1 ESCOPO

Esta Norma tem por objetivo estabelecer as regras e restrições para classificação e tratamento da Informação de propriedade ou sob a responsabilidade da Fundação Carlos Alberto Vanzolini (FCAV).

2 ABRANGÊNCIA

Esta Norma é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a partir da sua publicação aos colaboradores, parceiros e fornecedores da FCAV.

3 REFERÊNCIAS

Política de Governança de Dados Pessoais.

Política de Segurança da Informação.

ISO/IEC 16167:2020 – Segurança da informação — Diretrizes para classificação, rotulação, tratamento e gestão da informação.

ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.

ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

ISO/IEC 27701: – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.

4 DEFINIÇÕES

- ✓ **Ativo:** É qualquer coisa que tenha valor e precisa ser adequadamente protegido.

- ✓ **Classificação da Informação:** atribuição do nível de sigilo, pelo Gestor da Informação, com a indicação de rótulos que determinam os controles necessários para preservar a informação.

- ✓ **Evento:** é qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da Web, um usuário que envia um e-mail ou um firewall que faz um bloqueio de uma tentativa de conexão, entre outros.

- ✓ **Evento adverso (ou ofensivo):** é um evento com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de malware que destrói dados, entre outros.

- ✓ **Gestor da informação:** Colaborador responsável pela criação/recebimento, classificação, divulgação, compartilhamento, eliminação e destruição da informação. Também é incumbido da gestão de validação, liberação e cancelamento dos acessos à informação destes. Vale ressaltar que tais atividades podem ser delegadas para outro colaborador, desde que concedidas pelo Gestor da informação.

- ✓ **Impacto:** Consequência ou efeito potencial de um risco aos objetivos da FCAV.

- ✓ **Incidente de Segurança da Informação:** Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

- ✓ **Informação:** É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

- ✓ **Risco:** Ameaça ou perigo de ocorrência de evento capaz de gerar impacto à FCAV.

- ✓ **Sanitização:** Processo de apagar os dados de um dispositivo de armazenamento de forma irreversível, tornando inviável a recuperação dos dados por métodos de limpeza, expurgo e destruição.

- ✓ **Vulnerabilidade:** Fragilidade capaz de gerar risco à FCAV.

5 DIRETRIZES

A classificação da informação consiste na atribuição do nível de sigilo e a indicação de seu respectivo rótulo pelo Gestor da Informação para determinar quais os controles devem ser aplicados para preservar a informação.

A classificação da informação na FCAV deve ser realizada considerando:

- ✓ A importância, a criticidade, a sensibilidade e a relevância da informação para as atividades da instituição;
- ✓ Os requisitos legais e as políticas e normas vigentes da FCAV;
- ✓ A necessidade de sigilo para a FCAV, de modo a preservar a agilidade dos processos e a otimização dos investimentos em controles de proteção;
- ✓ A análise de riscos e potenciais impactos para as atividades da instituição, caso a informação seja acessada, divulgada, modificada ou excluída de forma indevida.

Os níveis de classificação superestimados devem ser evitados para reduzir a aplicação de medidas e controles de segurança desnecessários, despesas adicionais ou impactos nas atividades.

Com vistas a reduzir a aplicação de medidas e controles de segurança desnecessários, despesas adicionais ou impactos nas atividades da FCAV, não se deve classificar a informação de maneira mais restritiva do que é necessário.

As informações de propriedade ou sob a responsabilidade da FCAV devem ser imediatamente classificadas pelo Gestor da Informação quando são geradas, adquiridas, processadas ou armazenadas, para assegurar que recebam tratamento e proteção adequados com controles compatíveis em todo o seu ciclo de vida.

O acesso às informações da FCAV deve estar condicionado à necessidade de conhecimento do colaborador para a estrita realização de suas atividades profissionais.

A interpretação da classificação e o tratamento da informação de terceiros, fornecedores e parceiros comerciais deve ser realizada atendendo ao fixado nos contratos, termos de confidencialidade ou acordos estabelecidos com a FCAV

6 CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as Áreas da FCAV devem classificar as informações geradas, adquiridas, processadas ou armazenadas no desenvolvimento de suas atividades, por meio dos Gestores da Informação.

Todo documento classificado deve apresentar, de forma visível e clara, qual o nível de classificação da informação contida no documento.

