RESOLUCIÓN DE LA SECRETARÍA GENERAL POR LA QUE SE APRUEBA LA NORMATIVA DE USO DEL CORREO ELECTRÓNICO CORPORATIVO EN EL CSIC

ÍNDICE

1 OBJETO DEL DOCUMENTO

Es objeto de esta Resolución establecer la normativa de uso del servicio de correo electrónico corporativo en el Consejo Superior de Investigaciones Científicas.

2 ALCANCE

La normativa se aplicará al servicio de correo electrónico corporativo del CSIC que se ofrece desde la plataforma DEUCALION de la SGAI (Secretaría General Adjunta de Informática).

Esta normativa es de obligado cumplimiento para los servicios de correo de centros, institutos o departamentos que no se encuentren en la plataforma mencionada, a excepción de aquellos apartados en los que expresamente se indique que tiene carácter de recomendación.

Afecta, por tanto, a todas las direcciones de correo electrónico del dominio *@csic.es*, de todos los subdominios *@xxx.csic.es* y de todos los dominios singulares registrados por el CSIC o por cualquiera de sus centros.

3 VIGENCIA

Esta normativa entrará en vigor en la fecha de su publicación en BO.CSIC (Boletín de Normas Internas del CSIC).

4 USUARIOS DEL SERVICIO DE CORREO DEL CSIC

Podrá solicitar y utilizar una cuenta de correo electrónico del CSIC su personal funcionario, contratado, laboral o becario en activo, así como el resto de colectivos que figura en el cuadro “Usuarios del Servicio de Correo del CSIC”, en cualquier caso con las limitaciones que marca este documento.

Los usuarios que deseen obtener una cuenta de correo deberán aceptar los "Términos y Condiciones de Uso del Correo Electrónico" del CSIC (Ver ANEXO1).

La siguiente tabla muestra la relación de los colectivos que pueden disponer de una cuenta de correo electrónico de subdominios del CSIC, identificando, en cada caso, el tipo de cuenta.

Colectivo			Grupo	Cuenta	Tipo Cuenta	Observaciones
CSIC	Funcionario (de carrera, interino, en prácticas)		1	SI	Personal	-
			2		Institucional	Sólo cargos institucionales
	Laboral / Contratados		3	SI	Personal	-
	Funcionario Ad-Honorem		4	SI	Personal	-
NO CSIC	Personal Emérito		5	SI	Personal	-
	Personal Centro Mixto (NO CSIC)		6	SI	Personal	-
			7		Institucional	Sólo cargos institucionales
	Becario (investigación, predoctoral, posdoctoral)		8	SI	Personal	-
	Becario Introducción		9	NO		(1)
	Estancias Breves		10	NO		(1)
	Alumno Master		11	NO		(1)
	Otros Colectivos	Empresas de Servicio contratadas	12	NO		(2)
		Personal en prácticas (formación o investigación)	13	NO		(1)
		Doctor Vinculado	14	SI	Personal	-
		Sabático	15	SI	Personal	-
		Doctor ICREA, Doctor ARAID	16	SI	Personal	-
		Otros	17	NO		(3)

(1) Si fuese necesario dotar de una cuenta de correo a una persona de este colectivo, le podrá ser asignada siempre que su estancia en las dependencias del CSIC fuese superior a 6 meses y su actividad así lo requiriese. Cualquier excepción a esta norma deberá ser propuesta y autorizada por el Departamento de Postgrado del CSIC

(2) 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 Secretario General del CSIC

(3) La relación anterior es extensiva, por lo que sólo los colectivos que figuran de manera expresa en esta relación están autorizados a disponer de cuentas de correo electrónico de subdominios del CSIC. Se requiere, por tanto, la previa autorización y modificación de esta relación para autorizar el uso de cuentas de correo CSIC a otros colectivos; siendo necesario para ello la previa autorización del Secretario General del CSIC.

