

20 "Recomendações de segurança para a arquitetura de um sistema de corte", ssi.gouv.fr

21 "Assistência às vítimas de ciber-malware", cybermalveillance.gouv.fr

# FOLHA 5 - TORNAR OS LOCAIS DE TRABALHO SEGUROS

### Evitar acesso fraudulento, execução de vírus ou controle remoto, especialmente através da Internet.

Os riscos de intrusão nos sistemas de TI são significativos e as estações de trabalho são um dos principais pontos de entrada.

## Precauções básicas

- Fornecer um mecanismo de **bloqueio automático da sessão se** a estação de trabalho não for utilizada por um determinado período de tempo.
- Instalar um *firewall de* software na estação de trabalho e limitar a abertura das portas de comunicação àquelas estritamente necessárias para o bom funcionamento das aplicações instaladas na estação de trabalho.
- Use software **antivírus atualizado regularmente** e tenha uma política de **atualização regular de software**.
- Configurar o software para **atualizar automaticamente para segurança** sempre que possível.
- Limitar os direitos dos usuários ao mínimo estritamente necessário, de acordo com suas necessidades nos postos de trabalho.
- **Incentivar o armazenamento dos dados dos usuários em um espaço de armazenamento com backup regular, acessível através da rede interna da organização** e não em estações de trabalho. Onde os dados são armazenados localmente, fornecer aos usuários facilidades de sincronização ou backup e treiná-los em seu uso.
- **Apagar com segurança os dados em uma estação de trabalho antes de serem reatribuídos** a outra pessoa.
- Para **mídias removíveis** (por exemplo, pendrives, discos rígidos externos):
  - conscientizar os usuários sobre os riscos associados a o uso de mídias removíveis, particularmente se elas vierem de fora da organização;
  - **limitar a conexão de mídias removíveis** ao essencial;
  - Desativar *o autorun* de mídia removível.
- Para **apoio à estação de trabalho** :
  - As ferramentas de administração remota devem **obter o acordo** do usuário antes de qualquer intervenção em sua estação de trabalho (por exemplo, respondendo a uma mensagem exibida na tela);
  - o usuário também deve ser capaz de **ver se o controle remoto está em andamento** e quando ele termina (por exemplo, exibindo uma mensagem na tela).

## O que não fazer

- Usar sistemas operacionais que não são mais suportados pela editora.
- Dando direitos privilegiados, tanto localmente como na rede, aos usuários que não possuem habilidades de segurança de TI.

PARA IR A MAIS

- **Proibir a execução de aplicações baixadas que** não sejam de fontes seguras.
- **Limitar o uso** de aplicações que requerem direitos de administrador para execução.
- Implementar uma solução para a análise e **descontaminação de meios removíveis** antes de cada utilização.
- **Se uma estação de trabalho for comprometida, investigar a fonte e qualquer evidência de intrusão** no sistema de informação da organização para detectar o comprometimento de outros elementos.
- **Realizar uma vigilância de segurança no software e hardware utilizados no sistema de informação da organização**. CERT-FR, o centro governamental francês de monitoramento, alerta e resposta a ataques informáticos, publica em seu site[22] alertas e avisos sobre vulnerabilidades descobertas em software e hardware e fornece, sempre que possível, formas de proteção contra elas.
- **Atualizar aplicações** quando as falhas críticas tiverem sido identificadas e corrigidas.
- Instalar atualizações **críticas do sistema operacional** sem demora, agendando uma verificação semanal automática.
- Fixar estações de trabalho a móveis específicos ou difíceis de mover (por exemplo, uso de cabos anti-roubo).
- Disseminar a todos os usuários **o procedimento a seguir e a lista de pessoas a serem contatadas no caso de um incidente de segurança ou evento incomum** que afete os sistemas de informação e comunicação da organização.
- Ver página [23] do CERT-FR sobre bons reflexos em caso de uma intrusão em um sistema de informação.

22 "CERT-FR - Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques", cert.ssi.gouv.fr

23 "Bons reflexos em caso de intrusão em um sistema de informação", cert.ssi.gouv.fr

# FOLHA 6 - FIXAÇÃO MÓVEL INFORMATIQUE

## Antecipar violações de dados fora do local, incluindo roubo ou perda de equipamentos móveis.

O aumento das práticas de trabalho fora das instalações da organização (por exemplo, viagens, teletrabalho) implica riscos específicos ligados ao uso de laptops, chaves USB ou smartphones: é essencial supervisioná-los.

## Precauções básicas

- **Aumentar a consciência dos usuários sobre os riscos específicos associados ao uso de ferramentas de TI móveis** (por exemplo, roubo de equipamentos, riscos associados à conexão a redes e equipamentos não controlados, especialmente equipamentos públicos) e os procedimentos para limitá-los.
- **Implementar mecanismos controlados de backup ou sincronização** para estações de trabalho móveis, para proteger contra o desaparecimento de dados armazenados.
- **Fornecer meios de criptografia para estações de trabalho móveis e mídias de armazenamento removíveis** (por exemplo, laptop, pendrive, disco rígido externo, CD-R, DVD-RW), tais como :
  - criptografia de disco rígido (muitos sistemas operacionais têm esta característica);
  - criptografia arquivo por arquivo ;
  - a criação de recipientes criptografados (arquivos que podem conter vários arquivos).
- **Para *smartphones*,** além do código PIN do cartão SIM, **ativar o bloqueio automático do terminal e exigir um segredo para desbloqueá-lo** (por exemplo, senha, diagrama).
- **Informar aos usuários** da pessoa a ser contatada em caso de perda ou roubo de seu equipamento.

## O que não fazer

- Utilizar como uma ferramenta de backup ou sincronização os serviços *em nuvem* instalados por padrão em um dispositivo sem uma análise completa de suas condições de uso e dos compromissos de segurança assumidos pelos fornecedores desses serviços. Estes geralmente não possibilitam o cumprimento das recomendações dadas na Folha de Fatos 13: Gerenciamento da terceirização.