A classificação da informação deve ser realizada com base nos seguintes níveis de sigilo:

- ✓ **CONFIDENCIAL:** Informação que deve ser mantida em sigilo e manuseada/acessada apenas por Colaboradores autorizados, por exemplo: informações estratégicas da FCAV. A preservação da confidencialidade desta informação é vital. Também deve ser classificada como confidencial os dados pessoais e dados pessoais sensíveis, como informações recebidas diretamente de clientes, partes do processo, dados de colaboradores, documentos físicos ou digitais de pessoas naturais. A divulgação ou acesso indevido pode gerar impacto financeiro, legal, normativo, contratual ou reputacional ao negócio como um todo ou alguns de seus processos.

- ✓ **RESTRITA:** O acesso à informação deve ser gerenciado e autorizado para pessoas, terceiros ou áreas pré-definidas; a divulgação deste tipo de informação deve ser previamente aprovada e classificada. A perda de confidencialidade destas informações pode causar perda de produtividade no processo operacional, perda financeira, divulgação de informações para competidores de mercado, dentre outras;

- ✓ **INTERNO:** São informações disponibilizadas a todos os colaboradores e determinados terceiros. A informação deve ser classificada como interna quando não for desejável que ela se torne conhecida por pessoas de fora da organização, pois o acesso não autorizado às informações, podem causar danos pequenos e/ou inconveniências à organização.

- ✓ **PÚBLICA:** Informação que pode ou deve ser de conhecimento público, sem restrição ou controle de acesso, por exemplo: serviços prestados ou produtos ofertados pela FCAV. Sua divulgação não causa qualquer dano a FCAV. Somente os Gestores de Informação, com apoio do Gestor da Área de Comunicação & Marketing e aprovação da Diretoria podem classificar uma informação como PÚBLICA.

As informações protegidas por legislações específicas, tais como sigilos bancário, fiscal, comercial, profissional e segredo de justiça, da mesma forma que ocorre em relação aos dados pessoais devem ser tratadas conforme disciplinado na respectiva legislação.

Todas as informações da FCAV devem ser rotuladas de acordo com o seu nível de sigilo, independente de se encontrarem em formato físico ou digital (ex. Confidencial).

Qualquer sistema que permita a saída de informações da FCAV deve ter um rótulo apropriado de classificação.

Quando a aplicação de rótulos físicos ou eletrônicos não for possível, outras formas para rotular a classificação da informação devem ser usadas. Em caso de dúvidas, o Gestor da Informação pode contatar a Área de Tecnologia da Informação.

Os Colaboradores têm o dever de assegurar a proteção das informações que tiverem contato contra perda, acesso, alteração ou divulgação não autorizada, de acordo com a sua classificação, além de não as utilizar para obtenção de vantagens para si ou outrem.

Todo Colaborador que identificar uma informação que ainda não está classificada, deve informar imediatamente o Gestor da Informação e tratá-la como INTERNA.

A classificação de um grupo de informações deve ser a mesma atribuída à informação classificada com o nível mais alto de sigilo.

Quando a informação pertencer a terceiros e a FCAV desempenhar o papel de custodiante, a classificação da informação e os requisitos e controles que serão aplicados para proteção devem ser informados pelo terceiro e formalizados em instrumento específico.

7 CICLO DE VIDA DA INFORMAÇÃO

O tratamento de uma informação classificada deve ser seguido pelos colaboradores da FCAV durante todas as etapas do ciclo de vida da informação, a saber:

- ✓ Criação, aquisição e recebimento;
- ✓ Registro, acesso, tramitação, transporte, compartilhamento, distribuição, destinação e demais formas de utilização;
- ✓ Cópia, impressão e demais formas de reprodução;
- ✓ Transmissão via fax, correio eletrônico, telefonia, voz, vídeo ou quaisquer outros meios de comunicação;
- ✓ Guarda, arquivamento e armazenamento;
- ✓ Descarte e eliminação.