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

5 CUENTAS Y BUZONES DE CORREO

5.1 TIPOLOGÍA

Bajo el dominio o subdominios “csic.es”, se pueden distinguir tres tipos de cuentas: Personales, Institucionales y Organizativas.

5.1.1 Cuentas Personales

Identifican las direcciones de correo electrónico de una persona.

5.1.2 Cuentas Institucionales

Están asociadas a cargos.

Las cuentas institucionales predefinidas en el CSIC son:

- dirección
- gerencia
- coordinador institucional
- coordinador área
- Administración de las delegaciones

Una persona tendrá acceso a una cuenta institucional en función de su cargo o de su actividad.

5.1.3 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.

5.2 SOLICITUD Y CREACIÓN

Para disponer de una cuenta personal en un dominio alojado en la plataforma Deucalion, el usuario deberá estar dado de alta en el directorio corporativo del CSIC (esto es, alta en la aplicación GEP) y haber realizado “su primer acceso” desde la Intranet corporativa del CSIC.

Las cuentas institucionales se crean a petición de la Unidad de Coordinación Técnica (UCAT) o del Área de Organización Institucional de la Vicepresidencia Adjunta de Relaciones Institucionales (VORI).

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.

5.3 VIGENCIA, DESACTIVACIÓN Y ELIMINACIÓN DE CUENTAS DE CORREO

5.3.1 Vigencia

5.3.1.1 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 el CSIC. Excepcionalmente, este periodo podrá variar por necesidades del servicio debidamente motivadas. Esta excepcionalidad no podrá en ningún caso exceder 2 años.

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 al CSIC, el responsable de la persona ante el CSIC 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.

5.3.1.2 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 del CSIC.

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

5.3.1.3 Cuentas organizativas.

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

5.3.2 Procedimientos de desactivación y eliminación

5.3.2.1 Borrado automático de cuentas.

Se eliminarán aquellas cuentas de correo que no han sido consultadas durante un periodo continuado de seis meses. Esto conlleva el borrado de los correos almacenados en dicha cuenta.

5.3.2.2 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.

5.3.2.3 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. Esto podría impedir al usuario el acceso al resto de los servicios basados en las credenciales de la Intranet.

5.4 FORMATO DE LAS DIRECCIONES DE CORREO

Las cuentas personales correspondientes al dominio institucional "csic.es" se ajustan a lo expuesto en el Anexo 3 *Criterios nominales de creación de cuentas personales en dominio institucional "csic.es"*.

5.5 TAMAÑO DE LOS BUZONES DE CORREO

La capacidad máxima para los buzones puede variar a lo largo del tiempo. Para el correo corporativo, podrá consultarse en el Documento de Especificaciones Técnicas de la Plataforma de Correo Corporativo Deucalion disponible en la Intranet.

En dicha Plataforma de Correo Deucalion, cuando el sistema detecta que la ocupación del buzón de correo es superior al 90% automáticamente envía una notificación al usuario, con el fin de que pueda tomar las medidas pertinentes. Una vez alcanzado el 100% de la cuota asignada, todos los mensajes son rechazados por el sistema, siendo necesario que el usuario vacíe el buzón para restablecer la recepción normal de mensajes.

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 de Envío de Grandes Archivos (SEGA) que permite el envío de ficheros de muy grandes.

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.

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 (del tipo @gmail.com, @hotmail.com, etc.) para enviar correo mediante las estafetas de correo del CSIC.

Los parámetros técnicos anteriores podrán consultarse en el Documento de Especificaciones Técnicas de la Plataforma de Correo Corporativo Deucalion disponible en la Intranet.

7 DOMINIOS DE CORREO

En el CSIC conviven los siguientes tipos de dominio de correo:

- Tipo I: Dominio institucional “csic.es”
- Tipo R: Dominios de centros, institutos y Organización Central “xxx.csic.es” u otros (“xxx.es”, “xxx.org”, etc. de acuerdo con la Política de Dominios del CSIC), (donde xxx corresponde al dominio del centro, instituto u Organización Central)

Los usuarios de los grupos 1, 3, 4, 5, 6 y 8 pueden disponer de una cuenta institucional de Tipo I (véase la columna “Clase” de la Tabla “Usuarios del Servicio de Correo CSIC”).