**PARA IR A MAIS**

- **Colocar um filtro de privacidade** nos monitores utilizados em locais públicos.
- **Não deixar equipamentos ou documentos sem vigilância** em locais públicos.
- Não discutir (por exemplo, conversas em grupo ou telefônicas) informações sensíveis em locais públicos.
- **Limitar o armazenamento de dados** em dispositivos móveis ao estritamente necessário e possivelmente proibi-lo quando viajar [ao exterior24].
- **Fornecer mecanismos para proteção contra roubo** (por exemplo, cabo de segurança, marcação visível do equipamento) **e para limitar seu impacto** (por exemplo, travamento automático, criptografia).
- Quando dispositivos móveis são usados para coleta de dados em roaming (por exemplo, PDAs, *smartphones*, laptops), criptografar os dados no dispositivo. Prever também o travamento do dispositivo após alguns minutos de inatividade e a purga dos dados coletados assim que estes forem transferidos para o sistema de informação da organização.

24 "Boas práticas para profissionais em movimento", ssi.gouv.fr

# FOLHA 7 - PROTEÇÃO DA REDE INTERNA DE COMPUTADORES

**Permitir somente as funções de rede necessárias para os processos que estão sendo implementados.**

## Precauções básicas

- **Limitar o acesso à Internet**, bloqueando serviços desnecessários (por exemplo, VoIP, peer-to-peer).
- **Gerenciar redes Wi-Fi.** Devem usar criptografia de última geração (WPA3 ou WPA2 em conformidade com as recomendações ANSSI sobre a configuração desta [última25] ) e as redes abertas aos hóspedes devem ser separadas da rede interna.
- **Impor uma VPN para acesso remoto** com, se possível, forte autenticação do usuário (por exemplo, cartão inteligente, senha única baseada no tempo (TOTP)).
- **Garantir que n e n h u m a interface de administração seja acessível diretamente da Internet.** A manutenção remota deve ser feita através de uma VPN.
- **Limitar os fluxos de rede ao estritamente necessário**, filtrando os fluxos de entrada/saída dos equipamentos (por exemplo, firewalls, servidores proxy e outros). Por exemplo, se um servidor web utiliza HTTPS, apenas permita o tráfego de entrada para esta máquina na porta 443 e bloqueie todas as outras portas.

## O que não fazer

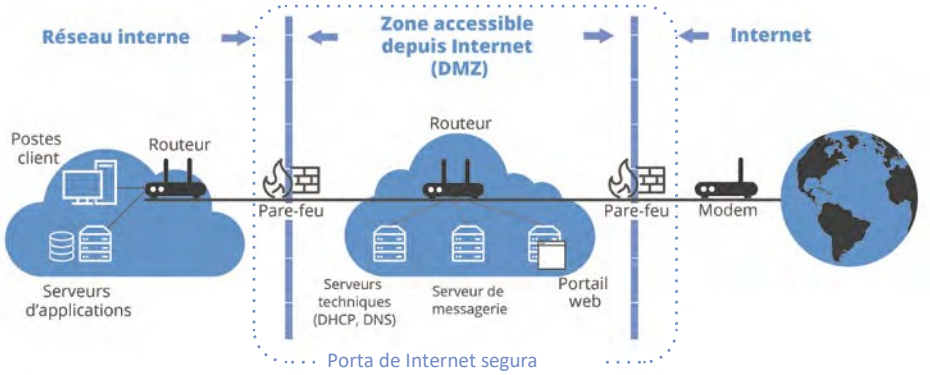
- Use o protocolo Telnet para se conectar a equipamentos de rede ativos (por exemplo, firewalls, roteadores, gateways). Ao invés disso, deve-se usar SSH ou acesso físico direto ao equipamento.
- Proporcionar aos usuários acesso não filtrado à Internet.
- Configurar uma rede Wi-Fi usando criptografia WEP.

25 "Segurança do acesso Wi-Fi", ssi.gouv.fr

PARA IR A MAIS

- **A ANSSI publicou boas** práticas[26], por exemplo, para proteger sites[27] e configurar o TLS[28].
- **A identificação automática do dispositivo pode ser implementada** pela implementação da autenticação do dispositivo (protocolo 802.1X) ou, no mínimo, pelo uso de identificadores de cartão de rede (endereços MAC) para evitar a conexão de um dispositivo não listado.
- **Sistemas de detecção de intrusão** (IDS) **e sistemas de prevenção de intrusão** (IPS) podem analisar o tráfego de rede para detectar e responder a ataques. **Informar os usuários sobre a implementação de** tais sistemas, após informar e consultar os órgãos representativos do pessoal.
- **A partição da rede** reduz o impacto em caso de comprometimento. Pode-se distinguir uma rede interna na qual nenhuma conexão com a Internet é autorizada e uma rede DMZ (DeMilitarised Zone) acessível da Internet, separando-os por *gateways*. Sobre este assunto, a ANSSI publicou recomendações relativas à interconexão de um sistema de informação com a Internet[29] (das quais o diagrama abaixo é inspirado).

**Exemplo de implementação da DMZ**




26 "Boas práticas", ssi.gouv.fr

27 "Garantindo um site", ssi.gouv.fr

28 "Recomendações de segurança para TLS", ssi.gouv.fr

29 "Recomendações sobre a interconexão de um sistema de informação com a Internet", ssi.gouv.fr

# FOLHA 8 - SERVIDORES DE SEGURANÇA

### Reforçar as medidas de segurança aplicadas aos servidores.

A segurança dos servidores deve ser uma prioridade, pois eles centralizam uma grande quantidade de dados.

## Precauções básicas

- **Desinstalar ou desativar serviços e interfaces desnecessários.**
- **Restringir o acesso às ferramentas administrativas e interfaces somente a pessoas autorizadas.** Utilizar contas com privilégios menores para operações de rotina.
- **Adotar uma política de senha específica** para administradores. Mudar as senhas, no mínimo, cada vez que um administrador sai e em caso de suspeita de comprometimento.
- **Instalar atualizações críticas** sem demora, especialmente patches de segurança, tanto para sistemas operacionais quanto para aplicações, com uma verificação semanal automática.
- **Usar software de detecção e remoção de malware atualizado** regularmente (por exemplo, antivírus).
- No campo da administração de banco de dados :
  - **usar contas nomeadas** para acesso a bancos de dados e criar contas específicas para cada aplicação;
  - implementar medidas contra ataques (por exemplo, ataques de injeção SQL, scripts).
- **Fazer backups e verificá-los regularmente** (ver Ficha 10: Planejamento de backup e continuidade de negócios).
- **Implementar TLS** (substituindo SSL[30] ), ou um protocolo que forneça criptografia e autenticação, como um mínimo para todo intercâmbio de dados pela Internet e verificar sua correta implementação com ferramentas apropriadas[31].
- **Configurar um sistema de registro de eventos** no servidor (ver Folha Nº 4: Rastreamento de operações e gerenciamento de incidentes).

