

Índice de contenido

1	Introducción y objetivos	2
2	Ámbito de aplicación	2
3	Términos y condiciones de uso del servicio de correo electrónico	2
4	Tipos de cuentas de correo electrónico	3
4.1	Cuentas de correo personales	3
4.2	Cuentas de correo no personales	4
4.3	Alias	4
5	Formato de las cuentas de correo electrónico institucionales de la UMU	5
6	Operativa del servicio	5
6.1	Creación de cuentas de correo electrónico	5
6.2	Estados de las cuentas de correo	7
6.3	Cancelación de cuentas de correo	8
6.4	Gestión del buzón de correo electrónico	8
6.5	Mantenimiento del servicio	9
6.6	Gestión de incidencias	9
6.7	Copias de seguridad	10
6.8	Supervisión y monitorización	10
6.9	Registro de eventos	10
6.10	Estadísticas del servicio	11
6.11	Encaminamiento del correo	11
6.12	Detección y eliminación de virus	11
6.13	Detección y eliminación de correo basura (spam)	12
7	Identidad del usuario de correo electrónico	14
8	Confidencialidad del servicio de correo electrónico	14
9	Integridad de los mensajes de correo	14
10	Límites y parámetros de gestión del servicio de correo electrónico	15
11	Política Institucional de la UMU frente al ACE	16
12	Abuso en el Correo Electrónico (ACE)	18

1 Introducción y objetivos

El servicio de correo electrónico (en adelante correo) consiste en la disponibilidad de una dirección de correo electrónico y de un espacio de almacenamiento de mensajes (en adelante buzón de correo).

El objetivo del servicio de correo es dotar de una herramienta útil para el desarrollo de las labores de aprendizaje, docencia, investigación o administración de los distintos colectivos de la Universidad de Murcia (alumnos, PDI, PAS) así como de otras personas vinculadas con la UMU aunque no formen parte de los citados colectivos.

2 Ámbito de aplicación

Esta norma regula el uso de los recursos informáticos y telemáticos del servicio de correo en los servidores institucionales de la Universidad de Murcia sin perjuicio de las normas y políticas de seguridad de uso generales proporcionados por ATICA, por las normas y disposiciones de la Universidad de Murcia y por otras leyes de categoría superior que en su momento puedan aplicarse.

Las condiciones que aquí se exponen pueden ser actualizadas para adecuarlas a nuevas situaciones. En particular los plazos de tiempo o límites de espacio en disco que se citan en el presente documento pueden ser modificados en función de las necesidades del servicio y de su evolución en el tiempo.

3 Términos y condiciones de uso del servicio de correo electrónico

A los términos y condiciones que con carácter general se aplican a todos los servicios proporcionados por ATICA, el usuario de una cuenta de correo electrónico de la UMU se compromete a aceptar y cumplir los siguientes:

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo en nuestra organización
- está prohibido facilitar u ofrecer la cuenta de correo personal (la clave de acceso al servicio) a terceras personas
- se permite usar la cuenta para actividades privadas, actividades no relacionadas con la educación e investigación o gestión administrativa de la UMU siempre que no interfieran con el objetivo principal indicado en el capítulo 1 del presente documento
- debe ser consciente de los términos, prohibiciones y perjuicios indicados en el documento "Abuso en el Correo Electrónico" (capítulo 11 del presente documento)
- está prohibida la utilización en nuestras instalaciones de cuentas de correo de otros proveedores de Internet

- no se permite utilizar como encaminador de correo otras máquinas que no sean las puestas a disposición por nuestra organización
- no se permite enviar mensajes con direcciones no asignadas por los responsables de nuestra institución 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 un herramienta de difusión masiva e indiscriminada de información. Para ello existen otros canales mas adecuados y efectivos
- no es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener ésta práctica deberá de hacerlo. Si nuestra organización recibe quejas, denuncias o reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas
- está completamente prohibido realizar cualquier abuso de los tipos definidos en el capítulo 12 "Abuso en el Correo Electrónico", además de cualquiera de las siguientes actividades:
 - utilizar el correo electrónico para cualquier propósito comercial o financiero
 - no se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares
 - distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra organización
- estará penalizado el envío a foros de discusión (listas de distribución y/o grupos de noticias) de mensajes que comprometan la reputación de nuestra organización o violen cualquiera de las leyes españolas

Para asegurar un normal funcionamiento del servicio y un uso eficiente de los recursos del sistema de correo el usuario se compromete a:

- leer periódicamente su correo
- hacer un uso responsable de la opción "dejar mensajes en el servidor" (leave mail on server), vaciando periódicamente su buzón, de forma que su tamaño no sea excesivo
- hacer uso de la opción "Avisar durante ausencias" cuando el usuario prevea no poder leer el correo durante un intervalo de tiempo largo
- hacer uso de la opción "Redireccionar el correo" cuando el usuario desee recibir el correo en una cuenta alternativa
- avisar de cualquier incidencia que pueda surgir y que estime puede afectar al normal comportamiento del servicio

Si, en el ejercicio de sus funciones, el personal informático detecta cualquier anomalía que muestre indicios de usos ilícitos, lo pondrá en conocimiento de la autoridad competente de la UMU y, si procede, de la autoridad judicial.

