E-mail

- Configuração E-Mail
- Configuração POP3 para GMail
- Listas de e-mail
- Regulamento sistema correio eletrónico
- Configuração Mail Outlook

Configuração E-Mail

Domínio @isr.uc.pt

Os parâmetros genéricos da configuração de clientes de e-mail para todos os endereços de correio electrónico com o domínio **@isr.uc.pt** são os que a seguir se apresentam.

Recepção/Entrada (*Incoming settings*)

Protocolo	IMAP
Nome do Servidor	imap.isr.uc.pt
Segurança	SSL
Porto	993
Método de Autenticação	*Password* (normal)
Utilizador	seu.username@isr.uc.pt
Password	<a sua palavra chave>

Envio/Saída (*Outgoing settings*)

Protocolo	SMTP
Nome do Servidor	smtp.isr.uc.pt
Segurança	STARTTLS
Porto	587
Método de Autenticação	*Password* (normal)
Utilizador	seu.username@isr.uc.pt
Password	<a sua palavra chave>

Webmail

Pode aceder ao sistema Webmail do DEEC, através do endereço https://zimbra.isr.uc.pt

Configuração POP3 para GMail

Apresentam-se abaixo screenshots do procedimento de configuração do cliente POP3 do GMail para o e-mail do ISR, para melhor ilustração do processo.

279

No ponto 5, introduza o seu endereço de e-mail do ISR.

280

281

No ponto 7, introduza a password associada à sua conta do ISR.

No ponto 8, introduza pop3.isr.uc.pt e certifique-se que está seleccionado o porto 995 no ponto 9.

282

Neste momento, o GMail passará a obter e-mail da sua conta do ISR em intervalos regulares.

Listas de e-mail

O ISR Coimbra dispõe de um sistema de listas de correio electrónico, permitindo o contacto célere com todos os serviços e grupos.

Tecnicamente, as listas são suportadas pelo software Mailman e/ou pelo sistema Zimbra/Carbonio. Por este motivo, algumas listas possuem um sistema de moderação, para redução do Spam enviado para as mesmas, sendo que a entrega das mensagens poderá acontecer de forma deferida.

Consulte a lista abaixo para informação detalhada.

Lista	Destinatários
All Users ISR Coimbra *allusers@isr.uc.pt*	Todos os membros do Instituto de Sistemas e Robótica (Pólo de Coimbra)

Regulamento sistema correio eletrónico

A atribuição de conta de e-mail no domínio ISR passa pela solicitação da mesma para o endereço webmanager@isr.uc.pt, com o conhecimento do responsável local no ISR.

Posteriormente, após aprovação, validação dos dados recebidos e criação da conta, será comunicada ao utilizador a informação de configuração para o endereço de e-mail alternativo que foi indicado.

O procedimento de criação de contas passa pela atribuição do username com base no formato primeironome.ultimonome@isr.uc.pt por, nomeadamente, questões de normalização, organização interna, entre outros.

No sentido de combater as crescentes ameaças de segurança informáticas, concretamente nos sistemas de correio electrónico, tornou-se essencial rever e modificar algumas regras e requisitos que regem o funcionamento destes sistemas.

SPF – Sender Policy Framework

Sender Policy Framework (SPF) é um mecanismo que identifica quais os servidores de e-mail autorizados a enviar email em nome do seu domínio, através do sistema de DNS.

Sistemas que enviem e-mail com endereço remetente ***@isr.uc.pt*** serão mais provavelmente classificados como Spam, se não estiverem na lista dos autorizados nos registos SPF.

Se necessitar de um sistema ou serviço que envie e-mail com remetente ***@isr.uc.pt***, deverá entrar em contacto com o informatica@isr.uc.pt, com vista a obter indicações de como proceder.

DKIM – DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) é um mecanismo para validação e garantia de integridade do conteúdo do e-mail durante o seu transporte, no que diz respeito à sua modificação tanto no

conteúdo como nos cabeçalhos. Este mecanismo valida também se os anexos de e-mail, caso existam, não foram alterados durante o transporte desde o remetente até ao destinatário.

É incluída, em todos os emails enviados, uma assinatura digital do servidor emissor.

Este mecanismo permite evitar ataques de spoofing. Spoofing é uma técnica maliciosa de alteração do remetente de uma mensagem para que a vítima abra os e-mails, por exemplo, com vírus ou outras artimanhas maliciosas (phishing, etc.). Isso acontece porque a mensagem maliciosa chega à caixa de e-mail com o remetente de alguém conhecido.

Os sistemas do ISR implementam o sistema DKIM, para aumento da segurança no correio electrónico.

Anti-Spam

A massificação do e-mail como forma de comunicação quotidiana tornou-o num alvo óbvio para as actividades maliciosas de pessoas mal intencionadas. O correio enviado neste contexto é denominado de Spam.

A resposta dos administradores de sistemas para esta ameaça são sistemas e mecanismos cuja função é filtrar e bloquear mensagens não solicitadas e de carácter malicioso, que são denominados de sistemas anti-spam.

Estes sistemas são colocados antes do servidor final, onde o correio é entregue e funcionam normalmente de forma transparente para o utilizador final. Actualmente, todos os fornecedores de serviços de e-mail implementam algum tipo de filtro anti-spam.

Devido à sua natureza, não existe um sistema anti-spam perfeito. Por este motivo, o sistema pode, em situações particulares, reter um e-mail, classificando-o como Spam. Existem formas de recuperar esses e-mails, quando considerado um falso positivo, associado a mecanismos que permitam que tal não se repita.

Devido à descontinuação do serviço Anti-spam em funcionamento no ISR, tornou-se necessário proceder à sua substituição por um novo. Este processo foi alvo de um estudo cuidado das alternativas existentes seguida de uma fase de testes em laboratório, tendo-se optado pela solução MailCleaner.

Características do MailCleaner

O sistema MailCleaner é baseado num conjunto de tecnologias sofisticadas de filtragem que funcionam em conjunto. Os utilizadores finais têm a capacidade de controlo total sobre a função de quarentena: com um simples clique, o utilizador pode apagar ou libertar qualquer mensagem retida pelo filtro.

O MailCleaner implementa um número de técnicas complementares para detecção e bloqueio de Spam, combinando algoritmos de inteligência artificial que se adaptam constantemente para a identificação das técnicas dos spammers sempre em mudança.

O filtro antí-vírus incorporado no MailCleaner filtra mensagens em busca de vírus, worms e anexos suspeitos com conteúdos potencialmente maliciosos.

O MailCleaner consegue reconhecer e classificar newsletters. O utilizador só receberá as newsletters que pretende efectivamente receber e manter as restantes em quarentena.

O MailCleaner possui uma interface Web autenticada para gestão simplificada em regime de Self Service das mensagens em quarentena, listas negras e brancas, entre outras funcionalidades.

O endereço para Self Service é https://antispam.isr.uc.pt.

Configuração Mail Outlook

image-1672674476142.png

image-1672674553916.png

image-1672674637124.png

image-1672674687146.png

image-1672674753418.png