Política de Segurança da Informação

Versão 3.1

SUMÁRIO

1 INTRODUÇÃO

Definir diretrizes essenciais para proteger os ativos de informação da CERC, garantindo confidencialidade, integridade e disponibilidade dos dados em toda a operação da empresa. Esta Política tem como objetivo proteger as informações contra quaisquer ameaças, garantir a continuidade operacional e melhorar o desempenho em segurança da informação. Isso visa preservar interesses de clientes, fornecedores e parceiros, reforçando a resiliência e confiança no Sistema CERC para contribuir com a estabilidade do mercado financeiro nacional.

2 ABRANGÊNCIA

As diretrizes desta Política devem ser observadas e aplicadas por toda a estrutura da CERC nos pilares de pessoas, produtos e tecnologia, que acessam, armazenam, processam ou transmitem informações nos sistemas CERC.

3 PRINCÍPIOS GERAIS

A segurança da informação é aqui caracterizada pelos seguintes princípios:

- **Confidencialidade:** garantir que as informações estão disponíveis apenas a pessoas ou entidades autorizadas;
- **Integridade:** garantir que as informações são precisas, completas e livres de alterações indevidas; e
- **Disponibilidade:** garantir que as informações são acessíveis por indivíduos ou entidades autorizadas.

Quando algum dos princípios acima é quebrado, a empresa tem riscos materializados que podem gerar impactos financeiros e de negócio, além de comprometer sua imagem perante clientes, parceiros e acionistas.

4 DIRETRIZES

A Política de Segurança da Informação apresentas diretrizes que devem ser adotadas de forma contínua para a constante evolução da jornada de maturidade de Segurança dentro da CERC.

4.1 Proteção e Classificação das Informações

4.1.1 Classificação da confidencialidade das informações

O objetivo da classificação da informação é auxiliar no mapeamento de ativos da informação e estabelecer o nível de proteção que deve ser aplicado em seu armazenamento, transmissão e uso.

As informações devem ser classificadas com base no impacto potencial para a CERC resultante de divulgação não intencional, quebra de confidencialidade ou indisponibilidade.

Classificação	Descrição	Exemplos
Pública	O acesso à informação “Pública” não precisa ser controlado, registrado e não exige implementação de mecanismos de segurança.	» Campanhas externas de Marketing; e » Publicações de vagas.
Interna	O acesso a esta informação é somente para uso interno, não devendo ser exposta a pessoas de fora da CERC.	» Anúncios organizacionais; » Políticas e Normativos; » Canais do Slack;

	Podem ser informações consideradas sensíveis.	» Calendários; » Diagramas de arquitetura e rede; » Procedimentos operacionais; » Código fonte de aplicações e infraestrutura; » Segredos comerciais; » Informações financeiras; » Dados de participantes ou colaboradores que possam ser identificáveis / PII; » Salários de profissionais.

Dados de classificação "**Interna"** considerados sensíveis ou confidenciais como, por exemplo, dados financeiros, pessoais e informações privilegiadas da Companhia, devem ter um nível de proteção dos mecanismos de Segurança da Informação mais elevado, observando medidas de criptografia, controles de acesso restritos e monitoramento constante.

Esta classificação deve ser respeitada sempre que houver transferência de posse ou comunicação do ativo de informação a outros profissionais, prestadores de serviços, parceiros de negócios e público em geral.

4.1.2 Comunicação e envio de informações externas

A comunicação e o fornecimento de informações a clientes, fornecedores, parceiros, reguladores e quaisquer outros interessados externos, devem obedecer à sua classificação de confidencialidade e o seu compartilhamento deve ser realizado com extremo zelo, devendo o remetente sempre assegurar que o destinatário está correto.

São canais oficiais de compartilhamento de informações homologados pela Companhia:

- Sharepoint – ferramenta de colaboração interna e externa;
- Plataformas internas em domínio *cerc.inf.br* ou *cerc.com*; e
- Ferramentas fornecidas por clientes previamente homologadas, pelas áreas de segurança e tecnologia da informação, com requisitos mínimos estabelecidos pelas nossas políticas que consideram segurança e privacidade.

São vedados os seguintes comportamentos:

- Realizar o *upload* de arquivos em plataformas públicas (ex: *4shared*, *megaupload*, *wetransfer*, *Dropbox*, *WhatsApp*) devendo-se utilizar do Sharepoint ou plataforma específica desenvolvida ou contratada pelo cliente;
- Usar dispositivos móveis e removíveis para a gravação de informações (*pen drives*, leitores/gravadores de CDs, entre outros); e
- Encaminhar, publicar ou qualquer outra forma de divulgação de informações "Internas" da CERC para partes externas sem aprovação prévia, necessidade comercial ou sem a devida justificativa.