En caso de no entender completamente alguno de estos apartados puede enviar un mensaje a la dirección postmaster@um.es solicitando le sea aclarado.

4 Tipos de cuentas de correo electrónico

4.1 Cuentas de correo personales

Las usadas por personas pertenecientes a alguno de los siguientes colectivos:

- Personal Docente e Investigador (PDI)
- Personal de Administración y Servicios (PAS)
- Alumnos
- Otros colectivos cuya relación con la UMU esté formalmente constituida: becarios, trabajadores externos, etc.

El responsable de una cuenta de correo personal es el titular (usuario) de la misma.

Sólo se permite una cuenta de correo personal por persona.

4.2 Cuentas de correo no personales

Además de las cuentas de correo personales los responsables de las distintas unidades organizativas de la UMU podrán solicitar cuentas de correo no personales siempre que estén justificadas y sean necesarias para el normal funcionamiento de la unidad.

Las cuentas de correo no personales estarán vinculadas a una unidad organizativa, siendo el jefe de dicha unidad el responsable de la cuenta.

Cuando las circunstancias lo requieran, el jefe de la unidad podrá delegar el uso de la cuenta de correo no personal a una o más personas, siempre que tengan relación formal con la UMU y realicen labores dentro de la unidad en cuestión. La delegación se hará efectiva en el mismo momento en que el jefe de la unidad comunique la clave de acceso al servicio al resto de usuarios de la cuenta. A partir de este momento la responsabilidad sobre el uso de dicha cuenta de correo será conjunta, del jefe de la unidad y de las personas en quien delega. Queda a criterio del jefe de la unidad el formalizar mediante escrito o cualquier otro medio la cesión en el uso de la cuenta de correo.

Las cuentas de correo no personales no pueden ser usadas bajo ningún concepto para otros fines que no sean los propios de la unidad a la que pertenece y que motivaron su creación.

En último término será la autoridad competente de la UMU la que decidirá a qué unidad organizativa pertenece cada una de las direcciones no personales ya existentes de la UMU, si procede su eliminación o si procede su mantenimiento.

4.3 Alias

Un alias es una dirección de correo que agrupa a una o más cuentas de correo. A diferencia de una cuenta de correo, los alias no tienen buzón ni clave para acceder al mismo. Los alias se usarán para:

- redirigir el correo a la dirección nueva en los casos en los que se proceda a cambiar el nombre de una dirección de correo antigua
- crear listas de correo
- crear direcciones de correo no personales que agrupen a una o más direcciones de correo

Siempre que las circunstancias lo aconsejen prevalecerá la creación de direcciones de correo no personales mediante alias antes que mediante cuentas de correo.

A diferencia del resto de cuentas de correo electrónico, los alias no permiten autenticar el envío de mensajes de correo electrónico.

Los criterios y normas aplicadas a los alias son los mismos que los indicados arriba para las cuentas de correo.

5 Formato de las cuentas de correo electrónico institucionales de la UMU

Todas las cuentas de correo electrónico institucionales gestionadas por ATICA se ajustan al siguiente formato xxxxxx@um.es, donde xxxxxx es el **login** o identificador de la cuenta de correo y **@um.es** es el dominio de correo electrónico institucional de la UMU.

Salvo causas justificadas, no se permite cambiar el login de la dirección de correo electrónico. En caso de que el cambio de login se produzca, es responsabilidad del usuario informar del cambio de su dirección de correo a las personas o sistemas a los que les coste la dirección antigua; así como cambiar la antigua dirección por la nueva en cualquier documento en el que conste la antigua, sea cual sea el soporte físico del documento (papel, electrónico, magnético, etc.)

No obstante, ATICA se compromete a reencaminar el correo dirigido a la antigua cuenta de correo a la cuenta de correo nueva durante el plazo indicado en el parámetro "**antigüedad máxima de una dirección de correo a extinguir**" (ver capítulo 10: Límites y parámetros de gestión del servicio de correo electrónico). Una vez cumplido el plazo, los mensajes que sigan llegando a la dirección antigua serán rechazados con un código de error "usuario desconocido".