## O que não fazer

- Uso de serviços não garantidos (por exemplo, autenticação no clear, fluxos no clear).
- Utilize os servidores que hospedam os bancos de dados para outras funções, como navegar em websites ou acessar o e-mail.
- Coloque os bancos de dados em um servidor diretamente acessível pela Internet.
- Utilizar contas de usuário genéricas (ou seja, compartilhadas entre vários usuários).

30 O protocolo TLS é às vezes referido como SSL ou SSL/TLS, sendo "SSL" o nome dado ao protocolo em suas primeiras versões, que agora são considerados vulneráveis e devem ser evitados.

31 Para TLS, existem várias ferramentas para este fim (por exemplo, "SSL Server Test", ssllabs.com, "SSL-Tools", ssl-tools.net).

**PARA IR A MAIS**

- Qualquer sistema que manipule dados sensíveis[32] deve ser implementado em um **ambiente dedicado** (isolado).
- **As operações de administração do** servidor devem ser realizadas através de **uma rede dedicada e isolada**, acessível após forte autenticação (ver Factsheet No. 2: Autenticação de usuários) permitindo maior rastreabilidade (ver Factsheet No. 4: Rastreamento de operações e gerenciamento de incidentes).
- Para software executado em servidores, é aconselhável usar **ferramentas de detecção de vulnerabilidade** (scanners de vulnerabilidade como o nmap[33], nessus[34] ou nikto[35]) para os processos mais críticos, a fim de detectar possíveis falhas de segurança. Sistemas de detecção e prevenção de ataques a sistemas ou servidores críticos também podem ser utilizados.
- Restringir ou negar o acesso físico e lógico às portas de diagnóstico e configuração remota.
- É preferível a versão 1.3 do TLS ou, na sua falta, a versão 1.2 em conformidade com as recomendações publicadas pela ANSSI sobre o assunto[36].
- **A ANSSI publicou em seu site[37] várias recomendações**, incluindo a segurança da administração de sistemas de informação[38] e a criação de partições de sistemas[39].

32 Os dados sensíveis são descritos no artigo 6 da Lei francesa de proteção de dados e no artigo 9 da GDPR.

33 "Nmap", nmap.org

34 "Nessus", tenable.com

35 "Nikto2", cirt.net

36 "Recomendações de segurança para TLS", ssi.gouv.fr

37 "Boas práticas", ssi.gouv.fr

38 "Recomendações sobre a administração segura dos sistemas de informação", ssi.gouv.fr

39 "Recomendações para a implementação da partição do sistema", ssi.gouv.fr

# FOLHA 9 - SEGURANÇA DE WEBSITES

### Assegurar que um mínimo de boas práticas seja aplicado aos websites.

Cada website deve garantir sua identidade e a confidencialidade das informações transmitidas.

## Precauções básicas

- **Implementar o TLS** (substituindo o SSL[40]) em todos os websites, utilizando apenas as versões mais recentes e verificando sua correta implementação.
- **Tornar obrigatório** o **uso de TLS** para toda autenticação, páginas de formulários ou páginas nas quais os dados pessoais são exibidos ou transmitidos.
- **Limitar as portas de comunicação** estritamente necessárias para o bom funcionamento das aplicações instaladas. Se o acesso a um servidor web for apenas via HTTPS, permitir apenas o tráfego de entrada da rede IP para esta máquina na porta 443 e bloquear todas as outras portas.
- **Limitar o acesso às ferramentas de administração e interfaces somente a pessoas autorizadas.** Em particular, limitar o uso de contas de administrador às equipes encarregadas das TI internas e somente para ações administrativas que o exijam.
- **Se forem utilizados *cookies* que não sejam necessários para o serviço, o consentimento** do **usuário deve ser obtido** após o usuário ter sido informado e antes que o *cookie* seja depositado.
- **Limitar o número de componentes utilizados,** monitorá-los regularmente e atualizá-los.
- **Limitar as informações devolvidas quando uma conta de usuário é criada ou uma senha é redefinida**, de modo a não informar um atacante da existência - ou não - de uma conta associada a um identificador (por exemplo, endereço de e-mail).

## O que não fazer

- Passar dados pessoais em um URL (por exemplo, detalhes de login, senhas).
- Uso de serviços não garantidos (por exemplo, autenticação no clear, fluxos no clear).
- Utilizar servidores como estações de trabalho (por exemplo, navegando em sites, acessando e-mails).
- Coloque os bancos de dados em um servidor diretamente acessível pela Internet.
- Utilizar contas de usuário genéricas (ou seja, compartilhadas entre vários usuários).

40 O protocolo TLS é às vezes referido como SSL ou SSL/TLS, sendo "SSL" o nome dado ao protocolo em suas primeiras versões, que agora são considerados vulneráveis e devem ser evitados.

**PARA IR A MAIS**

- Com relação ao uso de *cookies*, é aconselhável consultar o arquivo *"Website, cookies e outros rastreadores"* no site da CNIL[41].
- Para software executado em servidores, é aconselhável usar **ferramentas de detecção de vulnerabilidade** (scanners de vulnerabilidade como o nmap, nessus ou nikto) para os processos mais críticos, a fim de detectar possíveis falhas de segurança. Sistemas de detecção e prevenção de ataques a sistemas ou servidores críticos também podem ser utilizados. Estes testes devem ser realizados regularmente e antes de qualquer nova versão de software ser colocada em produção.
- **A ANSSI publicou em seu site[42] recomendações específicas** para implementar o TLS[43] ou assegurar um site[44].

41 "Website, cookies e outros rastreadores", cnil.fr

42 "Boas práticas", ssi.gouv.fr

43 "Recomendações de segurança para TLS", ssi.gouv.fr

44 "Garantindo um site", ssi.gouv.fr

# FOLHA 10 - SALVAGUARDA E PLANEJAMENTO PARA A CONTINUIDADE DOS NEGÓCIOS

## Realizar backups regulares para limitar o impacto de uma perda ou alteração indesejada de dados.

Os backups devem ser feitos e testados regularmente. Deve ser preparado um plano de continuidade ou de recuperação de desastres antecipando possíveis incidentes (por exemplo, falha de hardware).

