POLÍTICA DE USO DEL CORREO ELECTRÓNICO de la Diputación de Valladolid

Índice de contenidos

1. INTRODUCCIÓN.

Este documento se enmarca en las "**Directrices y Política de Uso y Buenas Prácticas en la utilización de los Sistemas de Información y la Red Corporativa de la Diputación de Valladolid",** siendo de aplicación los objetivos, el ámbito de aplicación, las definiciones, responsabilidades y demás cuestiones tratadas en él.

El presente documento articula de forma específica, dentro de este marco, la política de uso del correo electrónico que provee la Diputación de Valladolid, reflejando recomendaciones de buen uso y medidas de protección.

El correo electrónico es uno de los principales servicios de comunicaciones electrónicas en una organización, por lo que es responsabilidad de la misma garantizar una adecuada gestión del mismo y unas políticas de uso adecuadas así como una adecuada seguridad.

Asimismo, la calidad y seguridad del servicio depende del uso individual que se realice por lo que es muy importante que el usuario conozca sus obligaciones así como recomendaciones de uso y buenas prácticas para contribuir a una utilización adecuada de los recursos.

2. OBJETO Y ALCANCE

El objeto de este documento es establecer la política de uso del servicio de correo electrónico corporativo en la Diputación de Valladolid y de los organismos a los que la Diputación provea de este servicio de comunicaciones y cuyos dominios gestione.

Afecta, por tanto, a todas las direcciones de correo electrónico del dominio @dip-valladolid.es, y de todos los dominios singulares registrados por la Diputación de Valladolid.

Podrá solicitar y utilizar una cuenta de correo electrónico de la Diputación de Valladolid su personal funcionario, contratado, laboral o becario en activo, así como el personal de esta misma tipología que pertenezca a organismos a los que la Diputación provea del servicio de correo electrónico, en cualquier caso con las limitaciones que marca este documento.

Como norma general, no se podrán asignar cuentas de correo a personal de empresas de servicio contratadas. Si, por alguna razón excepcional esto fuera preciso, la cuenta será de uso temporal, debiendo ser autorizada previamente por el responsable del área tecnológica de la Diputación de Valladolid.

La posesión de una cuenta de correo no implicará EN NINGÚN CASO una vinculación laboral con la Diputación de Valladolid. Se considera una herramienta de trabajo necesaria para que el personal pueda desempeñar su labor eficazmente en la organización.

3. CUENTAS Y BUZONES DE CORREO

3.1. Tipología

Se pueden distinguir tres tipos de cuentas: Personales, Institucionales y Organizativas.

- Cuentas Personales: Identifican la dirección de correo electrónico de una persona.
- Cuentas Institucionales: Están asociadas a cargos. Una persona tendrá acceso a una cuenta institucional en función de su cargo o de su actividad.
- Cuentas Organizativas: Las cuentas organizativas están orientadas fundamentalmente a unidades, grupos y servicios. Pueden ser utilizadas por una o varias personas conjuntamente y son gestionadas por un responsable. Por consiguiente, este tipo de cuentas no están asociadas a cargos o personas.

3.2. SOLICITUD Y CREACIÓN

Para disponer de una cuenta en un dominio alojado en la plataforma de correo de la Diputación de Valladolid se deberá realizar una petición a través de los formularios y procedimientos disponibles en Portal de Soporte TIC (http://soporteTIC.diputaciondevalladolid.es).

Las cuentas personales deben ser solicitadas por el responsable del departamento o servicio al que pertenezca el trabajador.

Las cuentas institucionales se crean a petición del Área correspondiente.

La solicitud de una cuenta organizativa o genérica debe ser realizada por las unidades, departamentos o grupos al administrador del dominio de correo. Se requiere definir el responsable de la misma, que será el interlocutor o persona de contacto con los equipos de administración de correo.

3.3. VIGENCIA, DESACTIVACIÓN Y ELIMINACIÓN DE CUENTAS DE CORREO

3.3.1. Vigencia

Cuentas personales

Se podrá disponer de una cuenta de correo personal hasta 3 meses después de la fecha de baja o extinción de la situación que originó la creación de la cuenta en la

Diputación de Valladolid. Excepcionalmente, este periodo podrá variar por necesidades del servicio debidamente motivadas.