6 Operativa del servicio

6.1 Creación de cuentas de correo electrónico

Cuentas de correo personales

Dos son las condiciones que deben darse para crear una cuenta de correo personal:

1. El usuario de la cuenta debe tener una relación formal y vigente con la UMU, apareciendo sus datos de filiación en las bases de datos de ATICA. Esto es, la persona en cuestión pertenece al colectivo PDI, PAS o alumno o bien a otro colectivo conocido de la UMU (becario, trabajador externo, etc.)
2. Pertenece a un colectivo con derecho a obtener una cuenta de correo.

El PDI, PAS y alumnos de la UMU siempre tienen derecho a obtener una cuenta de correo. La autoridad competente de la UMU decidirá qué otros colectivos de la UMU (al margen de PDI, PAS y alumnos) tienen derecho a obtener una cuenta de correo.

Cuentas de correo no personales

El solicitante de la cuenta debe estar autorizado para obtener una cuenta de correo no personal. Normalmente estarán autorizados de oficio los responsables de cada unidad organizativa: jefes de sección, departamento, servicio, etc.

La autoridad competente de la UMU decide, en cualquier caso, qué personas están autorizadas para solicitar y obtener cuentas de correo no personales independientemente del cargo que ocupen.

Procedimiento de creación de las cuentas de correo

Siempre que sea posible, la solicitud de creación de la cuenta de correo se efectuará por medios informáticos, para ello el solicitante de la cuenta deberá acreditar su identidad mediante certificado digital personal.

Cuando el solicitante no disponga de certificado digital y no pueda solicitar la cuenta por medios informáticos, ATICA pondrá a disposición de los usuarios un formulario, el cual deberá cumplimentarse y ser dirigido a ATICA debidamente sellado por el jefe de la unidad organizativa de la UMU interesado en la creación de la cuenta de correo. En este caso es responsabilidad del jefe de la unidad organizativa el comprobar la identidad del usuario de la cuenta cuando se trate de cuentas personales.

Una vez comprobada la identidad del solicitante y el derecho a obtener una cuenta de correo, se procederá a la creación de la cuenta. La creación de la cuenta puede postergarse por motivos técnicos justificados, en cualquier caso ATICA informará al solicitante por los medios que considere más conveniente de:

- cuándo ha sido o será creada la cuenta
- la clave de acceso a la misma
- parámetros de configuración para usar la cuenta de correo
- a qué listas de correo corporativas de la UMU ha sido suscrita la cuenta
- normativa general de uso del servicio de correo

En el caso de que la solicitud sea rechazada se informará al usuario de los motivos del rechazo.

Cuando las circunstancias lo aconsejen (procesos de automatrícula, nuevas adscripciones del PAS, etc.) ATICA podrá crear cuentas de correo sin que medie solicitud previa del usuario o responsable de la cuenta de correo.

En cualquier caso, el procedimiento de solicitud y obtención de cuentas de correo puede variar en función de las necesidades y circunstancias particulares de cada momento.

La creación de la cuenta de correo lleva pareja el alta automática en todos o alguno de estos servicios:

- listas de correo: la nueva cuenta será suscrita automáticamente a las listas de correo que le correspondan en función de las características del usuario propietario
- directorio público: la nueva cuenta aparecerá como un atributo más de la persona propietaria en el directorio corporativo de la UMU
- servicio de acceso remoto vía Infovía Plus
- servicio de redes privadas virtuales (RPV/VPN)

6.2 Estados de las cuentas de correo

Se tienen en cuenta los siguientes estados en una cuenta de correo:

- **activa:** una cuenta de correo está activa cuando puede enviar y recibir mensajes con normalidad
- **bloqueada:** una cuenta de correo está bloqueada cuando no puede enviar o recibir mensajes. Las causas que motivan el bloqueo de una cuenta de correo puede ser alguna de las siguientes:
 - por decisión de las autoridades de la UMU (por comisión de infracciones graves o muy graves) o por requerimiento legal
 - por haberse llenado su buzón. En este caso la cuenta permanece bloqueada hasta que el usuario de la misma no borra mensajes del buzón
 - por detectarse un flujo anormal de mensajes, con esa dirección de correo como destino o como origen, que repercuta en el normal funcionamiento del servicio
 - por cualquier otra causa que lo aconseje
 - El bloqueo de una cuenta de correo puede producirse sólo en la recepción de mensajes, sólo en la emisión o en ambos sentidos.
- **abandonada:** se considera que una cuenta de correo está abandonada cuando no tiene redirigido su correo y se ha excedido el "tiempo máximo de inactividad de una cuenta de correo" recogido en el capítulo 10: Límites y parámetros de gestión del servicio de correo electrónico