## Precauções básicas

- **Com relação ao backup de dados :**
  - **fazer backups freqüentes de dados,** seja em papel ou em formato eletrônico. Pode ser apropriado ter backups diários incrementais[45] e backups completos em intervalos regulares;
  - **Armazene pelo menos um backup em um local externo,** se possível em cofres à prova de fogo e à prova d'água;
  - **Isolar pelo menos um backup offline**, desconectado da rede corporativa;
  - **proteger os dados de backup com o mesmo nível de segurança que aqueles armazenados nos servidores operacionais** (por exemplo, criptografando os backups, providenciando o armazenamento em um local seguro, providenciando uma estrutura contratual para terceirização de backups);
  - quando os backups são transmitidos pela rede, o canal de transmissão deve ser criptografado se não for interno à organização.
- **Em relação à recuperação e continuidade dos negócios :**
  - **Elaborar um plano de recuperação e continuidade de TI,** inclusive um plano sumário, incluindo a lista de interessados;
  - **garantir que os usuários, empreiteiros e subcontratados saibam quem devem alertar no caso de um incidente;**
  - **testar regularmente a restauração de backups e a aplicação do plano de continuidade ou recuperação do negócio;**
  - Sobre os materiais :
    - utilizar um UPS para proteger os equipamentos utilizados para tratamentos essenciais;
    - fornecer redundância de hardware do equipamento de armazenamento, por exemplo, por meio d a tecnologia RAID[46].

45 Um backup incremental consiste em salvar apenas as alterações feitas em um backup anterior.

46 RAID (*Redundant Array of Independant Disk*) refere-se a técnicas de distribuição de dados em múltiplas mídias de armazenamento (por exemplo, discos rígidos) a fim de evitar a perda de dados devido à falha de uma das mídias.

## O que não fazer

- Mantenha os backups nos mesmos sistemas que os dados de backup sem isolá-los. Uma ameaça informática (por exemplo, um resgate) poderia então atacar tanto os dados quanto os backups.
- Mantenha os backups no mesmo local que as máquinas que hospedam os dados. Um grande desastre neste local resultaria em perda permanente de dados.

**PARA IR A MAIS**

- A Secretaria Geral de Defesa e Segurança Nacional (SGDSN) publicou um guia[47] sobre o estabelecimento de um plano de continuidade de negócios ou de recuperação de desastres.
- Se as demandas de dados e disponibilidade do sistema forem altas, é aconselhável configurar a replicação de dados para um local secundário.

47 *Guia para elaboração de um plano de continuidade comercial* (PDF, 1.1 MB), economie.gouv.fr

# FOLHA 11 - ARQUIVAMENTO SEGURO

**Arquivamento de dados que não são mais utilizados diariamente, mas ainda não atingiram seu período de retenção, por exemplo, porque são mantidos para uso em litígio.**

Os arquivos devem ser protegidos de forma adequada aos riscos apresentados pelo arquivamento dos dados, à natureza dos dados a serem protegidos e ao impacto sobre as pessoas em questão no caso de uma violação.

## Precauções básicas

- **Definir um processo de gerenciamento de arquivo:** que dados devem ser arquivados? como e onde são armazenados? como são gerenciados os dados descritivos?
- **Implementar acordos específicos de acesso aos dados arquivados,** pois o uso de um arquivo só deve ser feito de forma ad hoc e excepcional.
- Para a destruição dos arquivos, **escolha um procedimento que garanta que todo o arquivo tenha sido destruído**.

## O que não fazer

- Usar meios de comunicação que não são garantidos para durar o tempo suficiente. Por exemplo, os CDs e DVDs graváveis raramente duram mais de 4 ou 5 anos.
- Mantenha os dados ativos, simplesmente anotando-os como arquivados. Os dados arquivados devem ser acessíveis somente a um departamento específico que tenha a tarefa específica de acessá-los.

**PARA IR A MAIS**

- A CNIL publicou uma recomendação[48] relativa às modalidades de arquivamento eletrônico.
- Os dados de interesse histórico, científico ou estatístico que justificam sua não destruição são regidos pelo Livro II do Código do Patrimônio. Mais informações sobre estas questões de arquivamento estão disponíveis no site dos Arquivos da França (ver, em particular, o artigo sobre a perpetuação da informação digital[49]).
- Em parceria com o Service interministériel des archives de France (SIAF), a CNIL publicou um guia prático sobre os períodos de retenção[50].
- O Delegado e o Comitê Interministerial de Arquivos na França lideram e coordenam a ação das administrações do Estado no campo dos arquivos. Neste contexto, eles publicaram vários documentos e diretrizes[51], incluindo as diretrizes gerais de gestão de arquivos.

48 "Deliberation 2005-213 of 11 October 2005 adopting a recommendation concerning the modalities of electronic archiving, in the private sector, of personal data", legifrance.gouv.fr

49 "Preservar dados digitais: do que estamos falando", francearchives.gouv.fr

50 "Períodos de retenção de dados", cnil.fr

51 "Publicações e recursos, gouvernement.fr

# FOLHA 12 - EMOLDURAMENTO INFORMATIQUES DESENVOLVIMENTOS

### Integrar a segurança e a proteção de dados pessoais nos projetos o mais cedo possível.

A proteção de dados pessoais deve ser integrada no ciclo de desenvolvimento de TI desde a fase de projeto e para configurações padrão, a fim de dar aos sujeitos de dados um melhor controle sobre seus dados e para limitar erros, perda, modificações não autorizadas ou uso indevido de dados em aplicações.

## Precauções básicas

- **Integrar a proteção de dados, incluindo seus requisitos de segurança de dados, no projeto da** aplicação ou serviço. Estes requisitos podem ser traduzidos em várias opções d e arquitetura (descentralizada ou centralizada), funcionalidades (por exemplo, anonimização a curto prazo, minimização de dados), tecnologias (por exemplo, criptografia de comunicação), etc.
- Implementar sistemas de **defesa em profundidade** (combinação de várias medidas de segurança).
- **Para qualquer desenvolvimento destinado ao público em geral, pense sobre os parâmetros que afetam a privacidade e**, em particular, as configurações padrão.
- **Evite o uso de campos de texto livre ou de comentários**, que podem coletar dados pessoais adicionais desnecessários ou desproporcionais.
- **Realização de testes abrangentes (unidade, integração e funcionalidade)** antes que um produto seja lançado ou atualizado.
- Realizar desenvolvimento e testes de TI em um ambiente de TI separado da produção (por exemplo, em diferentes computadores ou máquinas virtuais) e em dados fictícios ou anonimizados.
- **Realizar uma auditoria ou revisão de código antes de qualquer atualização entrar em produção** para evitar fontes de violação de dados pessoais.

