Política de Segurança da Informação

dezembro/2021

Omega

1. Introdução

Esta política define normas e diretrizes que buscam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Omega.

A proteção adequada dos ativos e dos dados utilizados é fundamental para que possibilite a identificação, proteção, detecção, resposta e recuperação de eventos em caso de eventual falha da segurança da informação.

Além disso, a Política complementa a Seção 13 do Código de Conduta da Companhia, no que diz respeito às diretrizes e às condutas esperadas dos funcionários, terceiros, parceiros, fornecedores e prestadores de serviços, quanto à proteção dos ativos e dados com intuito de assegurar a confidencialidade, a integridade e disponibilidade das informações.

Aprovada pelo Conselho de Administração em 17 de dezembro de 2021, esta Política será disponibilizada no website, Workplace (rede social interna) e na plataforma do Microsoft Teams para toda Omega.
Sempre que necessário, e com uma periodicidade mínima de 2 (dois) anos, a Política será verificada pelo Comitê de Ética e poderá ser revisada.

A área de Tecnologia da Informação manterá em atividade um programa de revisão/atualização, que assegure que os requisitos de segurança técnicos e legais implementados estão sendo cumpridos e em conformidade com a legislação vigente, incluindo também a revisão periódica dos planos de ação e sua adesão a iniciativas de compartilhamento de informações sobre incidentes cibernéticos.

A adesão a essa Política e eventuais desvios de conduta serão endereçados pela Diretoria de Tecnologia da Omega e, sempre que necessário, reportados ao Comitê de Ética.

Os termos usados em letra maiúscula possuem os significados definidos no glossário do Código de Conduta ou nesta Política de Segurança da Informação.

2. Regras básicas de segurança da informação

2.1 Princípios da Segurança da Informação:

Nosso compromisso com o tratamento adequado das informações da Omega, clientes e público em geral estão fundamentados nos seguintes princípios:

Confidencialidade

Assegurar que a informação não será divulgada a indivíduos, entidades ou aplicativos sem autorização prévia dos seus titulares ou da Omega.

Integridade

Assegurar que o conteúdo da informação não tenha sido alterado e, portanto, seja íntegro e autêntico.

Disponibilidade

Permitir que a informação confidencial seja utilizada apenas quando necessário pelos usuários e destinatários.

2.2 Ciclo de Vida da Informação:

Para efeito desta política, considera-se como ciclo de vida da informação:

A

Manuseio: é a etapa onde a informação é criada e manipulada.

B

Armazenamento: é a guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.

C

Transporte: ocorre quando a informação é transportada para algum local, não importando o meio onde ela está armazenada.

D

Descarte: é a eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives) por completo.

2.3 Classificação da Informação:

A classificação das informações deve ser avaliada de acordo com seu conteúdo, relevância do conhecimento externo e pelos elementos específicos do documento.

O acesso, divulgação e tratamento de documento (físico ou digitalizado), dado ou informação são restritos aos funcionários que tenham necessidade de conhecê-los em razão de suas atividades dentro da Omega, sendo esse acesso pautado pelas regras previstas nesta Política e demais normas da empresa.

Toda informação de uso corporativo deve ser classificada de acordo com o grau de sigilo para o negócio da empresa, considerando-se três níveis:

A Confidencial

É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da empresa.

B Interno

São informações específicas para uso interno, com circulação exclusiva dentro da empresa. Essas informações podem estar disponíveis a todos os funcionários e prestadores de serviço e devem ser utilizadas somente para atividades da Omega. Esse conteúdo, mesmo sendo de circulação livre dentro da empresa, não devem ser divulgados para externos sem os devidos cuidados, incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela área responsável.

C Público

São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

2.3 Incidentes de Segurança da Informação

Para efeito desta Política, um incidente de segurança é definido como qualquer evento prejudicial, decorrente da ação ou omissão de funcionários e de terceiros ou, ainda, de uma ameaça que ataque os princípios da Segurança da Informação.

3. Sistema de gestão da segurança da informação

O **Sistema de Gestão da Segurança da Informação** é o conjunto de processos e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação com ações em quatro grandes frentes de atuação:

Governança das políticas e procedimentos de segurança da informação;

Recursos e componentes de segurança da informação;

Monitoramento contínuo do ambiente de tecnologia da informação;

Gestão de crises e continuidade de negócios.

4. Controles internos de segurança da informação e cyber security

4.1 Identificação/Avaliação de Ameaças e Vulnerabilidades

Caberá à área de Segurança da Informação da Omega a identificação e avaliação dos riscos a que os processos e ativos estejam sujeitos e possíveis cenários de ameaça.