8 TRATAMENTO DA INFORMAÇÃO

O tratamento de informação classificada como CONFIDENCIAL ou deve atender, no mínimo, aos seguintes requisitos:

- ✓ Rotular CONFIDENCIAL, RESTRITA ou INTERNA em todas as páginas, nas capas e cópias, se houver, de forma que não comprometa a leitura ou compreensão do documento e que possibilite sua eventual reprodução;
- ✓ Incluir advertência sobre restrição de acesso;
- ✓ Incluir o responsável pela Classificação (nome do Gestor da Informação ou Área da FCAV);
- ✓ Identificar Colaboradores, Áreas da FCAV ou Terceiros autorizados de acesso;
- ✓ Identificar numeração e total em cada página;
- ✓ Autorizar acesso apenas aos Colaboradores, Áreas da FCAV ou Terceiros que necessitem para o desenvolvimento da atividade profissional para a FCAV;
- ✓ Aplicar medidas de proteção lógica e física que assegurem o acesso exclusivo as pessoas autorizadas.

Somente a Área Responsável pela Gestão da Informação, juntamente com Gestor da Área de Comunicação & Marketing e aprovação da Diretoria podem classificar uma informação como PÚBLICA ou ratificar o que será divulgado pela FCAV como sendo pública em materiais de divulgação, promocionais ou institucionais.

9 MANUSEIO DA INFORMAÇÃO – DIRETRIZES GERAIS

As seguintes atividades quanto ao manuseio das informações encontram seu detalhamento no ANEXO I – TABELA DE CLASSIFICAÇÃO DA INFORMAÇÃO:

- ✓ Armazenamento de Informação em suporte físico
- ✓ Armazenamento de Informação em suporte digital
- ✓ Armazenamento de Informação em Dispositivos Removíveis
- ✓ Reprodução da Informação (Física ou Digital)
- ✓ Impressão
- ✓ Transporte Físico dentro das Dependências da FCAV
- ✓ Transporte Físico fora das Dependências da FCAV
- ✓ Transmissão pelo Correio Eletrônico
- ✓ Transmissão Digital Externa (por exemplo: FTP, SSH, link, aplicativos de comunicação instantânea e Internet)
- ✓ Transmissão por Voz ou Vídeo
- ✓ Transmissão por Fax
- ✓ Descarte de Dispositivos de Armazenamento de Informações;
- ✓ Descarte de Dispositivos de Armazenamento de Informações Digitais
- ✓ Descarte de Informações Impressas

10 MANUSEIO DA INFORMAÇÃO – DIRETRIZES ESPECÍFICAS

Em complemento as informações presentes no ANEXO I – TABELA DE CLASSIFICAÇÃO DA INFORMAÇÃO, nesta seção se encontram diretrizes específicas em relação a algumas atividades.

10.1 Armazenamento de Informação em suporte digital

A Área de Tecnologia da Informação poderá decidir por encriptar todos os discos das estações de trabalho e servidores da FCAV conforme as necessidades da instituição. O algoritmo a ser utilizado para tal tarefa não deve ter nível de segurança inferior a Advanced Encryption Standard (AES), com 128 bits.

10.2 Transmissão das Informações

O colaborador deve ter cautela ao repassar ou transmitir informações corporativas para outras pessoas, seja de forma presencial, por telefone, aplicativos de comunicação instantânea, mensagens eletrônicas, mídias sociais e outros meios.

Antes de transmitir informações CONFIDENCIAIS, RESTRITAS (INTERNAS) ou INTERNA, o colaborador deve sempre confirmar a identidade do solicitante ou destinatário, a procedência da solicitação e a real necessidade do compartilhamento, tal qual aplicação de Criptografia conforme o caso.

10.3 Transmissão Digital Externa

Informações classificadas como CONFIDENCIAL, RESTRITA (INTERNA ou EXTERNA) ou INTERNA não devem ser publicadas na Internet e nas mídias sociais, exceto quando o compartilhamento for autorizado pelo Departamento Jurídico e Área de Tecnologia da Informação juntamente com a Diretoria.

Não é permitido:

- ✓ Transmitir informações classificadas como CONFIDENCIAL para serviços de armazenamento na nuvem ou repositórios digitais fora da infraestrutura da FCAV ou não homologados pela Área de Tecnologia da Informação;
- ✓ Compartilhar informações classificadas como CONFIDENCIAL pelos aplicativos de comunicação instantânea não homologados pela Área de Tecnologia da Informação, ou sem a aplicação adequada de Criptografia e autorização prévia e expressa do Gestor da Informação;
- ✓ Compartilhar informações classificadas como RESTRITA (INTERNA ou EXTERNA) ou INTERNA sem a autorização prévia e expressa do Gestor da Informação ou por aplicações que não atendam aos critérios de conexão segura acima indicados.