## O que não fazer

- Utilizar dados pessoais reais para as fases de desenvolvimento e teste. Os jogos fictícios devem ser utilizados sempre que possível.
- Desenvolver uma aplicação e depois pensar nas medidas de segurança ou proteção de dados a serem colocadas em prática.
- Colocando a proteção de dados em uma única linha de defesa. Se essa linha de defesa cair, não há nada para proteger os dados.

PARA IR A MAIS

- A CNIL publicou um **guia** [RGPD52] **especificamente para as equipes de desenvolvimento** para ajudá-las a colocar seus desenvolvimentos de TI em conformidade com a regulamentação sobre a proteção de dados pessoais.
- O desenvolvimento deve impor **formatos de entrada de dados e de registro que minimizem os dados coletados.** Por exemplo, se apenas o ano de nascimento de uma pessoa deve ser coletado, o campo do formulário correspondente não deve permitir a entrada do mês e do dia de nascimento. Isto pode ser conseguido através da implementação de um menu suspenso limitando as escolhas para um campo de formulário.
- Um artigo dedicado às áreas de texto livre ou de comentários está disponível no site da [CNIL53].
- As convenções ou regras de codificação e documentação são essenciais para manter a aplicação ou serviço ao longo do tempo sem introduzir novas vulnerabilidades e para corrigir efetivamente as falhas de funcionamento.
- Os formatos de dados devem ser compatíveis com a implementação do período de retenção escolhido. Por exemplo, se um documento digital tiver que ser retido por 20 anos, pode ser apropriado favorecer formatos abertos que tenham maior probabilidade de ser mantidos a longo prazo.
- A criação e o gerenciamento de perfis de usuários com diferentes direitos de acesso aos dados para diferentes categorias de usuários devem ser integrados na fase de projeto.
- O teste em dados falsos ou anônimos às vezes não é suficiente para garantir que um novo serviço ou recurso funcione. É então possível testar em um ambiente de pré-produção com dados reais. O ambiente de pré-produção deve ser configurado e fixado no mesmo nível que o próprio ambiente de produção e o novo serviço ou atualização já deve ter sido submetido a todos os testes (unidade, integração e funcionalidade) nos ambientes de desenvolvimento e teste.
- Dependendo da natureza da aplicação, pode ser necessário assegurar sua integridade através do uso de assinaturas de código executável para garantir que não tenha sido adulterada.

52 "RGPD Guide for the Development Team", linccnil.github.io

53 "Bloco de notas e zonas de comentários: os reflexos certos para evitar escorregamentos", cnil.fr

# FOLHA 13 - GERENCIAMENTO DA MANUTENÇÃO E DO FIM DE VIDA ÚTIL DE HARDWARE E SOFTWARE

### Garantir a segurança dos dados em todos os estágios do ciclo de vida do hardware e software.

As operações de apoio devem ser controladas para garantir que o acesso aos dados pelos prestadores de serviços seja controlado. Os dados devem ser apagados de antemão dos equipamentos que devem ser descartados.

## Precauções básicas

- **Registro de intervenções de** manutenção **em um diário de bordo**.
- **Abrir os acessos necessários** para manutenção remota **a pedido** do prestador do serviço e por uma duração adaptada à intervenção e definida com antecedência. Estes acessos devem ser fechados novamente no final deste período.
- Inserir uma cláusula de segurança nos contratos de manutenção realizados pelos prestadores de serviços.
- **Supervisão por um gerente da organização de intervenções de terceiros.**
- **Não deixe um trabalhador externo sozinho**, especialmente em salas sensíveis (por exemplo, sala de servidores).
- **Apagar com segurança os dados do equipamento antes que ele seja sucateado, enviado a um terceiro para conserto** ou no final do contrato de locação.

## O que não fazer

- Instalação de aplicações de manutenção remota com vulnerabilidades conhecidas (por exemplo, aplicações que não criptografam as comunicações).
- Reutilizar, revender ou descartar mídia que tenha contido dados pessoais sem que os dados tenham sido apagados com segurança.
- Permitir o acesso total ou permanente aos sistemas para manutenção remota.

**PARA IR A MAIS**

- Escrever e implementar um procedimento seguro de exclusão de dados.
- Usar software dedicado à eliminação de dados sem destruição física que tenham sido auditados ou certificados. A ANSSI concede certificações de primeiro nível[54] a tais softwares.
- Implementar ferramentas de monitoramento em tempo real (por exemplo, sessões de "quatro olhos") ou a posteriori (por exemplo, gravação) para intervenções de manutenção remota por terceiros[55].

54 "Produtos certificados CSPN", ssi.gouv.fr

55 Assim como nos sistemas de registro, tais dispositivos devem ser implementados de acordo com as disposições legais aplicáveis e com o conhecimento dos sujeitos dos dados.

**Exemplo de cláusulas que podem ser usadas em caso de manutenção por terceiros:**

Cada operação de manutenção deve ser objeto de uma descrição especificando as datas, a natureza das operações e os nomes dos envolvidos, transmitidos a X.

Em caso de manutenção remota que permita o acesso remoto aos arquivos de X, Y só poderá intervir após a autorização de acesso emitida por X. O acesso deve ser fechado após cada intervenção por Y.

[*Redação alternativa, dependendo da natureza da manutenção :*

Em caso de manutenção remota que permita o acesso remoto aos arquivos de X, Y só pode intervir após a informação ter sido dada a X, permitindo a este último identificar e monitorar o acesso ao seu sistema de informação.

]

Os registros serão mantidos sob as respectivas responsabilidades de X e Y, mencionando a data e a natureza detalhada das intervenções de manutenção remota, bem como os nomes de seus autores.

Nota: esta cláusula de manutenção deve necessariamente ser acoplada à cláusula de confidencialidade para subcontratação.

# FOLHA 14 - GESTÃO DA SUBCONTRATAÇÃO

## Supervisionar a segurança dos dados com os subempreiteiros.

O processamento de dados realizado por um processador em nome do controlador deve se beneficiar de garantias suficientes, em particular no que diz respeito à segurança. O controlador deve ter conhecimento dos detalhes das medidas de segurança implementadas por seus processadores é necessário para a demonstração do cumprimento[56].