4.1.3 Controles de armazenamento e criptografia de dados

A CERC utilizará, quando apropriado, os seguintes controles para proteger seus dados:

- **Armazenamento Seguro:** os dados devem ser armazenados em ambientes que oferecem controles robustos de segurança. Para dados confidenciais, o armazenamento deve incluir criptografia em repouso e controles de acesso;
- **Criptografia de Dados:** utilizar padrões de criptografia fortes para proteger dados em repouso e em trânsito cujo acesso precisa ser controlado. As chaves de criptografia devem ser geridas de forma segura, evitando a exposição indevida;
- **Transmissão Segura:** assegurar que os dados em trânsito sejam protegidos por meio de protocolos seguros como SSL e TLS, bem como VPN. Implementar medidas para garantir a segurança dos dados durante a transmissão e recepção; e
- **Backup e Recuperação:** o dono da informação deve seguir políticas rigorosas de backup de seus dados considerados críticos para o negócio segundo o BIA (Business Impact Analysis), garantindo que cópias de segurança sejam realizadas regularmente e armazenadas em locais seguros. Os procedimentos de recuperação devem ser testados e validados periodicamente.

4.1.4 Data Loss Prevention (DLP)

O *Data Loss Prevention* (DLP) é um conjunto de ferramentas e processos que buscam prevenir e/ou impedir que informações confidenciais/sensíveis saiam do ambiente interno de uma organização sem autorização.

O DLP abrange todo o escopo das ferramentas de comunicação, colaboração e produtividade da CERC e/ou utilizados pelos profissionais da CERC, compreendendo Computadores, Celulares, Email, Repositório de Documentos, Chat, dentre vários outros existentes no ambiente.

As seguintes diretrizes devem ser respeitadas na utilização do DPL:

- Devem ser monitoradas informações classificadas como “Interna” que sejam consideradas sensíveis ou confidenciais de acordo com a confidencialidade das informações e dados que se enquadrem de forma regulatória e/ou legal;
- Devem também ser identificadas ameaças e/ou comportamentos inadequados que podem ir além das informações classificadas;
- Informações da CERC somente poderão ser armazenadas em dispositivos homologados, que tenham criptografia de disco, *antimalwar*e e gerenciamento remoto;
- Somente ferramentas ou tecnologias aprovadas poderão ser utilizadas para compartilhamento de informações com partes externas;
- Somente soluções autorizadas/homologadas poderão processar informação sensível fora do ambiente da CERC;
- Encaminhar, publicar ou qualquer outra forma de divulgação de informações “Internas” da CERC para partes externas sem aprovação prévia e necessidade comercial é estritamente proibido.

4.1.5 Armazenamento e destruição de ativos de informação

- Os ativos de informação exclusivamente relacionados à CERC permanecerão armazenados por tempo indeterminado.

Os ativos de informação, inclusive dados pessoais, recebidos de seus participantes, parceiros e fornecedores deverão ser arquivados por, no mínimo, 10 (dez) anos para cumprimento de obrigação legal e regulatória e para exercício regular de direitos, nos termos da Lei de Proteção Geral de Dados. Após este prazo e após constatação de inexistência de dever legal e regulatório ou quaisquer processos administrativos, criminais ou civis em andamento, os ativos de informação deverão ser anonimizados ou destruídos.

4.1.6 Descarte de documentos e mídias de armazenamento

Devem ser seguidas as seguintes diretrizes para descarte de documentos e mídias de armazenamento:

- **Documentos Confidenciais:** não se deve deixar à disposição papéis com informações confidenciais sem supervisão. Eles devem ser destruídos (triturados) ao invés de reciclados; e
- **Descarte de Equipamentos:** a equipe de TI Corporativa deve garantir o descarte seguro de equipamentos. Antes de descartar ou doar dispositivos com armazenamento de dados, todos os dados devem ser completamente apagados usando métodos de exclusão seguros.

4.1.7 Adoção de novas tecnologias

A avaliação de maturidade de Segurança de novas tecnologias deve ser conduzida antes de ocorrer a contratação e implementação dessas ferramentas ou soluções, visando a continuidade das operações da CERC, bem como a confidencialidade, integridade e disponibilidade dos dados confidenciais.

