Normativa del servicio de correo electrónico de la Universidad de Cantabria

Versión 3.1 Agosto 2014

1. Introducción.

El presente documento describe el servicio de correo electrónico que la Universidad de Cantabria presta a su personal a través del Servicio de Informática.

Con este documento se pretende dar una visión general del servicio abarcando tanto los aspectos administrativos como técnicos, actuando como guía para los usuarios en la utilización de este servicio.

Este documento se refiere, salvo que se especifique lo contrario, al servicio central de correo proporcionado por el Servicio de Informática de la UC para el PAS y PDI. El Servicio de Correo para alumnos dispone de su propia normativa.

El servicio central de correo es el único que tiene carácter oficial.

La Universidad de Cantabria es responsable de cualquier nombre de dominio DNS de tercer nivel bajo el dominio “unican.es”.

1.1. Acceso

El acceso a este servicio se realiza mediante cuentas de intranet o cuentas personales. La creación y cancelación de estas cuentas, así como otros aspectos específicos, se establecen en la “Normativa sobre cuentas personales” del Servicio de Informática (SdeI) de la Universidad de Cantabria.
Los buzones de correo electrónico personales, como el resto de servicios asociados, se cancelan con la cancelación de la cuenta.

1.2. Condiciones

Como cualquier otro servicio TIC, las condiciones generales de uso de los buzones de correo se establecen en la “Reglamento de uso de recursos TIC de la Universidad de Cantabria” aprobado por Consejo de Gobierno el 14-02-2008.

De manera específica para este servicio, se establece la siguiente normativa,

- Los usuarios son completamente responsables de todas las actividades realizadas con sus buzones.
- Es una falta grave facilitar u ofrecer el buzón personal a personas no autorizadas.
- Los usuarios deben ser conscientes de la diferencia de utilizar direcciones de correo electrónico suministradas por el Servicio de Informática o privadas ofrecidas por un proveedor de Internet. El campo remite de las cabeceras de correo indica el origen al que pertenece el emisor de un mensaje, por que hay que tener en cuenta las posibles repercusiones.
- Debe ser consciente de los términos, prohibiciones y perjuicios englobados en el punto 5.4 de este documento. Esta completamente prohibido realizar cualquiera de las prácticas detalladas en dicho punto.
- No se permiten 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, esta prohibido manipular las cabeceras de correo electrónico saliente
- No se debe 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.
- Estará penalizado con la cancelación del buzón, el envió a foros de discusión (listas de distribución, newsgroups, blogs,....) de mensajes que comprometan la reputación de nuestra organización o violen cualquiera de leyes españolas

2. Definición de los buzones de correo.

2.1. Tipos de buzones de correo.

Existen varios tipos de buzones de correo que vamos a pasar a enumerar.

2.1.1. Buzones personales.

Son los buzones de uso individual proporcionados por la universidad para realización de las tareas académicas y profesionales de su personal, nunca para actividades privadas o ajenas a la institución. Están asociados a las cuentas personales definidas en el documento "Normativa sobre cuentas personales" del Servicio de Informática de la Universidad de Cantabria. Los buzones de correo electrónico personales, como el resto de servicios asociados, se cancelan con la cancelación de la cuenta.
Sus características se indican en el [Cuadro 1].

	Capacidad Buzón	Tamaño máximo correo	Número Máximo de destinatarios
PDI /PAS	2.5 GB	50 MB.	150

Cuadro 1: Características de las cuentas de correo.

Los buzones personales tendrán dos direcciones: una de la forma usuario@dominio y otra de la forma nombre.apellido@dominio. El personal (PAS/PDI) podrá solicitar el cambio de la dirección larga siempre que se ajuste a una serie de condicionantes que permitan la correcta identificación del usuario mediante su nombre y apellidos.

2.1.2. Buzones comunes.

Son buzones a los que se puede acceder con varias cuentas personales. En ningún caso se crean "cuentas genéricas" para prestar este tipo de servicio. El acceso debe ser siempre con identificación personal. Normalmente están asociadas a los miembros de los servicios de atención al público de la universidad. Los buzones de correo electrónico comunes se crean y cancelan a petición de la unidad o servicio titular del mismo.