- **cancelada:** a efectos prácticos para el usuario una cuenta de correo cancelada es una cuenta de correo eliminada. Los mensajes dirigidos a una cuenta de correo cancelada se rechazan con un código de error de "usuario desconocido". El buzón de una cuenta de correo desactivada podrá ser eliminado definitivamente o bien traspasado a un medio de almacenamiento secundario, pero en ningún caso el usuario podrá acceder al mismo

En el capítulo 10: Límites y parámetros de gestión del servicio de correo electrónico, se indican los valores que inciden en el estado de una cuenta.

En cualquier caso, ATICA se compromete a avisar con antelación al usuario de una cuenta de correo cuando se prevea un cambio de estado en su cuenta de forma que el usuario pueda adoptar las medidas oportunas que eviten su bloqueo o cancelación.

6.3 Cancelación de cuentas de correo

Se procederá a cancelar una cuenta de correo cuando:

1. La cuenta permanezca abandonada durante un tiempo que exceda el marcado en el anexo I "Límites y parámetros de gestión del servicio de correo electrónico"
2. Por decisión de la autoridad competente de la UMU por comisión de infracciones que lleven pareja la eliminación de la cuenta de correo
3. El responsable de la cuenta solicita la eliminación de la misma, siempre que esto no repercuta negativamente en el normal funcionamiento de la UMU
4. En el caso de cuentas de correo personales no pertenecientes al colectivo PDI, PAS o alumnos, o en el caso de cuentas de correo no personales, desaparece el motivo por el que la cuenta fue creada

En cualquier otro caso será la autoridad competente de la UMU la que decida, cuándo y cómo se cancela una cuenta de correo, así como la de arbitrar excepciones a las normas de carácter general arriba expuestas.

Salvo indicación expresa de la autoridad competente de la UMU, o causas de fuerza mayor, la cancelación de una cuenta de correo será avisada con tiempo suficiente para que el responsable de la misma efectúe las acciones oportunas sobre los mensajes almacenados en su buzón antes de que éstos sean definitivamente eliminados o movidos. El aviso se efectuará mediante mensaje de correo electrónico o por cualquier otro medio que se estime oportuno.

ATICA no se responsabiliza de los perjuicios ocasionados por la eliminación de una cuenta de correo y de los mensajes de su buzón en las condiciones arriba expuestas.

La eliminación de una cuenta de correo supone la baja en todos o parte de los servicios citados más arriba.

6.4 Gestión del buzón de correo electrónico

ATICA efectuará un control de los siguientes parámetros relacionados con el uso del correo electrónico:

- estado de los mensajes: nuevo, ya leído, marcado para borrar, respondido, fecha de recepción, etc.
- tamaño del buzón (espacio total ocupado por los mensajes)
- fecha del último acceso al buzón del usuario

En el capítulo 10 de este documento (Límites y parámetros de gestión del servicio de correo electrónico) se cuantifican los límites y parámetros que afectan a la gestión de buzón del usuario y que aparecen en negrita en el presente capítulo. Estos límites y parámetros podrán ser modificados en función de las necesidades y evolución del servicio de correo electrónico. ATICA avisará a sus usuarios de cualquier modificación que pudiese efectuarse en este sentido.

A fin de garantizar un correcto funcionamiento del servicio de correo electrónico, evitando el derroche de recursos y optimizando el rendimiento del sistema, ATICA procederá del siguiente modo a la hora de gestionar el espacio dedicado a almacenar los mensajes de correo de cada usuario:

1. Una vez alcanzado el **tamaño máximo del buzón** no se podrán recibir más mensajes en el buzón hasta que el usuario no borre mensajes del mismo. En estos casos también se podrá restringir el envío de mensajes
2. Si se alcanza el **tiempo máximo de inactividad de una cuenta de correo** (cuenta de correo abandonada) se procederá a cancelar la cuenta de correo desuscribiendo la dirección de correo de las listas de correo de la UMU a las que pudiera estar suscrita

En cualquier caso ATICA se compromete a avisar con la antelación suficiente y por los medios oportunos al usuario afectado antes que se dé alguna de las situaciones contempladas arriba.

6.5 Mantenimiento del servicio

ATICA se reserva el derecho a cambiar cualquier parámetro de configuración del servicio de correo con el fin de incorporar mejoras, monitorizar el servicio, restringir accesos, etc. ATICA se reserva el derecho de parar el servicio cuando las circunstancias lo requieran; si se prevee una parada larga ATICA avisará con antelación enviando un mensaje a todos los usuarios de correo.