A Omega revisou ou irá revisar as cláusulas contratuais obrigatórias para a contratação de fornecedores e prestadores de serviços com intuito de adequar todos às políticas vigentes.

4.2 Ações de Prevenção e Proteção

Serão adotadas rotinas padronizadas de prevenção e proteção dos processos e ativo, conforme previstas na norma interna, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

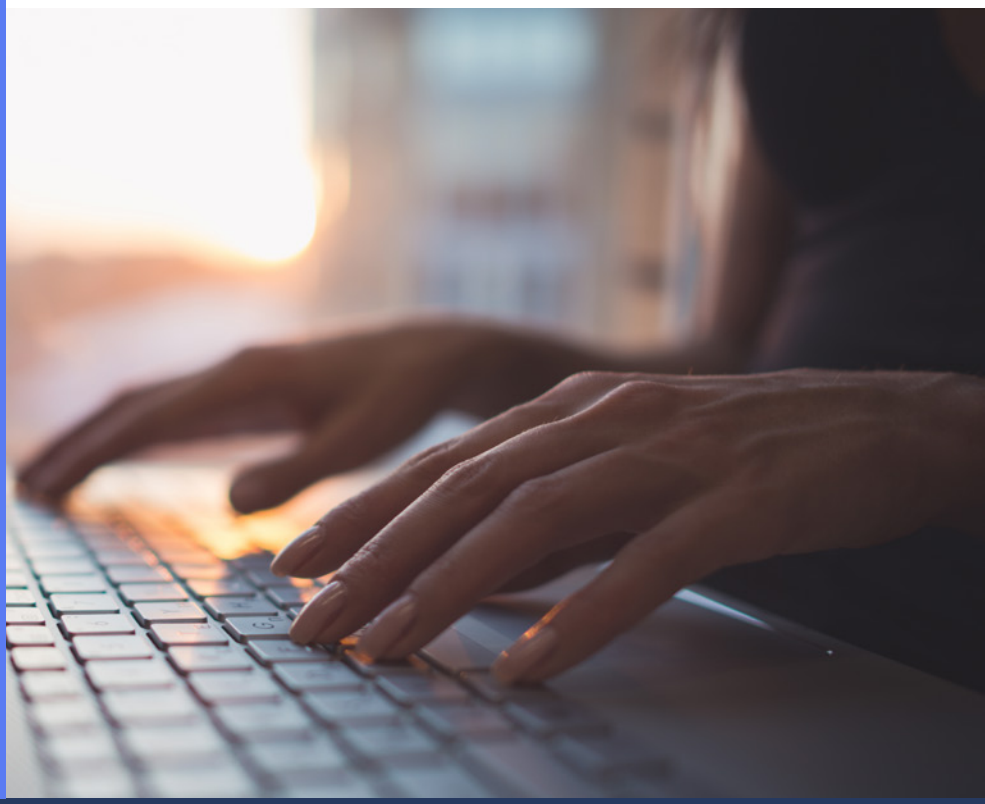
Destacando a execução periódica de testes de ataque e invasão, visando monitorar a eficiência de seu sistema de proteção a vulnerabilidades cibernéticas, a Omega realiza testes, tanto em ambiente interno (na modalidade Gray Box) como o externo (na modalidade Black Box).

4.3 Monitoramento e Testes

Devem ser implementados controles internos efetivos para proteção dos RTICs (Recursos de Tecnologia da Informação e Comunicação) da Omega, garantindo a sua confidencialidade, integridade, disponibilidade sempre observando as melhores práticas de mercado e regulamentações vigentes.

A área de Segurança da Informação pode monitorar ou inspecionar os RTICs que estiverem em suas dependências ou que interajam com os ambientes da Omega sempre que considerar necessário.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre ambientes de produção e homologação. As ameaças cibernéticas devem ser analisadas em conjunto com as vulnerabilidades detectadas pela Segurança da Informação nos ativos de informação e devem possuir monitoramento proativo da área de Segurança da Informação.



4.4 Plano de Ação e de Resposta a Incidentes

Os incidentes de Segurança da Informação devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades respeitando o nível de exposição a risco definido pela Omega.