4.2 Controle de Acesso

4.2.1 Gestão de Acesso a dados

As credenciais e chaves de acessos aos sistemas de informação da CERC são pessoais e intransferíveis e devem ter suas permissões baseadas no Princípio do Menor Privilégio, garantindo que os profissionais e terceiros acessem apenas os dados necessários para suas funções, que não divulguem suas credenciais e que utilizem única e exclusivamente para o fim que foi autorizado, conforme previsto em normativo interno específico para este fim.

4.2.2 Gerenciamento de Senhas

Senha é o conjunto de caracteres destinado a identificar o usuário ou a permitir acesso a dados, programas ou sistemas que não estão disponíveis ao público combinado com um identificador único (nome de usuário, por exemplo). As diretrizes para o gerenciamento de senhas serão descritas em normativo interno específico para este fim.

4.3 Proteções do ambiente corporativo

4.3.1 Utilização de Softwares

Todos os profissionais e terceiros devem utilizar as ferramentas oficiais da CERC e eventuais exceções devem ser avaliadas pela área de TI Corporativa (para sua aquisição e distribuição) e pela área de InfoSec caso não atendam aos requisitos mínimos de segurança descritos no normativo interno específico para este fim, como mecanismos de autenticação integrada via Single Sign ON (SSO).
Adicionalmente, todos os patches de atualização dos softwares utilizados pela CERC são aplicados assim que disponíveis pelos fornecedores, primeiramente, em ambiente de homologação a fim de evitar problemas no ambiente de produção da CERC.
Todos os notebooks e computadores da CERC, além de seus servidores, devem possuir proteções de segurança implementados.

4.3.2 Uso de Internet

- O acesso à Internet, nas dependências ou utilizando equipamentos da CERC, tem a finalidade única e exclusiva de atender aos interesses do negócio, enriquecimento intelectual, ferramenta de busca de informações e tudo o que possa contribuir para o desenvolvimento de atividades relacionadas à CERC;
- Os usuários deverão utilizar a Internet através dos recursos da CERC, de maneira segura e ética, seguindo os Princípios da Legalidade e do Interesse Profissional;

- O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades do trabalho ou colocar a CERC em risco;
- O acesso à internet por visitantes deve ser concedido através de rede WIFI segregada destinada a este fim; e
- Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

4.3.3 Ambiente de trabalho físico e remoto

- O profissional deverá sempre bloquear seu computador ao deixar a estação de trabalho, ainda que momentaneamente, e não deverá deixar informações sensíveis ou confidenciais disponíveis ao alcance de outras pessoas (outros profissionais ou não);
- Informações confidenciais e de uso restrito não devem ser impressas ou anotadas em papel. Quando isto for necessário, devem ser sempre guardados em local seguro, como armários e gavetas com chave;
- Os profissionais devem sempre dar preferência a um local de trabalho remoto privado, e diante da impossibilidade, ter cuidado com as informações que estão sendo acessadas ou comunicadas; e
- Ao final do expediente (no escritório ou home office), todo profissional deverá guardar os documentos que estiver utilizando em local fechado com chave e desligar sua estação de trabalho, a fim de evitar a exposição de informação (sensível ou não).

4.3.4 Segurança Física

As diretrizes de Segurança física foram estabelecidas para garantir que as instalações, equipamentos e informações estejam protegidos contra uma ampla gama de ameaças físicas, contribuindo para a integridade geral da segurança da informação, incluindo, mas não limitado a:

- **Controle de Acesso Físico:** devem existir controles adequados visando garantir a correta autorização de pessoas, o registro e o monitoramento e vigilância dos acessos;
- **Proteção de áreas sensíveis:** devem existir controles que possam disponibilizar a segregação de ambientes e quem poderá acessá-los;
- **Proteção conta ameaças ambientais:** deve haver sistemas de supressão e detecção de incêndio, bem como um controle de clima; e
- **Treinamento e Conscientização:** deve haver programas de treinamento sobre segurança física e simulação e testes de emergência com o objetivo de avaliar o preparo dos profissionais em caso de um incidente.

4.4 Proteção de Infraestrutura

Uma ou mais soluções e processos que combinados permitem a prevenção, detecção e identificação de possíveis ataques aos componentes da CERC devem estar em vigor.