A la finalización del plazo mencionado, se procederá a la cancelación de la cuenta y al consiguiente borrado de los correos almacenados.

Para aquellas cuentas utilizadas por personal externo o ajeno a la Diputación, el responsable de la persona ante la Diputación deberá poner en conocimiento del administrador de correo la baja de dicha persona para que se proceda, entre otras acciones, a la cancelación de su cuenta en un plazo máximo de 3 meses desde la fecha de baja.

Cuentas institucionales

Las cuentas institucionales permanecen hasta que desaparece el cargo o función que las motivó; por lo que serán utilizadas por las personas que ocupan ese cargo o función a lo largo del tiempo. Dado que los usuarios de las cuentas lo hacen en función de su situación, la asignación de personas a cuentas se realiza directamente desde los servicios centrales de la Diputación de Valladolid.

La baja de la persona en el cargo implica el cambio de contraseña de la cuenta de correo institucional.

Cuentas organizativas

Este tipo de cuentas se cancelan o gestionan a petición de la unidad o persona responsable de las mismas.

3.3.2. Procedimientos de desactivación y eliminación

Borrado automático de cuentas.

Se eliminarán aquellas cuentas de correo que no han sido consultadas durante un periodo continuado de un año, salvo causa justificada. Esto conlleva el borrado de los correos almacenados en dicha cuenta.

Cancelación voluntaria de cuentas.

Se podrá solicitar el cierre o cancelación de una cuenta de correo. Para ello, su titular deberá realizar la solicitud al administrador del dominio de correo, quién hará efectiva la solicitud tras la comprobación de su veracidad y la remisión de un correo de confirmación al solicitante dos días antes de efectuar la cancelación de la cuenta.

La cancelación de una cuenta implica:

- la imposibilidad de enviar y recibir nuevos correos.
- la eliminación de los correos almacenados.

Desactivación temporal de cuentas.

El uso inapropiado o el abuso en el servicio de correo electrónico puede ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido se pueden llevar a cabo en función de las posibles repercusiones en el buen funcionamiento del servicio.

La desactivación de la cuenta implica la imposibilidad de enviar y recibir nuevos correos mientras no vuelva a ser activada.

Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio, se podrá cambiar la contraseña de una cuenta.

3.4. FORMATO DE LAS DIRECCIONES DE CORREO

Las cuentas personales correspondientes al dominio institucional se ajustan a los siguientes criterios:

- La forma común de una cuenta de correo electrónico será la siguiente: nombre.apellido1@dominio.
- En el caso de que la forma común ya exista y esté utilizada por otro usuario, el orden de selección de alternativas para asignar la denominación de la cuenta será:
    - Inicial.apellido1@domino
    - Inicial.apellido1.apellido2@dominio
    - Nombre.apellido1.apellido2@dominio

- Los caracteres con tilde son sustituidos por el mismo carácter sin tilde.
- El carácter ñ es sustituido por la letra n.
- El carácter "." es un separador obligatorio entre nombre y apellidos o iniciales.
- Para el caso de nombres compuestos o apellidos compuestos se podrá optar por abreviaturas en los campos nombre, apellido1 y apellido2.

3.5. TAMAÑO DE LOS BUZONES DE CORREO

El sistema enviará mensajes automáticamente a los usuarios que tengan tamaños de buzón muy elevado, con el objetivo de que realicen tareas de depuración y limpieza en sus buzones. Estos mensajes estarán perfectamente identificados e irán dirigidos a concienciar en el buen uso de recursos compartidos. En ningún caso, se le pedirá al usuario claves y contraseñas de acceso.

Por razones de gestión de recursos compartidos, los buzones de correo serán susceptibles de ser limitados en cuanto a su capacidad máxima, la cual podrá ir regulándose y variar a lo largo del tiempo. En ese caso, siempre que la ocupación del buzón de correo fuera superior al 90% del tamaño que se asigne, el sistema automáticamente enviaría una notificación al usuario, con el fin de que pueda tomar las medidas pertinentes. Una vez alcanzado el 100% de la cuota que se asignara, todos los mensajes serían rechazados por el sistema, siendo necesario que el usuario hiciera limpieza en el buzón para restablecer la recepción normal de mensajes.