## Precauções básicas

- **Utilizar somente subcontratados com garantias suficientes** (particularmente em termos de conhecimentos especializados, confiabilidade e recursos). Exigir que o prestador de serviços comunique sua política de segurança dos sistemas de informação e quaisquer certificações.
- **Prever um contrato com** processadores[57] , que define em particular o objeto, duração e finalidade do processamento, bem como as obrigações das partes, particularmente em termos de segurança do processamento. Garantir que ele contenha, em particular, disposições que estabeleçam :
  - a distribuição de responsabilidades e obrigações no que diz respeito à **confidencialidade dos dados pessoais** confiados;
  - **requisitos mínimos para autenticação do** usuário;
  - **as condições para a devolução e destruição dos dados** no final do contrato;
  - **regras para gerenciamento e notificação de incidentes**. Estas devem incluir informar o controlador sobre a descoberta de u m a violação ou incidente de segurança o mais rápido possível no caso de uma violação de dados pessoais[58] ;
  - a assistência a ser prestada pelo subcontratante para garantir o cumprimento das obrigações de segurança[59] ;
  - a revisão regular das medidas de segurança e, se necessário, as condições para sua revisão.
- **Prever os meios para verificar a eficácia das garantias oferecidas pelo processador** com relação à proteção de dados (por exemplo, auditorias de segurança, visitas às instalações). Estas garantias incluem, em particular:
  - criptografia dos dados de acordo com sua sensibilidade ou, na falta desta, a existência de procedimentos que garantam que o prestador de serviços não tenha acesso aos dados a ele confiados, se isso não for necessário para a execução de seu contrato;
  - criptografia das transmissões de dados (por exemplo, conexão HTTPS, implementação de VPN);
  - garantias em termos de proteção da rede, rastreabilidade, gestão d e autorizações, autenticação, auditorias, etc.

56 Artigos 5.2 e 24.1 do GDPR.

57 A Comissão Européia publicou cláusulas contratuais padrão nas quais este contrato pode ser baseado (ver: "Cláusulas contratuais padrão entre controlador e processador", cnil.fr).

58 Um incidente de segurança é caracterizado como uma "violação de dados pessoais" quando afeta dados pessoais.

59 Ver artigo 32 do GDPR e §41 das Diretrizes 07/2020 adotadas pelo Comitê Europeu de Proteção de Dados (AEPD).

## O que não fazer

- Comece a terceirização sem ter assinado um contrato com o prestador de serviços que inclua os requisitos do Artigo 28 do GDPR.
- Utilizar serviços de *nuvem* sem garantir a localização geográfica real dos dados e sem garantir as condições legais e possíveis formalidades com a CNIL para transferências de dados fora da União Européia.

**PARA IR A MAIS**

- A CNIL publicou um guia para processadores[60].
- Consultar e implementar as disposições do artigo 28 do GDPR.
- Com relação à *computação em nuvem*, dê preferência aos subcontratados que aderem a códigos de conduta[61] e garanta que esses códigos de conduta contenham, entre outras coisas, exigências de segurança e detalhes das obrigações regulamentares específicas da *nuvem*. Ver em particular os códigos aprovados pelas autoridades após o parecer d o Comitê Europeu de Proteção de Dados (AEPD): CISPE[62] e EU Cloud CoC[63].
- Com relação aos dados de saúde, um hospedeiro deve ser certificado como hospedeiro de dados de saúde (HDS)[64]. A Agência de Saúde Digital (ANS) publica a lista de hospedeiros certificados[65]. Deve-se observar que a certificação tem gradualmente substituído a aprovação do HDS desde 2018 e que alguns hospedeiros ainda têm uma aprovação válida[66].

60 "European Data Protection Regulation: a guide to support processor", cnil.fr

61 Artigo 40 do GDPR.

62 "CNIL aprova o primeiro código de conduta europeu para prestadores de serviços de infraestrutura em nuvem (IaaS)", cnil.fr

63 "Autoridade de Proteção de Dados aprova seu primeiro Código de Conduta Europeu", autoriteprotectiondonnees.be

64 "HDS - Certification of Health Data Hosts", esante.gouv.fr

65 "Lista de anfitriões certificados", esante.gouv.fr

66 "Lista de anfitriões aprovados", esante.gouv.fr

# FOLHA 15 - ASSEGURAR O INTERCÂMBIO COM OUTRAS ORGANIZAÇÕES

### Reforçar a segurança de qualquer transmissão de dados pessoais.

**Sem medidas adicionais, os canais públicos de transmissão de dados** (por exemplo, e-mail, mensagens instantâneas, plataformas de depósito de arquivos) **raramente são uma maneira segura** de transmitir dados pessoais. Uma simples supervisão pode levar pessoas não autorizadas a tomar conhecimento de dados pessoais, violando assim os direitos de privacidade das pessoas em questão. Além disso, entidades com acesso aos servidores através dos quais as informações são transmitidas podem ter acesso ao seu conteúdo ou a metadados.

## Precauções básicas

- **Criptografia de dados antes de serem gravados em um meio físico para transmissão a um terceiro** (por exemplo, pendrive, disco rígido portátil, disco óptico).
- **Ao enviar através de uma rede :**
  - **criptografando os documentos** sensíveis a serem transmitidos. A este respeito, consulte as recomendações da Folha nº 17 - Encriptação, hashing ou assinatura ;
  - utilizar um protocolo que garanta a confidencialidade e autenticação do servidor destinatário para transferências de arquivos, por exemplo, **SFTP** ou **HTTPS**, utilizando **as versões mais recentes dos protocolos** ;
  - **assegurar a confidencialidade dos segredos** (por exemplo, chave de criptografia, senha) transmitindo-os através de um canal separado dos dados protegidos (por exemplo, envio do arquivo criptografado por e-mail e comunicação da senha por telefone ou SMS).
- Abra um arquivo externo somente se o remetente for conhecido e após submeter-se a uma **verificação de vírus.**
- Se você for utilizar o **fax**, implemente as seguintes medidas:
  - Instalar o aparelho de fax em uma sala fisicamente controlada, acessível somente a pessoal autorizado;
  - exibir a identidade do aparelho de fax do destinatário ao enviar mensagens;
  - duplicar o envio por fax dos documentos originais para o destinatário;
  - pré-registar os números de possíveis destinatários no catálogo de endereços do fax (se a função existir).

## O que não fazer

- Transmitir arquivos contendo dados pessoais em texto claro através de sistemas de mensagens e outras plataformas públicas.