10.4 Transmissão por Voz ou Vídeo

As chamadas telefônicas consideradas suspeitas devem ser encerradas e nenhuma informação deve ser fornecida a quem chamar.

11 DESCARTE DA INFORMAÇÃO

O Descarte de informações deve atender os seguintes requisitos:

- ✓ Prazo legal de retenção da informação;
- ✓ Prazo de caducidade estipulado pelo Gestor da Informação;
- ✓ O Gestor da Informação deve ser consultado antes do descarte.

12 RECLASSIFICAÇÃO

Informações que tiveram sua relevância ou potencial de impacto alteradas devem ser reclassificadas pelo Gestor da Informação.

Todos os colaboradores devem comunicar imediatamente o Gestor da Informação da inexistência ou inconsistência na classificação de uma informação.

Compete ao Gestor da Informação ou colaborador por ele designado formalmente, alterar ou cancelar a classificação atribuída às informações respeitando os interesses da FCAV, quando julgar necessário.

A marcação da reclassificação das informações deve obedecer às mesmas regras da classificação.

13 CONTRATOS

Os contratos estabelecidos com terceiros que implicarem no acesso à informação da FCAV devem conter cláusulas prevendo a:

- ✓ Obrigação da manutenção do sigilo das informações que tiverem acesso, do objeto do contrato e da sua execução;
- ✓ Obrigação de adoção de medidas de segurança adequadas no âmbito de suas atividades para manutenção do sigilo das informações que tiverem acesso;
- ✓ Devolução ou eliminação definitiva de todas as informações que estiverem em posse após a conclusão do projeto cuja execução exigia, por meio de métodos de descarte seguro, sob pena de multa e medidas judiciais cabíveis.

14 DAS RESPONSABILIDADES ESPECÍFICAS

14.1 Tecnologia da Informação

Aplicar esta Norma e demais Procedimentos Complementares relacionados às atividades de tecnologia da informação na FCAV;

Estabelecer controles de segurança para assegurar a confidencialidade, integridade e disponibilidade das informações armazenadas na rede corporativa;

Atualizar os controles de segurança e ferramentas de proteção conforme o estado da técnica de modo que esteja compatível com as necessidades da instituição.

Garantir a publicidade e disponibilidade desta Norma na FCAV.

14.2 Gestor da Informação

Cumprir e manter-se atualizado com esta Norma e demais Procedimentos Complementares;

Garantir a correta classificação de documentos, dados ou informações no momento de sua criação e/ou manuseio, bem como em necessidade de alteração;

Primar pelo correto manuseio das informações sob sua responsabilidade de gestão e guarda;

Classificar e reclassificar as informações sob a sua gestão;

Zelar para que todas as informações que tiver acesso estejam classificadas;

Gerenciar os direitos de acesso à informação sob sua responsabilidade;

Responsabilizar-se pelas atividades delegadas aos colaboradores que estão sob sua responsabilidade;

Garantir que os contratos celebrados com terceiros possuam cláusulas que preservem a segurança e a proteção das informações da FCAV;

Garantir que o acesso ou o manuseio das informações da FCAV sejam desempenhados mediante vigência de Acordo de Confidencialidade com as empresas contratadas

14.3 Gestores

Garantir e gerenciar o cumprimento desta Norma e demais documentos complementares pelos seus colaboradores;

Identificar violações ou eventual ação em desconformidade às regras de retenção e de descarte de informações praticada por pessoa no uso da informação ou sistemas e comunicar à Área de Segurança da Informação.

14.4 Colaboradores

Cumprir, estar ciente e manter-se atualizado com essa Norma e documentos complementares.

15 PENALIDADES

Qualquer atividade que desrespeite as disposições estabelecidas nesta Norma ou em quaisquer dos documentos complementares da FCAV deve ser considerada como uma violação e tratada

pela FCAV a fim de apurar as responsabilidades dos envolvidos de acordo com as “Medidas Disciplinares” da FCAV visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente

A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

16 DAS DISPOSIÇÕES FINAIS

Esta Norma deve ser revisada, no mínimo, anualmente, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da FCAV.

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis pela FCAV.

Esta Norma bem como os demais documentos que a complementam encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Encarregado pelo Tratamento de Dados Pessoais da FCAV.

Qualquer dúvida relativa a esta Norma deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da FCAV por meio do e-mail suportelgpd@vanzolini.org.br.

Esta Norma entra em vigor na data de sua publicação.