3.6. ENVÍO Y RECEPCIÓN DE MENSAJES

Se ha de considerar que el correo enviado circula por distintos servidores de Internet y que éstos imponen libremente restricciones sobre los tamaños admitidos, por lo que cuanto más grande sea el tamaño del mensaje de correo mayor es la probabilidad de que sea rechazado, impidiendo, de este modo, que llegue a su destino.

Para el envío de ficheros de gran tamaño, se recomienda el uso del Servicio Maletín, que permite compartir ficheros grandes en vez de enviarlos por correo electrónico.

El tamaño máximo de los correos que se pueden enviar y recibir se podrá modificar sin previo aviso. Asimismo y por razones de disponibilidad del servicio se podrán incluir otro tipo de restricciones, como limitar el número máximo de mensajes enviados desde una cuenta durante un período de tiempo o el número máximo de destinatarios por envío de correo.

Es obligatorio enviar un correo con una dirección de retorno válida y propia del sistema a través del cual se está enviando el correo. No se podrá usar como remitente direcciones externas de otros proveedores.

4. SEGURIDAD

Son múltiples los problemas de seguridad que pueden afectar al correo electrónico, entre los que cabe destacar:

- Robo de identidad. Phishing, Pharming…
- Virus: Virus y sobre todo los gusanos que utilizan técnicas de spam para propagarse después de infectar un PC
- Combinación de virus y spam. Las últimas generaciones de virus se han creado para ayudar a los spammers. Muchos spammers han incorporado código malicioso en su spam.
- Ataques con direcciones falsificadas. Consiste en inundar el servidor de un dominio real con los errores generados por una máquina atacada al procesar spam para distribuirlo a miles de destinatarios. El spammer coloca como dirección receptora de estos errores un dominio real y un usuario aleatorio. Esto provocará problemas de ancho banda, colapso del servidor (colas, disco etc.). Puede ser considerado una Ataque de denegación de Servicio.
- Generación innecesaria de tráfico SMTP. El envío y encaminamiento de un simple mensaje de correo electrónico implica el uso de varios recursos: conexiones SMTP, consultas DNS, procesamientos por MTA. Los propios errores de SMTP, el spam, los virus etc., generan informes a direcciones falsificadas provocando confusión en los usuarios y generando un exceso de tráfico

Por lo anterior se especifican las siguientes recomendaciones generales:

- La contraseña de acceso al correo no debe ser cedida o facilitada a otros usuarios, siendo responsabilidad del propio usuario su custodia.
- La transmisión del binomio usuario/clave debe realizarse de forma cifrada mediante la activación de protocolos seguros en los clientes de correo (SSL o TLS, según los clientes de correo).
- En caso de que su cliente de correo no admita los protocolos seguros de POPs e IMAPs, se debe actualizar la versión del cliente o utilizar un cliente que ofrezca dichos métodos.

Desde la Diputación de Valladolid y servicios de soporte TIC no se solicitará NUNCA a los usuarios las contraseñas de los servicios que se ofrecen. Ante una sospecha no se deberá abrir o responder a los mensajes. Ante cualquier duda, se deberá contactar con el Soporte TIC de la organización.

La Diputación dispone de un sistema encargado de eliminar el spam, basado en listas de reputación de los servidores que envían correos. El sistema ha sido configurado de modo que son eliminados aquellos mensajes considerados. Si un

correo de origen externo se cataloga como SPAM se marca la cabecera (el Asunto o Subject) con la etiqueta [SPAM].

Los servidores antivirus de la Diputación analizan todo el tráfico de correo entrante y saliente, y rechazan el envío de mensajes que contienen virus. Cuando un mensaje es rechazado se envía una notificación al destinatario, marcando en la cabecera (el Asunto o Subject) la etiqueta [ANÁLISIS ANTIVIRUS]. En ocasiones, los correos sospechosos de contener virus son movidos a carpetas denominadas "Cuarentena".

Por imperativos legales, las trazas del tránsito SMTP de los servidores de correo que gestiona la plataforma de correo de la Diputación se guardan por un periodo de 12 meses. Dichas trazas contienen los siguientes datos: IP de origen, remitente, destinatario fecha y hora y, si es pertinente, (salvo que se eliminase el correo por listas negras) el servidor de destino que ha procesado el correo.