PARA IR A MAIS

- Utilizar algoritmos de chave pública, onde os vários atores criaram uma **infra-estrutura de gerenciamento de chave pública** para garantir a confidencialidade e integridade das comunicações, bem como a autenticação do remetente.
- Fazer com que o remetente **assine eletronicamente os dados** antes de enviá-los para garantir que ele seja o autor da transmissão (ver Ficha 17: Criptografia, hash ou sinal).
- O uso de um **repositório de arquivos temporário** também pode ser apropriado. Neste caso, certifique-se de que o :
  - estabelecer um limite de tempo para a disponibilidade dos arquivos;
  - restringir o acesso aos arquivos somente a destinatários devidamente autorizados;
  - criptografar os arquivos antes de carregá-los para o serviço se a solução utilizada não previr essa possibilidade de forma integrada.
- Algumas ferramentas e soluções de comunicação também protegem os metadados relacionados com os itens trocados e podem ser usados quando estes são particularmente sensíveis.
- Para os sistemas mais sensíveis, confinar arquivos do exterior a áreas isoladas do resto do sistema para evitar a propagação de malware.

# FOLHA 16 - PROTEÇÃO DAS INSTALAÇÕES

### Reforçar a segurança das instalações que abrigam servidores de computadores e equipamentos de rede.

O acesso às instalações deve ser controlado para impedir ou retardar o acesso direto e não autorizado tanto a arquivos em papel quanto a equipamentos de informática, incluindo servidores. As instalações também devem ser protegidas contra outros tipos de ameaças (por exemplo, incêndio, inundação).

## Precauções básicas

- Instalar **alarmes de intrusão** e verificar seu bom funcionamento periodicamente.
- **Instalar detectores de fumaça e equipamentos de combate a incêndios** e inspecioná-los anualmente.
- Proteger as chaves de acesso às instalações e os códigos de alarme.
- **Distinguir as áreas do edifício de acordo com o risco** (por exemplo, fornecer controle de acesso dedicado para a sala de informática).
- Manter uma lista de pessoas ou categorias de pessoas autorizadas a entrar em cada área e revisar a lista periodicamente.
- **Estabelecer regras e meios de controlar o acesso** aos visitantes, pelo menos fazendo com que **os visitantes sejam acompanhados fora das** áreas de **recepção** pública67 por uma pessoa pertencente à organização.
- Proteger o acesso à rede (por exemplo, tomadas de escritório, painéis de patch) e permitir somente a conexão de equipamentos autorizados.
- Proteger fisicamente os equipamentos de TI por meios específicos (por exemplo, sistema dedicado de combate a incêndios, elevação contra possíveis inundações, alimentação de energia redundante, sistema de ar condicionado redundante).

## O que não fazer

- Sub-dimensionar ou negligenciar a manutenção do ambiente da sala de computadores (por exemplo, ar condicionado, UPS). Uma falha nestas instalações muitas vezes resulta no desligamento das máquinas ou na abertura do acesso às salas (para promover a circulação do ar), o que na verdade neutraliza elementos que contribuem para a segurança física das instalações.

67 Desde o momento em que entram, durante sua visita e até a saída do local.

PARA IR A MAIS

- Manter um registro do acesso a salas ou escritórios que possam conter dados pessoais de processamento de material que possam ter um sério impacto negativo sobre as pessoas envolvidas no caso de um incidente. **Informar os usuários** sobre a implementação de tal sistema, após informar e consultar os órgãos representativos do pessoal.
- Garantir que somente o pessoal autorizado seja permitido em áreas restritas. Por exemplo:
  - dentro de áreas restritas, **requerem identificação visível** (por exemplo, crachá) para todas as pessoas;
  - Os visitantes (por exemplo, o pessoal de suporte técnico) devem ter acesso limitado. A data e a hora de sua chegada e partida devem ser registradas;
  - revisar e atualizar regularmente as permissões de acesso para proteger áreas e removê-las se necessário.

# FOLHA 17 - ENCRIPTAR, CORTAR OU ASSINAR

## Assegurar a integridade, confidencialidade e autenticidade das informações.

**As funções de hash** garantem a **integridade dos dados. As assinaturas digitais,** além de garantir a integridade, verificam a autenticidade do signatário e garantem a não repúdio. Por fim**, a criptografia,** às vezes chamada impropriamente de criptografia, garante **a confidencialidade de** uma mensagem.

## Precauções básicas

- **Utilize um algoritmo reconhecido e seguro,** por exemplo, os seguintes algoritmos:
  - SHA-268 ou SHA-369 como famílias de funções de hash;
  - HMAC usando SHA-2 ou SHA-3, bcrypt, scrypt, Argon2 ou PBKDF2 para armazenar senhas;
  - AES70 com um modo de construção apropriado (CCM, GCM ou EAX) ou ChaCha2071 (com Poly1305) para criptografia simétrica;
  - RSA-OAEP72, ECIES-KEM73 ou DLIES-KEM73 para criptografia assimétrica;
  - RSA-SSA-PSS72 para assinaturas.
- **Use tamanhos chave suficientes**:
  - Para AES, é recomendado o uso de pelo menos 128 bits;
  - Para algoritmos baseados em RSA, é recomendado o uso de módulos e expoentes secretos de pelo menos 2.048 bits ou 3.072 bits, com expoentes públicos para criptografia superior a 65.536 bits.
- **Aplique as recomendações de uso apropriadas**, dependendo do algoritmo utilizado. Os erros de implementação têm um impacto significativo sobre a segurança do mecanismo criptográfico.
- **Proteger chaves secretas, ao** menos implementando direitos de acesso restritivos e uma senha segura.
- **Escreva um procedimento indicando como as chaves e certificados serão gerenciados**, levando em conta os casos em que a senha de desbloqueio for esquecida.

68 Como definido na norma NIST FIPS 180-4.

69 Como definido no NIST FIPS 202.

70 Como definido no NIST FIPS 197.

71 Como definido no RFC 8439.

72 Como definido na norma RSA PKCS#1 v2.2.

73 Como definido na ISO/IEC 18033-2.

## O que não fazer

- Usar algoritmos obsoletos, como a criptografia DES e 3DES ou as funções hash MD5 e SHA-1.
- Confundir funções de hash com criptografia e considerar que uma função de hash por si só é suficiente para garantir a confidencialidade de um dado. Embora as funções de hash sejam funções "unidirecionais", ou seja, funções que são difíceis de reverter, os dados podem ser recuperados a partir de sua impressão digital. Como estas funções são rápidas de executar, muitas vezes é possível testar automaticamente todas as possibilidades e assim reconhecer a impressão digital.