17 ANEXOS

Anexo I – Tabela de Classificação da Informação

18 NATUREZA DAS ALTERAÇÕES

Revisão	Alterações (Inclusões ou Exclusões)	Data
0	Emissão Inicial	10/04/2023

Este plano foi aprovado na Reunião da Diretoria Executiva de 19/04/2023

19 ANEXO I – TABELA DE CLASSIFICAÇÃO DA INFORMAÇÃO

#	ATIVIDADE	CONFIDENCIAL	RESTRITA ou INTERNA	PÚBLICA
1	Armazenamento de Informação em suporte físico	Ser armazenada em ambiente com acesso físico controlado e restrito ao grupo de colaboradores autorizados. Por exemplo: gavetas, armários com chaves e salas seguras. As chaves e combinações devem ser mantidas com o Gestor da Informação ou colaborador por ele autorizado;	Ser armazenada em Áreas da FCAV onde não exista o acesso de terceiros.	Sem restrições
2	Armazenamento de Informação em suporte digital	Ser armazenada nos servidores da FCAV, em local previamente indicado pelo Gestor da Informação, com controle de acesso e, sempre que necessário, mediante aplicação de criptografia ou cifragem com nível de segurança compatível com *Advanced Encryption Standard* (AES), com 128 ou 256 bits. Em caso de dúvidas quanto ao uso dos recursos de criptografia disponibilizados pela FCAV, o colaborador deve contatar o Área de Tecnologia da Informação;	Ser armazenada nos servidores da FCAV.	Sem restrições
3	Armazenamento de Informação em Dispositivos Removíveis	Ser armazenada em dispositivos removíveis somente após autorização do Gestor da Informação e mediante aplicação de criptografia ou cifragem com nível de segurança compatível com *Advanced Encryption Standard* (AES), com 128 ou 256 bits. Os dispositivos removíveis devem ser armazenados dentro das dependências da FCAV, em ambiente com acesso físico controlado e restrito ao grupo de acesso autorizado;	Os dispositivos removíveis devem ser armazenados dentro das dependências da FCAV.	Sem restrições
4	Reprodução da Informação (Física ou Digital)	Reprodução somente com autorização prévia e expressa do Gestor da Informação; A reprodução (cópia) de uma informação deve receber a mesma proteção e tratamento dado a informação original.	Reprodução somente para colaboradores da FCAV. A reprodução (cópia) de uma informação deve receber a mesma proteção e tratamento dado a informação original.	Sem restrições

5	Impressão	Somente com autorização prévia e expressa do Gestor da Informação. O colaborador deve acompanhar a impressão e garantir que ninguém terá acesso a ela;	Impressão somente no perímetro interno da FCAV ou que o colaborador deva acompanhar o documento impresso pelo tempo necessário e proceder com o descarte seguro quando não mais necessário.	Sem restrições
6	Transporte Físico dentro das Dependências da FCAV	A informação deve ser acondicionada em envelopes lacrados, com identificação externa do destinatário e o rótulo da classificação. Preferencialmente, o transporte deve ser realizado por um colaborador do grupo com acesso autorizado;	Sem restrições para dentro da FCAV.	Sem restrições
7	Transporte Físico fora das Dependências da FCAV	Somente com autorização prévia e expressa do Gestor da Informação e acondicionada em envelopes duplos. O envelope externo não deve constar qualquer identificação do nível de sigilo ou teor da informação. Já, o envelope interno deve ser lacrado e identificado o remetente, destinatário e a classificação da informação, além da seguinte observação de forma visível “Aberto apenas pelo destinatário”. Preferencialmente, o transporte deve ser realizado por um colaborador do grupo de acesso. Em caso de viagens, deve ser transportada junto ao colaborador ou armazenada em locais com chaves ou cofres;	Somente com autorização prévia e expressa do Gestor da Informação e que o colaborador deve acompanhar o suporte físico pelo tempo necessário e proceder com o descarte seguro quando não mais necessário.	Sem restrições