Cuando las circunstancias impidan avisar a los usuarios con antelación suficiente y la parada se prolongue durante más tiempo del deseado, ATICA informará a posteriori de los motivos de la parada.

6.6 Gestión de incidencias

Cualquier incidencia que afecte a un usuario de la UMU debe gestionarse a través del sistema DUMBO.

Las incidencias que supongan quejas o consultas de personas o entidades ajenas a la UMU se encauzarán a través de alguna de las siguientes direcciones de correo:

- postmaster@um.es: administrador del servicio de correo de la UMU (ATICA)
- abuse@um.es: para dirigir consultas y quejas sobre incidentes ACE originados en la UMU
- antivirus@um.es: para dirigir consultas y quejas sobre virus propagados por correo electrónico

6.7 Copias de seguridad

ATICA se compromete a realizar copia de seguridad de los siguientes aspectos del servicio de correo electrónico:

- programas y archivos de configuración del propio servicio
- archivos de registro de eventos o "logs"
- buzones de los usuarios de correo
- archivos de configuración personales de los usuarios depositados en el servidor

La frecuencia y número de copias de seguridad efectuadas podrán variar en función de la disponibilidad y características de los datos a almacenar. En cualquier caso, ATICA no asegura la recuperación de mensajes eliminados a partir de las copias de seguridad de los buzones. Es responsabilidad del usuario del buzón el efectuar copia de los mensajes que considere importantes en un medio local y personal: disco duro, disquete, cdrom, etc.

6.8 Supervisión y monitorización

ATICA, podrá monitorizar, intervenir y examinar el contenido de los mensajes y buzones de los usuarios en alguna de las siguientes circunstancias:

- cuando el responsable de la cuenta de correo lo pida, para detectar y corregir posibles problemas que afecten al normal funcionamiento de la cuenta
- cuando sucedan eventos que afecten al funcionamiento general del servicio, para detectar el origen y las causas del problema
- cuando la autoridad competente de la UMU así lo solicite
- por requerimiento legal

6.9 Registro de eventos

ATICA registra en archivos específicos el funcionamiento y uso del correo electrónico. En concreto se generan trazas de los siguientes eventos:

- envío y recepción de mensajes
- acceso a los buzones de los usuarios
- alta, baja, modificación y consulta de cuentas de correo
- cambios de claves de acceso al buzón
- cambios en archivos de configuración personales de los usuarios

Para cada uno de estos eventos se registra de manera detallada todos los datos concernientes al mismo: direcciones IP de los ordenadores, direcciones de correo del remitente y del destinatario, etc.

En el futuro podrán registrarse nuevos eventos relativos al servicio de correo electrónico.

6.10 Estadísticas del servicio

ATICA generará estadísticas del servicio de correo con el fin de medir su rendimiento, el uso que se hace del mismo y detectar o prevenir posibles comportamientos anómalos que pudieran producirse. Parte de las estadísticas podrán hacerse públicas para información de la comunidad universitaria.

En la medida de lo posible se generarán estadísticas de uso personal del correo para cada cuenta, las cuales sólo serán accesibles por el responsable de la cuenta.

6.11 Encaminamiento del correo

El encaminamiento de mensajes hacia y desde la UMU se efectuará a través de un sistema central (la estafeta de salida) gestionado directamente por ATICA. El resto de estafetas de la UMU no podrán recibir o enviar correo directamente desde o hacia Internet; sólo podrán hacerlo a través de la estafeta central. El objetivo de este esquema de encaminamiento institucional pretende:

- centralizar en un sólo punto el flujo de mensajes hacia y desde la Universidad, optimizando recursos y facilitando las tareas administrativas de detección y eliminación de virus, gusanos y spam
- generar estadísticas globales de tráfico hacia y desde la Universidad
- impedir el uso de estafetas de la UMU mal configuradas para generar spam

6.12 Detección y eliminación de virus

El correo electrónico es uno de los medios de difusión de virus más importantes. Para prevenir la propagación masiva de virus y gusanos informáticos, se aplican las siguientes medidas sobre todos los mensajes que entran o salen de la UMU, así como sobre el correo intrauniversitario

que tenga como origen o destino alguna de las direcciones de correo gestionadas por ATICA:

- no se permiten mensajes de correo con anexos ejecutables o susceptibles de contener código malicioso
- si se desea enviar un mensaje con un anexo ejecutable, sólo podrá hacerse si previamente se comprime en algún formato conocido (.zip, .gzip, etc.)
- los mensajes serán examinados por un programa antivirus, de forma que se garantice, en la medida de lo posible, que los mensajes que entran y salen de la UMU están limpios