**PARA IR A MAIS**

- Veja a página dedicada "*Entendendo os princípios principais da criptologia e criptografia*" no site da CNIL[74].
- A ANSSI publicou guias[75] para ajudar **os desenvolvedores e administradores na escolha de algoritmos criptográficos, dimensionamento e implementação**.
- Ao receber um certificado eletrônico, **verifique se o certificado** contém uma indicação de uso conforme esperado, se **é válido e não revogado e se possui uma cadeia de certificação correta em** todos os níveis.
- **Usar software ou bibliotecas criptográficas que tenham sido verificadas por terceiros com experiência comprovada.**
- Diferentes soluções de criptografia podem ser usadas, tais como :
  - soluções certificadas ou qualificadas pela ANSSI[76] ;
  - Software VeraCrypt, permitindo a implementação de recipientes criptografados[77] ;
  - o software GNU Privacy Guard, permitindo a implementação de criptografia assimétrica (assinatura e criptografia)[78].
- Para as autoridades administrativas, aplicam-se os anexos do Sistema Geral de Referência de Segurança (RGS)[79] , em particular os anexos B1 e B2 relativos aos mecanismos criptográficos e à gestão das chaves utilizadas, respectivamente.

74 "Entendendo os princípios principais da criptologia e criptografia", cnil.fr

75 "Mecanismos criptográficos", ssi.gouv.fr

76 "Visto de Segurança", ssi.gouv.fr

77 Um recipiente é um arquivo que pode conter vários outros arquivos.

78 "The Gnu Privacy Guard", gnupg.org

79 "Lista de documentos constituintes do RGS v.2.0", ssi.gouv.fr

# AVALIAR O NÍVEL DE SEGURANÇA DOS DADOS PESSOAIS DE SUA ORGANIZAÇÃO

## Você já pensou em...?

| FOLHAS | | MENSAGENS |
|---|---|---|
| 1 | **Aumentar a consciência do usuário** | Informar e conscientizar os manipuladores de dados |
| | | Elaborar uma carta de TI e dar-lhe força vinculativa |
| 2 | **Autenticar usuários** | Definir um login único para cada usuário |
| | | Adotar uma política de senha de usuário em conformidade com as recomendações de a CNIL |
| | | Forçar o usuário a alterar a senha atribuída automaticamente ou por um administrador |
| | | Limitar o número de tentativas de acesso a uma conta |
| 3 | **Gerenciar Direitos** | Definir perfis de empoderamento |
| | | Remover permissões de acesso obsoletas |
| | | Realizar uma revisão anual das autorizações |
| 4 | **Rastreamento de operações e gerenciamento de incidentes** | Fornecer um sistema de extração |
| | | Informar os usuários sobre a implementação do sistema de registro |
| | | Proteção de equipamentos de registro e informações registradas |
| | | Prever procedimentos e responsabilidades internas para a gestão de incidentes, incluindo o procedimento para notificar os reguladores sobre violações de dados pessoais |
| 5 | **Segurança das estações de trabalho** | Fornecer um procedimento de bloqueio automático da sessão |
| | | Usar um software antivírus atualizado regularmente |
| | | Instalar um *firewall de* software |
| | | Obter o acordo do usuário antes de qualquer intervenção em seu posto de trabalho |
| 6 | **Segurança da computação móvel** | Fornecer a criptografia de equipamentos móveis |
| | | Fazer backups regulares ou sincronizações de dados |
| | | Exigindo sigilo para desbloquear smartphones |
| 7 | **Proteger a rede interna de computadores** | Limitar os fluxos de rede ao que é necessário |
| | | Garantir o acesso remoto a dispositivos de computação móvel via VPN |
| | | Protegendo suas redes Wi-Fi, em particular implementando o protocolo WPA3 |
| 8 | **Segurança de servidores** | Limitar o acesso às ferramentas de administração e interfaces somente a pessoas autorizadas |
| | | Instalar atualizações críticas sem demora |

| FOLHAS | | MENSAGENS |
|---|---|---|
| 9 | **Seguro websites** | Usar o protocolo TLS e verificar sua implementação |
| | | Verificar que nenhuma senha ou dados pessoais sejam passados através dos URLs |
| | | Verifique se a entrada do usuário corresponde ao que é esperado |
| | | Estabelecer um banner de consentimento para *cookies* não necessários para o serviço |
| 10 | **Economizar e planejar continuidad e dos negócios** | Fazer backups regulares |
| | | Armazenar mídias de backup em um local seguro |
| | | Proteção de backups, especialmente durante o transporte |
| | | Planejar e testar regularmente a continuidade dos negócios |
| 11 | **Arquivar de forma segura** | Implementar acordos de acesso específicos para dados arquivados |
| | | Destruir com segurança arquivos obsoletos |
| 12 | **Supervisão de desenvolvimentos de TI** | Levando em conta a proteção de dados pessoais desde a fase de projeto |
| | | Fornecer configurações de privacidade por padrão |
| | | Evitar ou controlar estritamente as áreas de comentários |
| | | Usar dados falsos ou anonimizados para desenvolvimento e testes |
| 13 | **Gerenciar a manutenção e o fim da vida útil de hardware e software** | Registro de intervenções de manutenção em um diário de bordo |
| | | Supervisão de intervenções de terceiros por um gerente da organização |
| | | Apagar dados de qualquer equipamento antes de ser descartado |
| 14 | **Gerenciar terceirização** | Incluir cláusulas específicas em contratos de subcontratação |
| | | Prever as condições de devolução e destruição dos dados |
| | | Assegurar a eficácia das garantias fornecidas (por exemplo, auditorias de segurança, visitas) |
| 15 | **Seguro intercâmbios com outras organizações** | Criptografar os dados antes de enviá-los |
| | | Certifique-se de que é o destinatário certo |
| | | Transmitir o segredo em uma transmissão separada e através de um canal diferente |
| 16 | **Protegendo as instalações** | Restringir o acesso às instalações com as portas trancadas |
| | | Instalação de alarmes de intrusos e verificação periódica dos mesmos |
| | | Utilizar algoritmos, software e bibliotecas reconhecidos e seguros |

| | | |
|---|---|---|
| 17 | **Encriptar, cortar ou assinar** | Manter segredos e chaves criptográficas com segurança |

**Comissão Nacional de Tecnologia da Informação e Liberdades Civis**
3, Place de Fontenoy - TSA
80715 75334 PARIS CEDEX 07
01 53 73 22 22

Março 2023

www.cnil.fr
linc.cnil.fr