Devem ser utilizadas as melhores práticas de Segurança para construção de uma arquitetura robusta, para isso deve-se:

- Ter ativos de informação considerados críticos que armazenem ou processem informações sensíveis, segregados e com controles de acesso apropriados;
- Segregar ambientes, garantindo acesso somente aos autorizados;
- Implementar processos e/ou tecnologias de modo a garantir a detecção e intrusão no ambiente supracitado;
- Implementar processos e/ou tecnologias que efetuem a proteção do perímetro de Infraestrutura;

- Disponibilizar acessos ao ambiente de Infraestrutura através de mecanismos seguros como por exemplo o uso de VPN, e não diretamente pelo tráfego de rede;
- Manter um inventário atualizado de todos os ativos em uso na infraestrutura em *cloud*;
- Adotar processo para gerenciamento da capacidade, considerando planejamento, monitoração e otimização do ambiente, gestão de performance, além de automação e conjuntos ferramentais;
- Implementar processos e/ou tecnologias de modo a garantir a detecção e intrusão no ambiente supracitado; e
- Registrar Logs do ambiente considerando o log de aplicações e auditoria, com mecanismo a evitar que ocorram alterações dos logs, acesso indevidos, havendo monitoramento e alertas para as ações em questão.

4.4.1 Backup e Restore

A proteção das informações do ambiente de Infraestrutura deve possuir diretrizes estabelecidas em normativo interno específico para o tema de *backup* e *restore*.

4.4.2 Segurança em Data Center

Devem existir controles de segurança física e lógica para garantir a proteção adequada ao acesso das informações e sistemas hospedados neste ambiente, conforme orientações abaixo:

- Somente pessoas autorizadas poderão acessar o ambiente de Data Center; e
- Deverá ser implementado mecanismo de controle e rastreabilidade dos acessos ao ambiente de Data Center (ex: controle físico e lógico, log de acesso e câmeras de segurança).

4.4.3 Gerenciamento de Vulnerabilidades

Deve-se estabelecer um programa de gerenciamento de vulnerabilidades, contemplando a identificação/descoberta, avaliação, acompanhamento de mitigação, documentação e encerramento. Os controles apropriados que tratam o gerenciamento das vulnerabilidades estão dispostos devem estar dispostos em normativo interno específico para este fim.

4.5 Desenvolvimento Seguro

As práticas de segurança da informação devem ser rigorosamente aplicadas durante o desenvolvimento de sistemas internos e na aquisição de sistemas externos. Isso garante a aderência aos requisitos descritos em normativo interno específico sobre desenvolvimento seguro, assegurando uma governança efetiva em todo o ciclo de vida do *software*.

4.6 Cultura de Segurança da Informação - Conscientização

- **Programa de treinamento contínuo em segurança da informação:** a CERC deverá manter um programa de treinamento em segurança da informação, assegurando que todos os profissionais estejam cientes dos normativos internos, procedimentos e práticas de segurança.
- **Materiais de treinamento em segurança da informação atualizados:** garantir que os materiais de treinamento reflitam as ameaças e tecnologias mais recentes, e que sejam relevantes para os diferentes papéis dentro da empresa;
- **Campanhas de conscientização regulares:** desenvolver campanhas regulares de conscientização para manter a segurança da informação em destaque, abordando temas como engenharia social (*phishing*), segurança de senhas, segurança em dispositivos móveis, desenvolvimento seguro, uso seguro de IA, proteção e dados, dentre outros;

- **Avaliação e Feedback:** regularmente avaliar a eficácia dos programas de treinamento e conscientização, e ajustá-los com base no *feedback* dos participantes e nas mudanças nas ameaças à segurança; e
- **Integração de Novos Colaboradores:** incluir uma introdução à segurança da informação como parte do processo de integração de novos profissionais, garantindo que eles compreendam os normativos internos e práticas desde o início dada sua contratação. Todo profissional deverá ser treinado em até 30 dias da sua contratação.

4.7 Inteligência Artificial (IA)

O uso de Inteligência Artificial (IA) deve seguir as diretrizes e práticas definidas em normativo interno específico deste tema para sua aplicação ética, segura e responsável. É essencial que todos os envolvidos no desenvolvimento e uso de sistemas de IA garantam a conformidade com as regulamentações vigentes, priorizando a proteção de dados e a segurança das informações.