El procedimiento utilizado a la hora de detectar un mensaje con código malicioso en un anexo es el siguiente:

- nunca se envía un mensaje de aviso al remitente del mensaje, pues la mayoría de mensajes infectados son generados por gusanos que falsifican la dirección de correo del remitente
- en el caso de que el mensaje haya sido generado por un gusano, el mensaje se descarta y no se entrega a los destinatarios
- si se puede eliminar el virus del anexo se elimina y se entrega el mensaje a los destinatarios con el anexo libre de virus. En el mensaje se incluye un literal avisando del evento e indicando el tipo de virus eliminado
- si no se puede eliminar el virus del anexo se entrega el mensaje a los destinatarios sin el anexo. En el mensaje se incluye un literal avisando del evento e indicando el tipo de virus eliminado

Detección y control de PCs infectados y mensajes generados por los mismos

La detección de PCs infectados se realiza inspeccionando las cabeceras de los mensajes infectados, a partir de la dirección IP de origen del mensaje. A fin de minimizar la propagación de gusanos y virus (sobre todo cuando son de reciente aparición y los programas antivirus no logran detectarlos), ATICA podrá ejecutar todas o algunas de las siguientes acciones sobre los equipos infectados o mensajes generados desde los mismos:

- desactivar el punto de red al que está conectado el equipo
- no permitir el tráfico SMTP con origen en el equipo
- rechazar en la estafeta de salida de la UMU los mensajes generados desde ese equipo
- rechazar los mensajes que se ajusten a un determinado patrón en la cabecera o en el cuerpo

El usuario responsable del equipo afectado será informado del hecho tan pronto como sea posible para que proceda a la desinfección del equipo, al tiempo que personal de ATICA se pondrá a su disposición para dicha tarea. Una vez limpio el equipo, se procederá a restituir los servicios que pudieran haber sido desactivados.

Responsabilidades asociadas a la propagación de virus

La UMU declina cualquier responsabilidad derivada de la propagación de virus y gusanos a través del correo electrónico, siendo responsabilidad del usuario el tomar las medidas necesarias para evitar la infección y sus consecuencias; entre las medidas se incluyen:

- no abrir ficheros adjuntos en mensajes de correo no solicitados aunque procedan de remitentes conocidos
- usar un antivirus en el ordenador personal y mantenerlo actualizado
- efectuar copias de seguridad periódicas de los programas, datos y configuraciones de su equipo

6.13 Detección y eliminación de correo basura (spam)

En el capítulo 11 "Abuso en el Correo Electrónico (ACE)" se fija la política de la UMU con respecto al correo basura en particular y contra otros tipos de abusos en general.

Para minimizar la llegada de correo basura a los buzones de los usuarios se aplicarán todas o parte de las siguientes medidas sobre todos los mensajes que entran o salen de la UMU, así como sobre el correo intrauniversitario que tenga como origen o destino alguna de las direcciones de correo gestionadas por ATICA. Las medidas se categorizan según distintos criterios:

Control de la procedencia y destino de los mensajes

- uso de listas negras para el rechazo sistemático de mensajes provenientes de estafetas mal configuradas o "abiertas"
- uso de listas blancas para posibilitar la inclusión de excepciones a las listas negras
- uso de listas grises para evitar el spam generado desde programas especializados
- impedir el envío de mensajes con direcciones de correo falsificadas
- uso de filtros en la estafeta: rechazar estafetas no registradas en el DNS, sin resolución inversa o sin registros MX, etc.
- autenticación de los remitentes de mensajes
- autenticación de las estafetas intermedias
- uso de cualquier otro mecanismo de nueva aparición y que sea útil al propósito que nos ocupa

Control del flujo de mensajes

Tienen como objetivo detectar patrones de tráfico de correo desde y hacia la UMU anómalos, sospechosos de constituir ataques de spam. Cuando se detecta un flujo de mensajes de este tipo los mensajes no se entregan inmediatamente, sino que se almacenan para su posterior inspección. Si se comprueba que los mensajes son correo basura se eliminan, si no lo son se entregan normalmente.

Análisis del contenido de los mensajes

Se inspeccionan las cabeceras y los contenidos de los mensajes y se calcula la probabilidad de que se trate de un mensaje de spam o no. Si el mensaje se considera spam, se marca para que el receptor del mismo pueda

distinguirlo del resto de mensajes. Si no se considera spam el mensaje se entrega normalmente.