La existencia de logs tiene carácter obligatorio debido a la normativa legal reguladora y es muy útil para:

- Ofrecer información oficial y completa de si un determinado mensaje ha sido entregado, a qué hora y a qué servidor.
- Localizar trazas concretas de mensajes en caso de algún tipo de incidente.
- Por motivos estadísticos.

Aquellos organismos que tengan sus cuentas de correo en la plataforma corporativa de la Diputación, deberán solicitar la obtención de logs al área tecnológica de la Diputación.

5. ENTREGA Y ENVÍO DE LOS MENSAJES

Aunque en un tanto por cierto muy elevado de los casos los mensajes de correo electrónico llegan a su destino rápidamente, en ningún caso el servicio de correo electrónico garantiza de forma absoluta la entrega de un mensaje.

Generalmente los servidores de correo de la Diputación envían un correo al emisor debido a las siguientes incidencias: caídas imprevistas en las líneas de comunicaciones, límites de almacenamiento en los buzones del usuario receptor, rechazo de mensajes por virus, exceso de tamaño para el servidor que recibe, direcciones mal formadas, etc.

Es responsabilidad del propio usuario leer los mensajes de retorno que los sistemas de correo le envíen notificándole cualquiera de estas incidencias en la entrega de los mensajes remitidos por él.

Los únicos servidores autorizados a enviar correos al exterior de la red corporativa de la Diputación de Valladolid son aquellos gestionados por los servicios tecnológicos de la organización. En ningún caso un ordenador personal podrá realizar esta tarea y para enviar correo deberá entregarse a un servidor autorizado para su posterior procesamiento.

En los cortafuegos corporativos, el puerto 25 permitirá únicamente el tráfico desde los servidores de correo registrados y bloqueará el tráfico proveniente de los ordenadores personales.

Se recomienda, siempre que sea posible, el uso de la directiva SPF (Sender Policy Framework) al menos en la versión 1 (RFC 4408), tanto en su forma pasiva, es decir, incluyendo los registros DNS que indiquen las máquinas que están autorizadas a generar correo desde el dominio, como en su forma activa, utilizando métodos de verificación SPF en los servidores de correo receptores.

6. TÉRMINOS Y CONDICIONES DE USO DEL CORREO ELECTRÓNICO

Si tiene cualquier duda o cuestión sobre el servicio de correo electrónico, diríjase al Help Desk de Soporte Tecnológico (SoporteTIC@dip-valladolid.es). Si conoce o sospecha de un uso fraudulento de sus datos de acceso por parte de terceros deberá notificarlo a esta dirección. En general se comunicarán los malos usos en relación al correo electrónico y todos los problemas con procesamiento de mensajes de correo, además de permitir ponerse en contacto con los responsables del servicio.

Para el desarrollo del trabajo y de las funciones que los empleados públicos tienen encomendadas, respetando los principios de libertad de expresión y privacidad de información, se les ofrecen un serie de recursos de red, comunicaciones y de información. El acceso a estos recursos es un privilegio que está condicionado a la aceptación de la política de utilización de estos recursos. Se debe reconocer que la calidad de estos servicios depende en gran medida de la responsabilidad individual de los usuarios.

Las condiciones que se exponen se irán actualizando para acoplarse a nuevas situaciones.

- Los usuarios del servicio de correo son responsables de las actividades realizadas con sus cuentas y buzones asociados en esta organización. En todo momento deberán cumplir las Directrices, Política de Uso y Buenas Prácticas en el acceso a los Sistemas de Información y la Red Corporativa de la Diputación de Valladolid.

  Esta responsabilidad supone el cuidado de los recursos que integran dicha cuenta y, particularmente, de los elementos, como la contraseña, que pueden permitir el acceso indebido de terceras personas a dicha cuenta o a otros recursos personales que utilicen ese identificador. Se recomienda cambiar la contraseña de forma periódica, como medida de seguridad.

- Está prohibido facilitar y/o permitir el uso de la cuenta y buzón a cualquier otra persona distinta del propio usuario

- Los usuarios deben ser conscientes de la diferencia de utilizar direcciones de correo electrónico suministradas por la organización o privadas, ofrecidas por cualquier proveedor de Internet. El campo remitente de las cabeceras de correo indica el origen al que pertenece el emisor de un mensaje, por lo que hay que tener en cuenta las posibles repercusiones.