Asimismo, toda persona, excepto las salvedades indicadas en el apartado “Usuarios”, podrá disponer de una cuenta de tipo R, es decir, asociada a su destino o ubicación (centro, instituto u ORGC).

Existe compatibilidad entre las cuentas de tipo I y tipo R, por lo que un usuario podrá disponer de ambos tipos de cuentas de correo.

Se recomienda la utilización de cuentas de tipo I, ya que fomentan la movilidad independizando la cuenta de la localización o adscripción a una unidad concreta –centro, instituto, ORGC-.

Los dominios de correo de los centros e institutos pueden estar alojados en la plataforma Deucalion o en los servidores ubicados en los centros

En cualquier caso, es necesario el cumplimiento de la política de uso del servicio de correo definidos por RedIRIS y que se recoge, adaptándola a la especificad del CSIC, en el Anexo 1.

8 RESTRICCIONES EN LOS SERVICIOS RELACIONADOS CON EL CORREO ELECTRÓNICO

No se ofrece la posibilidad de redirecciones externas desde la plataforma DEUCALION y se desaconseja este mecanismo en las demás estafetas del CSIC por los problemas de seguridad que ello puede provocar.

9 SEGURIDAD

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

- Robo de identidad. Phishing y scams
- 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:

Contraseña

La contraseña de acceso al correo no debe ser cedida o facilitada a otros usuarios, siendo responsabilidad del propio usuario su custodia.

Ver política de contraseñas

Encriptación.

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 Secretaria General Adjunta de Informática (SGAI) y unidades informáticas del CSIC 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 Centro de Atención a Usuarios del CSIC o con el personal TIC del centro.

10 GARANTÍA DE ENTREGA 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 las estafetas de correo del CSIC envían un correo al emisor informando de los problemas surgidos en casos de que no se pueda entregar un correo a un destinatario 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.

11 VIRUS DE CORREO ELECTRÓNICO Y ANTISPAM

11.1 SPAM

El CSIC 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 SPAM con un 99,99% de certeza.

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

11.2 VIRUS

Las estafetas del CSIC 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, salvo en el caso de virus que falsifiquen la cabecera de origen.

12 POLÍTICA DE LOGS

Por imperativos legales, las trazas del tránsito SMTP de las estafetas principales de los correos que gestiona la plataforma de correo del CSIC 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 estafeta.
- Localizar trazas concretas de mensajes en caso de algún tipo de incidente.
- Por motivos estadísticos.

Aquellos centros e institutos que tengan sus cuentas de correo en la plataforma corporativa Deucalion, deberán solicitar la obtención de logs a la Secretaría General de Informática del CSIC. En función del tipo de solicitud se podrá proceder previa autorización de la Secretaria General.

13 ATENCIÓN A USUARIO. CONTACTOS E INFORMACIÓN

Si tiene cualquier duda o cuestión sobre el servicio de correo electrónico, diríjase a los Servicios Informáticos o al CAU.

Centro de Atención al Usuario, 91 568 0200, cau-csic@csic.es

Responsable de correo de la plataforma corporativa Deucalion: postmaster@csic.es

Información

Puede notificar las incidencias en el uso del correo electrónico a: abuse@csic.es y postmaster@csic.es.

abuse@csic.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.

postmaster@csic.es: En esta dirección se notifican todos los problemas con procesamiento de mensajes de correo, además de permitir ponerse en contacto con los responsables del servicio.

14 ESTAFETAS DE CORREO EN EL CSIC

Los únicos servidores autorizados a enviar correos al exterior de la red del CSIC son las denominadas estafetas de correo gestionadas por administradores TICs. En ningún caso un ordenador personal podrá realizar esta tarea y para enviar correo deberá entregárse a una estafeta para su posterior procesamiento.