A • Comunicação de incidentes

Os usuários devem comunicar imediatamente os casos de incidentes ao responsável por Segurança da Informação. Os incidentes deverão ser avaliados e investigados de forma a construir uma análise consistente de causa, riscos, partes envolvidas e planos de respostas. A avaliação deverá ser direcionada ao Diretor responsável pela Segurança Cibernética para decisão das ações iniciais a serem tomadas. Classificada a relevância do incidente, a Omega deverá emitir comunicação aos envolvidos, informando a situação ocorrida e ações definidas, ao menos, de forma preliminar, informando/notificando sobre as atividades que serão tomadas posteriormente. Além disso, o responsável pela Segurança da Informação deve elaborar e divulgar ao Conselho de Administração o relatório anual sobre os planos de ação e resposta aos incidentes.

B • Tentativa de burlar

A mera tentativa de burlar às diretrizes e controles estabelecidos pela Omega, quando constatada, deve ser tratada como uma violação/incidente.

C • Tratamento de vulnerabilidade identificadas

O tratamento e as correções proativas das principais fragilidades ou fraquezas dos ativos de informação a serem utilizados devem estar registradas, sendo necessário avaliar o risco residual e ser sustentado pelos envolvidos no plano.

D • Conflitos de interesse

A Omega deve possuir um processo de concessão de acessos que utiliza critérios claros e objetivos para identificar conflitos de interesse que decorrem de limitações técnicas ou de situações devidamente autorizadas. Deverá haver monitoramento das atividades dos acessos e das ameaças cibernéticas.

E • Elaboração de plano de ação

O plano de ação deverá ser elaborado pelos responsáveis de Segurança da Informação, podendo ser envolvidos outros departamentos caso necessários para implementação das soluções e para administração de eventuais contingências. Tal plano deve conter definição expressa dos papéis e responsabilidades na solução do impasse, prevendo acionamento dos funcionários chave e contatos externos relevantes, caso aplicáveis. Deverão ser levados em consideração os cenários de ameaças previstos na avaliação de risco, havendo critérios para classificação dos incidentes, dependendo da gravidade. O plano de ação deverá prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos, assim como o processo de retorno às instalações originais após o término do incidente. A documentação relacionada ao gerenciamento dos incidentes deverá ser arquivada para fins de auditoria.

F • Comunicado aos Órgãos Externos

A Omega comunicará os incidentes relevantes e interrupções de serviços relevantes que configurem uma situação de crise, bem como providências adotadas para o reinício dessas atividades para os órgãos externos, quando necessário, através do Departamento Jurídico e Departamento de Comunicação.

5. Programa de capacitação e conscientização

Através das suas plataformas internas, a Omega promove um plano de conscientização recorrente sobre a importância da Segurança da Informação voltada para todo público interno, além de um resumo de segurança divulgado nos portais da empresa.

Anexos

1. Gestão de Acessos
2. Gestão de Mudanças
3. Gestão de Operações
4. Termo de Uso e Política de Privacidade (omegaenergia.com.br) https://omegaenergia.com.br/termos-de-uso?Consumidor

ANEXO 1 • Gestão de Acessos

Objetivo

O processo de concessão de acesso aos ativos de informação da Omega deve levar em conta os recursos necessários para execução de suas tarefas e cargo dentro da empresa, além da autenticidade dessas credenciais de acesso.

Processo

1. Criação de Conta de Acesso

O processo de criação de conta deve geralmente ser derivado do processo de Onboarding, podendo também decorrer de ajustes de perfil e transferência de funções posteriores à contratação. Todo o controle deve ser realizado via abertura de chamado pela equipe de recrutamento e/ou gestor para gerar os devidos fluxos de validações e aprovações, além de garantir a segurança da informação, dados para auditoria e estatísticas de atendimento.

No chamado de contratação devem estar contidas as informações de Folha, Facilities, Microinformática e Sistemas, no qual todas as equipes envolvidas poderão acompanhar o desenvolvimento e atuar na devida ordem para cada equipe.

Nome completo, Data de Nascimento, Data de Início, Empresa, Centro de Custo, Gerente e **CPF** são dados imprescindíveis para o cadastramento nos sistemas e só quando o usuário de rede estiver criado e o e-mail licenciado é que a equipe de Sistemas estará apta a cadastrar o funcionário, devendo atentar-se à data de início para liberação dos dados de acessos encaminhados por e-mail pelo analista de sistemas.

Caso o funcionário a ser cadastrado seja um gerente de área é necessário que a equipe de recrutamento e gestão de pessoas informe se este será dono de um centro de custo e se deverá ser incluído em alguma hierarquia de aprovação, em caso positivo é necessário informar no descritivo do chamado para que seja efetuada tais configurações e assim definir os fluxos corretos nos sistemas.