4.8 Diretrizes para Incidentes de Segurança da Informação e Gestão de Continuidade de Negócios (GCN)

4.8.1 Procedimentos de resposta a incidentes

Deve ser estabelecido um processo claro para responder a incidentes de segurança, incluindo preparação, detecção, análise, contenção, erradicação, recuperação, *post-mortem* e comunicação interna com as áreas envolvidas para que estas deem início aos processos de comunicação externa com as partes interessadas, como clientes, parceiros e órgãos reguladores competentes, conforme descrito em normativo interno de resposta a incidentes cibernéticos.

4.8.2 Equipe de resposta a incidentes

Convém que seja definido uma equipe especializada em resposta a incidentes, com papéis e responsabilidades claros, incluindo a comunicação com partes interessadas internas e externas, conforme descrito em normativo interno.

4.8.3 Planos de continuidade de negócios

Devem estar integrados a resposta a incidentes com os planos de continuidade de negócios, assegurando a rápida recuperação das operações críticas após um incidente de segurança cibernética.

4.8.4 Testes e simulações

Convém que sejam realizados testes regulares e simulações de incidentes para avaliar a prontidão da equipe e a eficácia dos planos de resposta e recuperação.

4.8.5 Revisão e melhoria contínua

Após um incidente, realizar uma análise de *post-mortem* para identificar lições aprendidas e oportunidades de melhoria nos processos e controles de segurança.

4.8.6 Gestão de continuidade de negócios (GCN)

A CERC deve estabelecer princípios, definições, diretrizes e responsabilidades que assegurem que todas as medidas preventivas e mecanismos de recuperação de desastre estão implantados e submetidos a testes regulares, garantindo a sustentabilidade dos negócios da CERC, mesmo em situações adversas, conforme descrito na Política de Continuidade de Negócios.

4.8.7 Diretrizes para a Gestão de Riscos

A Gestão de Riscos adotada pela CERC visa estabelecer princípios, diretrizes e responsabilidades a serem observadas na gestão dos riscos, suficientes para propiciar à CERC capacidade de maneira proativa, manter os níveis de exposição dentro do aceitável descrito na RAS (*Risk Appetite Statement*) conforme Política Integrada de Riscos, Controles Internos e Conformidade.

5 DISPOSIÇÕES FINAIS

A segurança da informação é responsabilidade de todos os membros da organização. Cada indivíduo é responsável por proteger os ativos de informação aos quais tem acesso.

Exceções a essas diretrizes somente serão permitidas quando previamente aprovadas pelo Diretor de Segurança da Informação (CISO) e pelo Diretor de Riscos (CRO), com base no contexto, na justificativa, nos controles compensatórios e nos controles de mitigação.

Outros normativos internos deverão ser criados para prever outras diretrizes ou procedimentos para temas correlatos e complementares com a Segurança da Informação.

6 ATRIBUIÇÕES E RESPONSABILIDADES

Deverão ser observados conforme atribuição de cada membro abaixo listado, as diretrizes contidas nos seguintes documentos: Estatuto Social, Regimentos e demais Normativos Internos da CERC.

6.1 Conselho de Administração

» Revisar e aprovar periodicamente esta Política.

6.2 Comitê de Riscos

» Recomendar ao Conselho de Administração sobre a aprovação da Política; e
» Monitorar os riscos tecnológicos e os mecanismos para proteção de dados informacionais.

6.3 Diretorias, Gerências e Coordenadores de Áreas

» Cumprir as determinações da presente Política, informando à área responsável pelo sistema de gestão de Segurança da Informação, toda e qualquer ação não condizente às práticas estabelecidas nesta;
» Participar, se necessário, da investigação de incidentes relacionados à informação sob sua responsabilidade;
» Autorizar a liberação de acesso à informação sob sua responsabilidade;
» Revisar, de acordo com os prazos definidos, as liberações de acesso concedidas; e
» Participar junto à Diretoria de Integridade e Conformidade da elaboração de matrizes de riscos dos sistemas de informação sob sua gestão.

6.4 Área de InfoSec – Diretoria CoE

» Responsável pela diretriz, implementação, manutenção e melhoria contínua do **Sistema de Gestão de Segurança da Informação (SGSI)**;
» Atualizar e revisar esta Política periodicamente ou sempre que necessário;
» Estabelecer e gerir continuamente a estratégia de segurança da informação, desenhada de acordo com as necessidades e objetivos da CERC;
» Elaborar e revisar normativos internos relacionadas à Segurança da Informação com base em mudanças tecnológicas, processos de negócio, referências de mercado, também requisitos legais e regulatórios;

- Estabelecer controles, e processos que visam proteger as informações contra eventuais ataques cibernéticos ou modificações, divulgação e destruição não autorizada;
- Apoiar os responsáveis pelos ativos na redução do risco de acesso indevido; e
- Orientar os profissionais e fornecedores quanto aos quesitos de Segurança da Informação e fornecer treinamentos relacionados ao tema, quando necessário.