- Correo personal. Los servicios de correo electrónico suministrados por nuestra organización pueden ser usados, de forma incidental, para temas personales excepto si:

  - interfieren con el rendimiento del propio servicio,
  - interfieren en las labores propias de los gestores del servicio

- suponen un alto coste para nuestra organización.

Los mensajes de tipo personal están sujetos a los términos y condiciones de este documento.

- El usuario debe de ser consciente de los términos, prohibiciones y perjuicios englobados en Abuso en el Correo Electrónico.
- Es incorrecto enviar mensajes con direcciones (remitente) no asignadas por los responsables de nuestra organización y, en general, es ilegal manipular las cabeceras de correo electrónico saliente.
- El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión masiva e indiscriminada de información. Para ello existen otros canales más adecuados y efectivos, para lo que debe de ponerse en contacto con los responsables del servicio.
- La violación de la seguridad de los sistemas y/o red puede incurrir en responsabilidades penales.
- No es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener esta práctica deberá hacerlo. Si nuestra organización recibe quejas, denuncias o reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.
- Está completamente prohibido realizar cualquier de los tipos definidos en el Abuso de Correo Electrónico (ver apartado 7). Además de las siguientes actividades:
    - Utilizar el correo electrónico para cualquier propósito comercial o financiero.
    - Participar en la propagación de cartas encadenadas, participar en esquemas piramidales o similares.
    - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra organización.
    - Falsificar las cabeceras de correo electrónico.
    - Utilizar las cuentas de nuestra organización para recoger correo de buzones de otro Proveedor de Internet.
    - Utilizar mecanismos y sistemas que intenten ocultar la identidad del emisor del correo.
    - Está prohibida la suplantación de identidad de otra persona en el envío de mensajes de correo electrónico, actividad tipificada como infracción en la Ley General de Telecomunicaciones.
- Estará penalizado con la cancelación del buzón, el envío a foros de discusión (listas de distribución y/o newsgroups) de mensajes que comprometan la reputación de nuestra organización o violen cualquiera de las leyes españolas.

7. ABUSO EN EL CORREO ELECTRÓNICO

Documento de RedIRIS asumido por la Diputación de Valladolid.

http://www.RedIRIS.es/mail/abuso/ace.es.html

Introducción

Definimos ACE (Abuso en Correo Electrónico) como las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios. Algunos de los términos habitualmente asociados en Internet a estos tipos de abuso son spamming, mail bombing, unsolicited bulk email (UBE), unsolicited commercial email (UCE), junk mail, etc., abarcando un amplio abanico de formas de difusión.

De los tipos de abuso englobados en ACE, el que más destaca es el conocido como spam que es un término aplicado a mensajes distribuidos a una gran cantidad de destinatarios de forma indiscriminada. En la mayoría de los casos el emisor de estos mensajes es desconocido y generalmente es imposible responderlo (reply) de la forma habitual o incluso llegar a identificar una dirección de retorno correcta.

Tipos de abuso

Las actividades catalogadas como ACE se pueden clasificar en cuatro grandes grupos:

- Difusión de contenido inadecuado.
    - Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general... Más información sobre estostemas en el área de información legal.
    - Contenido fuera de contexto en un foro temático. Pueden definir lo que es admisible: el moderador del foro, si existe; su administrador o propietario, en caso contrario, o los usuarios del mismo en condiciones definidas previamente al establecerlo (por ejemplo, mayoría simple en una lista de correo).
- Difusión a través de canales no autorizados. Uso no autorizado de un servidor de correo ajeno para reenviar correo propio. Aunque el mensaje en sí sea legítimo, se están utilizando recursos ajenos sin su consentimiento (nada que objetar cuando se trata de una servidor de uso público, declarada como tal).
- Difusión masiva no autorizada. El uso de servidores de correo propios o ajenos para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado se considera inadecuado por varios motivos, pero

principalmente éste: el anunciante descarga en transmisores y destinatarios el coste de sus operaciones publicitarias, tanto si quieren como si no.

- Ataques con objeto de imposibilitar o dificultar el servicio. Dirigido a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de las líneas, de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario. Se puede considerar como una inversión del concepto de difusión masiva (1->n),en el sentido de que es un ataque (n->1).

  En inglés estos ataques se conocen como mail bombing, y son un caso particular de denial of service (DoS). En castellano podemos llamarlos bomba de correo o saturación, siendo un caso particular de denegación de servicio.