Responsabilidades asociadas a la detección y eliminación de spam

La UMU declina cualquier responsabilidad derivada de la aplicación de las medidas arriba expuestas. El usuario de correo de la UMU acepta las medidas arriba expuestas y cualquier otra que pueda ser adoptada en el futuro tendentes a reducir el tráfico de correo basura desde y hacia la UMU.

El usuario de correo debe ser consciente de que la aplicación de las medidas arriba expuestas puede dar lugar a las siguientes situaciones:

- rechazo sistemático de mensajes provenientes de estafetas mal configuradas
- rechazo sistemático de mensajes dirigidos a estafetas mal configuradas
- generación de falsos positivos: mensajes marcados como spam que no los son
- generación de falsos negativos: mensajes no marcados como spam que sí lo son
- retardos en la entrega o recepción de mensajes de correo

En cualquier caso ATICA se compromete a tomar las medidas necesarias para minimizar estos casos. Por su parte, el usuario de correo se compromete a avisar al personal informático de cualquier indicio o problema que pudiera acontecer relativo a la detección y eliminación de spam.

7 Identidad del usuario de correo electrónico

El usuario debe identificarse mediante su clave de acceso al correo siempre que se le solicite, en particular para acceder a su buzón. La solicitud de clave podrá ampliarse en cualquier otra circunstancia que en el futuro se considere necesaria.

Es obligación del usuario configurar adecuadamente su programa de correo para:

- identificarse correctamente ante el servicio cuando éste lo requiera
- que su nombre y apellidos (en el caso de cuentas de correo personales) o la descripción de la cuenta (en el caso de cuentas de correo no personales) aparezca en las cabeceras de los mensajes que envíe

En cualquier caso, ATICA no garantiza que la identidad aparecida en las cabeceras de un mensaje de correo se corresponda con la identidad real del usuario que envió el mensaje (limitación del protocolo SMTP de transferencia de mensajes de correo electrónico). Para salvar esta situación ATICA permitirá que los mensajes enviados desde cuentas personales sean firmados mediante un certificado digital personal del usuario, de manera que el destinatario del mensaje pueda comprobar la identidad del remitente. Es responsabilidad del usuario configurar adecuadamente su programa de correo para comprobar este hecho.

8 Confidencialidad del servicio de correo electrónico

El responsable de una cuenta de correo electrónico se compromete a no desvelar su clave de acceso (salvo en los casos en que delegue su uso), así como a elegir una clave suficientemente segura que impida que terceros puedan adivinarla mediante técnicas de "fuerza bruta" o similares.

En este sentido ATICA pondrá los medios necesarios para que los usuarios de correo usen claves seguras, en particular:

- forzará la elección de claves seguras durante los procesos de solicitud y creación de cuentas y durante el proceso de cambio de clave
- efectuará controles periódicos de las claves de sus usuarios, pudiendo obligar a cambiar claves de correo "débiles" a los usuarios que las tuviesen

Por su parte, ATICA se compromete a poner los recursos necesarios para permitir encriptar las claves de sus usuarios cuando circulen por la red; la encriptación se hará extensible al contenido de los mensajes cuando el usuario así lo solicite.

Es responsabilidad del usuario el configurar adecuadamente su programa de correo para solicitar los servicios de encriptación del correo. ATICA se compromete a ofrecer los mecanismos y la documentación necesaria para facilitar esta tarea.

9 Integridad de los mensajes de correo

Con objeto de garantizar la integridad de los mensajes de correo, ATICA pondrá a disposición de sus usuarios una infraestructura de clave pública y privada que permita efectuar un "hash" de los mensajes enviados y un posterior chequeo de la integridad por parte del destinatario de los mensajes

10 Límites y parámetros de gestión del servicio de correo electrónico

Los límites y parámetros que regulan aspectos concretos del funcionamiento del servicio de correo se describen en el documento: "[Parámetros de uso de los Servicios de ATICA](#)", apartado "Parámetros de uso del servicio de correo electrónico".

Los límites y parámetros pueden ser modificados en cualquier momento, así como ser definidos nuevos límites y parámetros.

Siempre que sea posible, ATICA informará con antelación suficiente de cualquier cambio efectuado en este sentido.

11 Política Institucional de la UMU frente al ACE

Introducción

La Universidad de Murcia reconoce los principios de libertad de expresión y privacidad de información como partes implicadas en el servicio de correo electrónico.