6.5 Áreas de Tecnologia (Infraestrutura e TI Corporativa) – Diretoria CoE

- Fazer cumprir os controles estabelecidos nesta Política de acordo com suas responsabilidades.

6.6 Diretoria de Integridade e Conformidade

- Supervisionar o modelo de gestão de riscos, apoiando a área de InfoSec no monitoramento de seus riscos e certificação dos controles internos;
- Realizar o controle de apontamentos de auditorias internas e independentes para garantir o cumprimento de prazos na implantação de plano de ação relativos à Segurança da Informação;
- Elaborar e revisar as matrizes de riscos dos sistemas de informação; e
- Avaliar a conformidade das diretrizes presentes na Política.

6.7 Área de Jurídico Regulatório - Diretoria Jurídica

- Manter as áreas informadas sobre eventuais alterações legais e/ou regulatórias que impliquem em responsabilidade e/ou ações envolvendo a governança da segurança da informação.

6.8 Profissionais, Prestadores de Serviços e Usuários do Sistema CERC

- Cumprir fielmente as orientações desta Política;
- Avaliar e classificar as informações de acordo com a sua confidencialidade: pública e interna;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela CERC;
- Notificar a área de InfoSec em caso de suspeita de anormalidades, descumprimentos ou qualquer violação identificada no seu ambiente de trabalho relacionada a segurança cibernética;
- Disseminar a cultura de proteção e segurança da informação; e
- Participar dos treinamentos de segurança da informação sempre que for convocada(o) e implementar os aprendizados em seu dia a dia.

7 CONTROLE DOCUMENTAL

CRIAÇÃO | REVISÃO | REVOGAÇÃO			
Versão Anterior	**Versão Atual**	**Data da Aprovação**	**Ref. De ATA/Aprovação**
3.0	**3.1**	**27/03/2025**	**Conselho de Administração**
Diretoria Responsável		**Área Responsável**	

CoE	InfoSec
PRINCIPAIS MODIFICAÇÕES	
Inclusões: » Responsabilidade da área de InfoSec – Diretoria CoE pela diretriz, implementação, manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI).	

LEGISLAÇÕES OU DOCUMENTOS RELACIONADOS
» Resolução 4893/2021 BCB; » Resolução 304/2023 BCB; » Lei n° 13.709/2018 (Lei Geral de Proteção de Dados); » Política Integrada de Riscos, Controles Internos e Conformidade; e » Política de Continuidade de Negócios.

8 ANEXOS

8.1 Definições

- **Ativo:** é tudo o que tem valor para a CERC.
- **Ativos de Informação:** são todos os ativos, tangíveis e intangíveis, que estão relacionados à informação.
- **Ciclo de Vida da Informação:** todas as fases pelas quais a informação passa dentro dos processos de negócio da CERC (produção, distribuição, armazenamento, processamento, transporte, consulta e destruição).
- **Classificação do Ativo:** é a indicação da importância do ativo.
- **Controle:** é toda forma de gerenciar o risco a que está submetido um ativo.
- **Criptografia:** é o processo de codificação de uma mensagem ou informação.
- **Proprietário:** é a pessoa responsável pelo ativo de informação. Ao proprietário cabe classificar o ativo e autorizar o acesso a ele.
- **Incidente de Segurança da Informação:** todo evento que constitua uma violação da Política de Segurança da Informação.
- **Risco:** é o potencial de uma ameaça trazer prejuízos para a CERC. É estimado com base na probabilidade da ameaça se concretizar e no impacto que poderá causar.
- **Segregação de Funções:** é o princípio de que, onde houver necessidade para o controle mais apurado dos riscos, cada pessoa seja encarregada e possa executar apenas parte do processo.
- **Segurança da Informação:** é a proteção da informação de forma que apenas as pessoas autorizadas tenham acesso a ela (Confidencialidade), que esteja disponível quando necessário (Disponibilidade) e com seu conteúdo correto (Integridade).
- **Sistema de Gestão de Segurança da Informação (SGSI):** é o conjunto de processos de trabalho e ferramentas que garantem que a CERC tenha uma efetiva e funcional segurança da informação.