Para todos os funcionários contratados é liberado o acesso dentro do ERP financeiro os módulos de requisição de compras e prestação de contas, para demais acessos requeridos por área o gestor deve passar para o RH quais os sistemas e perfis adicionais.

Quanto ao processo de contratação de terceiros, o Gestor da área é responsável pela administração do recurso, porém deve comunicar à equipe de gestão de pessoas para que estes providenciem a abertura do chamado para concessão de acesso e possam ter o controle dos terceiros vinculados à empresa.

Dentro dos cadastros nos sistemas é necessário criar um diferenciador de tipo de funcionário afim de facilitar o controle de acessos e auditoria.

2. Alteração de Conta de Acesso

Em sua maioria, é derivado do processo de transferência e deve ser descrito em chamado aberto pela equipe de recrutamento e gestão de pessoas, nele devem estar contidas as informações da nova **Unidade de Negócio, Centro de Custo** e/ou **Gestor**.

O gestor anterior é responsável por verificar junto ao funcionário se há alguma pendência nos processos e o gestor futuro responsável pela validação de acessos do liderado, caso haja necessidade de manutenção de funções ou unidades de negócio, realizar a abertura de chamado destacando as possíveis revogações e/ou inclusões.

Caso o funcionário esteja vinculado à algum fluxo de aprovação, ou seja, dono de centro de custo, é necessário que esteja descrito no chamado qual o novo fluxo a ser criado tanto na unidade de destino como na de origem.

Também se destaca o processo de internalização de terceiros, neste caso é necessário criar um cadastro afim de permitir que haja uma rastreabilidade das operações nas diversas fases de contratação. A atualização decorre de um chamado de Onboarding e ao finalizar a conceção de acesso deve ser comunicado ao colaborador sobre a mudança de logins, a fim de que ele se programe para finalizar todos os fluxos de trabalho no sistema antes de trocar de usuário.

3. Bloqueio de Conta de Acesso

É derivado do processo de rescisão de contrato ou alteração de função. No caso de alteração, este deve ser realizado conforme destacado no processo destacado no item 2, caso a exclusão seja pelo desligamento os processos deverão iniciar com a equipe de gestão de pessoas e gestor a fim de validar possíveis pendências e somente depois abrir chamado para revogação de acessos, a fim de garantir a confidencialidade no processo.

Cabe à Tecnologia da informação realizar uma nova validação de pendências e encerrar os acessos nos sistemas.

Para casos de desligamento com riscos de segurança e/ou confidenciais, a solicitação de bloqueio poderá ser direcionada para a Diretoria de Tecnologia para ação imediata e de exceção. O processo estará evidenciado por e-mail e posterior criação de chamado técnico.

4. Revisão de Acessos e mitigação de erro de processo

Mensalmente é realizada uma revisão dos acessos concedidos a todos os usuários e/ou funcionários da Omega, com base na planilha disponibilizada pelo RH sendo possível liberar, bloquear e/ou ajustar o que for necessário para observância à Política.

Semestralmente é feita a revisão de perfis de acesso em duas frentes. (i) Matriz de Acesso (ii) Usuários por perfil de acesso, conforme exemplo abaixo.

Será encaminhada aos gestores de áreas uma planilha de acessos por usuário, a fim de validar se as contas de acesso e os perfis atrelados estão em acordo com as regras de gestão e controles.
Matriz de Perfil X Revisor

Perfil de Acesso	Revisor
Oracle Contas à Pagar	Gestor da área Financeira
Oracle Contas à Receber	Gestor da área Financeira
Oracle Contabilidade	Gestor da área Contábil
Oracle Ativo Fixo	Gestor da área Contábil
Oracle Requisições	Gestor imediato
Oracle Relatório de Despesas	Gestor imediato
Oracle Alçada de Aprovações	Gestor da área Financeira

ANEXO 2 • Gestão de Mudanças

Objetivo

O andamento e o resultado de uma mudança em sistema ou infraestrutura tecnológica relevante, zela pela preservação dos controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade dos dados, que são geridos pelo Departamento de Tecnologia da Informação de forma planejada, aprovada, testada e obedecendo ao processo de gerenciamento de mudanças.