La UMU anima al uso del correo electrónico y respeta la privacidad de los usuarios. Nunca de forma rutinaria se realizarán monitorizaciones o inspecciones de los buzones sin el consentimiento del propietario del buzón. Sin embargo podrá denegarse el acceso a los servicios de correo electrónico locales e inspeccionar, monitorizar y cancelar una cuenta de correo:

- Cuando haya requerimientos legales
- Cuando haya sospechas fundadas de violación de la política interna de la institución, como comercio electrónico, falsificación de direcciones etc. Evitando caer en rumores, chismorreos u otras evidencias no fundadas y previo consentimiento del máximo responsable del servicio
- Cuando por circunstancias de emergencia, donde no actuar pudiera repercutir gravemente en el servicio general a la comunidad

Disposiciones generales

1. Nuestra institución es responsable de cualquier nombre de dominio DNS de tercer nivel bajo el dominio "um.es".
2. Dentro de los servicios de comunicaciones que nuestra institución provee, se ofrecen cuentas de correo electrónico y una o varias máquinas para el encaminamiento y recogida de correo a/desde Internet a los buzones de las cuentas. Teniendo registro de las personas que los están utilizando bajo las direcciones electrónicas de las que somos responsables.
3. Como gestores del servicio de correo electrónico dentro de nuestra institución, nos reservamos el derecho de tomar las medidas sancionadoras oportunas contra los usuarios internos y externos que realicen cualquiera de los abusos incluidos en el [Anexo III](#).
4. Disponemos de suficiente información acerca de:
 - Las diversas actividades que trascienden los objetivos habituales del uso del servicio de correo electrónico que presta nuestra Institución
 - Los perjuicios directos o indirectos que este problema ocasiona a nuestros propios usuarios, rendimientos de máquinas, líneas de comunicaciones etc reflejados en el [Anexo III](#)

Objetivos

Este documento ha sido escrito con los siguientes objetivos en mente:

1. Proteger la reputación y buen nombre de nuestra institución en la Red (Internet)
2. Garantizar la seguridad, rendimientos y privacidad de los sistemas de nuestra organización y de los demas

3. Evitar situaciones que puedan causar a nuestra organización algún tipo de responsabilidad civil o penal
4. Preservar la privacidad y seguridad de nuestros usuarios
5. Proteger la labor realizada por las personas que trabajan en nuestros servicios de comunicaciones frente a ciertos actos indeseables

Ámbito de aplicación

1. Todas las máquinas de nuestra institución capaces de encaminar correo electrónico (estafetas)
2. Todas las piezas de mensajes (texto, cabeceras y trazas) residentes en ordenadores propiedad de nuestra institución
3. Todos los usuarios responsables de cuentas de correo en o bajo el dominio um.es
4. Todos los servicios internos que utilizan el correo electrónico, como por ejemplo los servidores de listas de distribución y respondedores automáticos

Esta política sólo se aplica al correo electrónico en formato electrónico y no es aplicable a correo electrónico en formato papel.

Compromisos

1. Emplear los recursos técnicos y humanos a nuestro alcance para intentar evitar cualquiera de los tipos de abusos reflejados en el [Anexo III](#)
2. Proporcionar a los usuarios del servicio de correo electrónico de la UMU los mecanismos necesarios para denunciar cualquier abuso que pudieran sufrir
3. Intentar mantener nuestros servidores de correo institucionales con las últimas mejoras técnicas (actualizaciones, parches, filtros etc) para defenderlos de los ataques definidos en el [Anexo III](#) .
4. Proteger los datos personales de nuestros usuarios: **Nombre Apellidos** y **dirección de correo electrónico** de acuerdo con la legislación española reflejada en la LORTAD (Ley Orgánica de Tratamiento de Datos - Ley Orgánica 5/1992 del 29 Octubre) .
5. Intentar impedir y perseguir a usuarios internos que realicen cualquiera de las actividades definidas en el [Anexo III](#)
6. Coordinarnos con el equipo gestor del Programa RedIRIS para colaborar en la creación de un frente común frente a este tipo de actividades definidas en el [Anexo III](#). Esto incluye la colaboración al nivel necesario para la persecución de estas actividades
7. Dedicar un buzón (**abuse@um.es**) donde puedan ser enviados y atendidos los incidentes originados desde nuestra organización, así como las consultas y quejas de nuestros usuarios

12 Abuso en el Correo Electrónico (ACE)

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 en inglés habitualmente asociados en Internet a estos tipos de abuso son *spamming*, *mail bombing* (bombardeo de correo), *unsolicited bulk email* (UBE), *unsolicited commercial email* (UCE), *junk mail*, etc., abarcando un amplio abanico de formas de difusión. Los correspondientes términos en castellano son: correo basura, correo no solicitado, etc.

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.

Definición de términos

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

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
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 una estafeta ajena](#) 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 estafeta de uso público, declarada como tal)
- **Difusión masiva no autorizada**
El uso de estafetas propias o ajenas 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 acarrear 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