  Suscripción indiscriminada a listas de correo. Es una versión del ataque anterior, en la que de forma automatizada se suscribe a la víctima a miles de listas de correo. Dado que en este caso los ataques no vienen de una sola dirección, sino varias, son mucho más difíciles de atajar.

Problemas ocasionados

- Efectos en los receptores. Los usuarios afectados por el ACE lo son en dos aspectos: costes económicos y costes sociales. También se debe considerar la pérdida de tiempo que suponen, y que puede entenderse como un coste económico indirecto.

  Si se multiplica el coste de un mensaje a un receptor por los millones de mensajes distribuidos puede hacerse una idea de la magnitud económica, y del porcentaje mínimo de la misma que es asumido por el emisor. En lo que respecta a los costes sociales del ACE debe considerarse, aparte de la molestia u ofensa asociada a determinados contenidos, la inhibición del derecho a publicar la propia dirección en medios como News o Web por miedo a que sea capturada.

- Efectos en los operadores. Los operadores de destino y encaminamiento acarrean su parte del coste: tiempo de proceso, espacio en disco, ancho de banda, y sobre todo tiempo adicional de personal dedicado a solucionar estos problemas en situaciones de saturación.

8. ANEXO. GLOSARIO DE TÉRMINOS

Cuenta de Correo Electrónico. Servicio online que permite el envío, recepción y almacenamiento de mensajes de correo electrónico. Toda cuenta está asociada a una o varias direcciones.

A una cuenta de correo se puede acceder a través de un cliente de correo (Outlook, Thunderbird, …) o mediante un servicio de correo Web –Webmail-.

Plataforma corporativa de correo electrónico de la Diputación. Dispone de servicios de correo POP, IMAP, Correo Web, Envío de ficheros de gran tamaño, Almacenamiento y Recuperación de mensajes.

SMTP. El correo en Internet es procesado por máquinas o servidores de origen, de encaminamiento y de destino utilizando el estándar de correo SMTP. Los agentes implicados en la transferencia de correo son:

- Operador de Origen: Es la organización responsable de la máquina que encamina el mensaje de correo hacia Internet.
- Operador de Encaminamiento: Es la organización responsable de las máquinas que encaminan el mensaje de correo entre el operador de origen y el operador de destino).
- Operador de Destino: Es la organización o responsable de la máquina que mantiene el control de los buzones de los destinatarios.
- Emisor: Es la persona origen del mensaje. Incluso cuando el emisor es un programa o sistema operativo, habrá una o más personas que sea(n) responsable(s) del mismo.
- Receptor: Es la persona que recibe el mensaje. Al igual que en el caso del receptor, puede no tratarse de una persona física, pero siempre habrá al menos un responsable más o menos directo de cada dirección de destino.
- Listas de correo: Son receptores de correo que actúan distribuyendo el mensaje a un número de destinatarios. Se las puede considerar como una especie de encaminadoras de correo. Estas listas pueden ser gestionadas por una persona o por un proceso automático. No se les considera emisores ni receptores propiamente dichos, ya que la lista no es ni el origen ni el destinatario final de los mensajes. Sin embargo, pueden considerarse como tal en algunos casos: por ejemplo, los mensajes de control enviados para darse de alta o baja de una lista, y las respuestas del servidor a dichas acciones. Incluso en esos casos hay una persona detrás del servidor: el administrador del mismo.

POP y POPs: protocolo que permite a los usuarios descargar el correo electrónico, almacenado en un servidor de correo, mientras tienen conexión y revisarlo posteriormente incluso estando desconectados poder gestionar los correos sin tener que estar conectado. POPs es la versión segura y encriptada del protocolo POP.

IMAP y IMAPs: Los clientes de correo electrónico que utilizan IMAP dejan por lo general los mensajes en el servidor hasta que el usuario los elimina directamente. Esto y otros factores hacen que la operación de IMAP permita a múltiples clientes acceder al mismo buzón de correo. IMAP permite especificar carpetas del lado servidor. El protocolo IMAP permite los modos de operación conectado y desconectado. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP. IMAPs es la versión segura y encriptada del protocolo IMAP.

Encriptación: El uso de protocolos seguros permite que las credenciales del usuarios transiten por internet de forma seguras y encriptadas.