Processo

O processo de criação de conta deve geralmente ser derivado do processo de Onboarding, podendo também decorrer de ajustes de perfil e transferência de funções posteriores à contratação. Todo o controle deve ser

On Premise e IaaS

Para ambientes físicos e internos da Omega, Nuvem IaaS e Sistemas Corporativos (Oracle, GFT, XRT, etc.), seguiremos o processo de Gestão de Mudança, através de formulário de registro da mudança, comitê semanal para apresentação do objetivo, testes realizados e métodos de rollback e aprovação ou reprovação da mudança. Além disso, o mesmo formulário no Sharepoint possui a possibilidade de solicitar mudanças emergenciais – Casos que necessitem de intervenção imediata e passará por aprovação da liderança. Ambos os casos possuem registro para futuras auditorias e lições aprendidas.

Software Engineering - Cloud

Para ambientes DevOps, seguimos o processo de CI/CD ou seja, seguimos uma automação no agendamento da release, review das alterações em ambiente DEV, sempre por um desenvolvedor diferente do criador do código, Merge do ambiente DEV para ambiente STAGING, Homologação pelo time de QA em ambiente STAGING, Merge do ambiente STAGING para ambiente PROD. Todo Merge só é realizado por Tech Leads. Caso ocorra alguma situação não planejada, o Tech Lead é o responsável por executar o processo de rollback, através do merge da release anterior no ambiente PROD. Todo o processo possui logs de auditoria para futuras auditorias e lições aprendidas.

Importante destacar que a etapa MERGE, dispara CI/CD, ou seja, testes unitários, testes end to end, testes de componentes, segurança, checks e deploy.

Ambientes SaaS

Para ambientes SaaS, seguiremos o processo determinado pela contratada, ou seja, somos avisados pelos parceiros sobre as releases, normalmente trimestrais para todo o ambiente, com antecedência de testes e validações. A equipe Tech tem a responsabilidade de gerenciar as validações previas com os usuários chaves quando necessário e comunicar a empresa sobre essas atualizações.

Mensalmente, na própria reunião de Comitê GMUD, faremos ao final o report de quantidade de mudanças normais, emergenciais, mudanças canceladas e mudanças executadas sem devido processo e aprovação.

ANEXO 3 • Gestão da Operação

Objetivo

Realizar a gestão do ciclo de vida (aquisição, manutenção, atualização, suporte e descarte) dos recursos de tecnologia e telecomunicações da empresa e garantir aos usuários da empresa o pleno uso dos referidos recursos, levando em consideração as boas práticas do mercado e as práticas de segurança da informação definidas nessa Política.

Processo

Suporte e gestão de crises

A área de tecnologia atende às solicitações dos usuários, considerando que estes devem fazer uso adequado dos recursos de tecnologia, através do registro de incidentes, dúvidas, dificuldades ou problemas no uso dos recursos e tecnologia.

A área de tecnologia disponibiliza e organiza canais de comunicação para organização da operação diária:

- **Grupos em plataformas de comunicação**
  Há grupos fixos para o acompanhamento da operação e grupos específicos criados para gestões de crises pontuais.

- **Sistema para reporte de chamados**
  Há o sistema da própria empresa, gerido pela área de tecnologia, e os sistemas de chamados dos fornecedores de serviços, como NOC e SOC.

Monitoramento

A empresa possui monitoramento 24 x 7 em duas frentes:

- **NOC (Network Operations Center)**
  Equipe que monitora a disponibilidade e performance do ambiente de tecnologia.

  Ao ocorrerem alarmes e eventos, o NOC notifica a equipe técnica da área de tecnologia da empresa e, imediatamente, inicia a atuação (junto à provedores de telecomunicações, fornecedores de tecnologia e demais provedores de serviços).

O NOC também atua reativamente, quando usuários relatam problemas ou dúvidas na utilização de recursos de **comunicação** da empresa.

- **SOC (Security Operations Center)**
  Essa equipe monitora, através de ferramentas como SIEM e CAS, o ambiente de tecnologia com foco em segurança da informação, acompanhando constantemente os eventos gerados no ambiente (alertas, alarmes e outros dados provenientes das diversas plataformas utilizadas pela empresa, seja em cloud e on premise).

  Cada alarme ou alerta é devidamente analisado e tratado. De acordo com os níveis de criticidade de cada evento, ações mais ou menos enérgicas podem ser tomadas.

  Os eventos relevantes são notificados por e-mail.

  Os eventos críticos requerem contato telefônico com a área de tecnologia da empresa, em geral após as medidas de mitigação e contenção do risco, ameaça ou incidente terem sido tomadas.

  É realizada uma reunião semanal de acompanhamento dos indicadores relacionados à segurança da informação.