8	Transmissão pelo Correio Eletrônico	Quando enviada para fora do grupo de colaboradores autorizados é necessária autorização prévia e expressa do Gestor da Informação e mediante aplicação de criptografia ou cifragem com nível de segurança compatível com *Advanced Encryption Standard* (AES), com 128 ou 256 bits;	Sem restrições para os colaboradores da FCAV. Para pessoas fora da FCAV é necessária autorização prévia e expressa do Gestor da Informação.	Sem restrições
9	Transmissão Digital Externa (por exemplo: FTP, SSH, link, aplicativos de comunicação instantânea e Internet)	Somente para os colaboradores do grupo de acesso autorizado, por meio dos recursos tecnológicos homologados pela FCAV e mediante aplicação de criptografia ou cifragem com nível de segurança compatível com *Advanced Encryption Standard* (AES), com 128 ou 256 bits. Também, deve-se dar preferência para utilização de aplicações que suportem SSL ou TLS com uso de algoritmo SHA-256, SHA-384 ou posterior, ainda que a Criptografia já tenha sido aplicada. Para fora do grupo de colaboradores autorizado é necessária autorização prévia e expressa do Gestor da Informação; Informações classificadas como CONFIDENCIAL, RESTRITA (INTERNA ou EXTERNA) ou INTERNA não devem ser publicadas na Internet e nas mídias sociais, exceto quando o compartilhamento for autorizado pelo Departamento Jurídico e Área de Tecnologia da Informação juntamente com a Diretoria.	Somente com autorização prévia e expressa do Gestor da Informação e somente com a utilização de aplicações que suportem SSL ou TLS com uso de algoritmo SHA-256, SHA-384 ou posterior. Informações classificadas como CONFIDENCIAL, RESTRITA (INTERNA ou EXTERNA) ou INTERNA não devem ser publicadas na Internet e nas mídias sociais, exceto quando o compartilhamento for autorizado pelo Departamento Jurídico e Área de Tecnologia da Informação juntamente com a Diretoria.	Sem restrições

10	Transmissão por Voz ou Vídeo	Somente para os colaboradores do grupo com acesso autorizado, por meio dos recursos, ramais internos, canais de voz ou ambientes da FCAV. Em caso de reunião, a classificação da informação deve ser divulgada no início e no final da transmissão. Já as salas devem ter tratamento acústico adequado. Deve ser evitado o uso de sistema telefônico público, seja fixo, móvel ou rádios;	Somente aos colaboradores da FCAV.	Sem restrições
11	Transmissão por Fax	Somente com autorização prévia e expressa do Gestor da Informação, para os colaboradores do grupo de acesso autorizado e mediante a certificação da veracidade do número do destinatário indicado. O colaborador responsável deve acompanhar o envio e/ou recebimento do fax e garantir que ninguém terá acesso a informação;	Somente para as dependências e colaboradores da FCAV.	Sem restrições
12	Descarte de Dispositivos de Armazenamento de Informações e Informações Digitais	Os dispositivos de armazenamento de informações, independente se classificadas como CONFIDENCIAL, RESTRITA (INTERNA ou EXTERNA) ou INTERNA, devem ser destruídos fisicamente, por meio de fragmentadora ou trituradora, ou serem sanitizadas, de modo que tornem irrecuperáveis. Os dispositivos utilizados em reuniões (fitas, CDs, DVDs, etc.) devem ser removidos dos Recursos de TIC após o término das apresentações ou excluídos de modo permanente do disco rígido (Del + Shift nos sistemas baseados em Windows), caso o conteúdo tenha sido copiado para o recurso.	Os dispositivos de armazenamento de informações, independente se classificadas como CONFIDENCIAL, RESTRITA (INTERNA ou EXTERNA) ou INTERNA, devem ser destruídos fisicamente, por meio de fragmentadora ou trituradora, ou serem sanitizadas, de modo que tornem irrecuperáveis. Os dispositivos utilizados em reuniões (fitas, CDs, DVDs, etc.) devem ser removidos dos Recursos de TIC após o término das apresentações ou excluídos de modo permanente do disco rígido (Del + Shift nos sistemas baseados em Windows), caso o conteúdo tenha sido copiado para o recurso.	Sem restrições
13	Descarte de Informações Impressas	CONFIDENCIAL: Ser fragmentada nas dependências da Área custodiante da informação, inclusive rascunhos e demais materiais utilizados para produção destas informações e, quando impossível, encaminhado para incineração.	Ser fragmentada nas dependências da FCAV. As informações escritas em quadros brancos devem ser imediatamente apagadas pelo colaborador após a utilização.	Sem restrições

		As informações escritas em quadros brancos devem ser imediatamente apagadas pelo colaborador após a utilização.		