Todas las estafetas deberán estar dadas de alta en un registro específico de la SGAI.

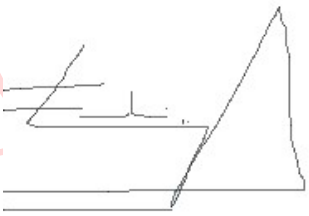
En los cortafuegos corporativos y de los centros, el puerto 25 permitirá únicamente el tráfico desde las estafetas de correo registradas y bloqueará el tráfico proveniente de los ordenadores personales.

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 las estafetas receptoras.

Madrid, 15 de julio de 2011

EL SECRETARIO GENERAL

Firmado digitalmente por NOMBRE JIMENEZ ARROYO EUSEBIO CARLOS - NIF 00694544J
Fecha: 2011.07.15 '14:16:11 +02'00



ANEXO 1. TÉRMINOS Y CONDICIONES DE USO DEL CORREO ELECTRÓNICO

El CSIC, como institución afiliada a RedIRIS hace suyos los términos y condiciones de uso del Correo Electrónico de dicha entidad.

En apoyo del objetivo fundamental de nuestra institución, la investigación, y respetando los principios de libertad de expresión y privacidad de información, se ofrece un serie de recursos de red, comunicaciones y de información a nuestra comunidad. 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.

En caso de no entender completamente alguno de estos apartados póngase en contacto con el responsable del Servicio de correo de su centro o con el CAU o el buzón postmaster@csic.es

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

1. 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 Normas de Uso Aceptable y Seguridad de la Red de datos del CSIC y las Leyes Vigentes en España.

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.

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

3. Los usuarios deben ser conscientes de la diferencia de utilizar direcciones de correo electrónico suministradas por la institución 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.

4. 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.

5. El usuario debe de ser consciente de los términos, prohibiciones y perjuicios englobados en Abuso en el Correo Electrónico.

6 Es incorrecto enviar mensajes con direcciones (remitente) no asignadas por los responsables de nuestra institución y, en general, es ilegal manipular las cabeceras de correo electrónico saliente.

7. 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.

8. La violación de la seguridad de los sistemas y/o red puede incurrir en responsabilidades penales.

9. 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.

10. Está completamente prohibido realizar cualquier de los tipos definidos en el Abuso de Correo Electrónico (ver Anexo 2). 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.

11. 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.

ANEXO 2. SEGURIDAD. ABUSO EN EL CORREO ELECTRÓNICO

Documento de RedIRIS asumido por el CSIC.

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 estos temas 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 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 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.

ANEXO 3. CRITERIOS NOMINALES DE CREACIÓN DE CUENTAS PERSONALES EN EL DOMINIO INSTITUCIONAL "CSIC.ES"

La forma común de una cuenta de correo electrónico para los alias del dominio "csic.es" es:

<alias_del_usuario>@csic.es

En el formulario de solicitud el generador de alias utiliza los siguientes criterios:

1. Las direcciones estarán formadas por combinaciones del nombre y apellidos o iniciales de una persona -pudiendo no seleccionar alguno de ellos:

- es obligatorio seleccionar un elemento de la columna "Nombre"
- tiene que seleccionar al menos un elemento de las columnas "Apellidos1" o "Apellidos2". Se recomienda seleccionar ambos si sus apellidos son frecuentes.
- si el alias elegido ya está en uso podrá utilizar la secuencia numérica para crear uno nuevo
- Los caracteres con tilde son sustituidos por el mismo carácter sin tilde. El carácter ñ es sustituido por la letra n.

2. El carácter "." es un separador obligatorio entre nombre y apellidos o iniciales

3. Cada persona podrá seleccionar hasta un máximo de dos alias para su cuenta "@csic.es" entre las posibles combinaciones que ofrezca el generador.

ANEXO 4. 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-.

Deucalion. Plataforma corporativa de correo electrónico del CSIC. 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.