2.1.3. Buzones institucionales.

Son buzones asociados a órganos de gobierno de la universidad (rector, vicerectores, etc). Estos buzones se pueden considerar buzones comunes ya que permiten acceso a las personas debidamente autorizadas. Los buzones de correo electrónico institucionales se crean y cancelan a petición de los órganos de gobierno de la universidad.

3. Acceso al correo electrónico.

Por motivos de seguridad, los servidores están configurados para canalizar tan solo los mensajes enviados desde lo ordenadores identificables localizados en el campus o, preferentemente, que se autentican para el envío (SMTP SSL-AUTH, HTTPS, MAPI, RPC sobre HTTPS, ActiveSync y Blackberry).

El acceso a las cuentas de correo se puede realizar en las formas indicadas en el [Cuadro 2].

	PDI/PAS
IMAP-SSL	Sí
HTTPS	Sí
RPC-HTTPS	Sí
MAPI	Sí
Active-Sync	Sí
Blackberry(**)	Sí

Cuadro 2: Protocolos de lectura de correo.

(*) Por razones de seguridad y funcionalidad el POP, POP-SSL e IMAP se eliminó en 2009

(**) El sistema Blackberry solo se ofrece desde determinados móviles corporativos.

La configuraciones recomendadas son:

3.1. Desde dentro de la universidad.

Se recomienda a los miembros del personal el acceso al correo electrónico a través del protocolo IMAP-SSL + SMTP SSL-AUTH, MAPI encriptado o RPC-HTTPS mediante un cliente de correo electrónico.

3.2. Desde fuera de la universidad.

Siempre que se acceda a la lectura del correo a través de un ordenador público o de uso esporádico, se recomienda a los miembros de la comunidad universitaria el acceso a través del Correo Web (protocolo HTTPS) utilizando cualquier navegador.

El acceso mediante la red WiFi de la UC se considera a estos efectos como “desde fuera de la universidad”.

Aquellos miembros de este colectivo que deseen acceder al los buzones desde su domicilio o lugar de desplazamiento a través de un cliente de correo, pueden configurar un acceso a través del protocolo RPC-HTTPS, IMAP-SSL + SMTP SSL-AUTH o sistemas para correo en el móvil (ActiveSync y Blackberry)

3.3 Configuración Automática

El personal de la UC dispone de un sistema de configuración automática que permite a los clientes de correo (Outlook, Mac Mail, ..) y los dispositivos móviles (Windows Phone, Iphone, Ipad, Android, ..) más avanzados configurarse automáticamente con los parámetros óptimos con solo conocer su usuario, contraseña y dirección de correo electrónico.

4. Opciones adicionales.

4.1. Desvío de correo a otras cuentas.

Aquellos miembros del Personal Docente e Investigador que deseen redireccionar su cuenta de correo a otra cuenta interna (departamental) de la universidad deben solicitarlo por al SdeI, aunque se desaconseja encarecidamente.
En ningún caso se realizan redirecciones a cuentas externas a la UC.

4.2 Respuesta automática en caso de ausencia.

El personal dispone de un sistema de respuesta automática en caso de ausencia configurable desde un cliente de correo Outlook o mediante el correo web. El sistema tiene en cuenta a las personas que ya han escrito de modo que el aviso no se envía dos veces al mismo remitente.

4.3 Cambio de clave

Los buzones de correo electrónico carecen de clave propia, ya que son un servicio al que se accede con una cuenta personal. El cambio de clave de la cuenta personal se puede realizar por web

4.4 Seguimiento de mensajes

El personal dispone de un sistema de acceso a los registros de los mensajes entregados y recibidos. El sistema es accesible mediante el correo web.

4.4 Control de dispositivos móviles

El personal dispone de un sistema para gestionar los dispositivos móviles que, utilizando tecnología

ActiveSync están vinculados a su cuenta, pudiendo realizar un borrado remoto en caso de pérdida del terminal. El sistema es accesible mediante el correo web.

4.5 Reglas de organización del correo.

El personal dispone de la posibilidad de crear reglas de procesado de mensajes que se ejecuten en el servidor sin necesidad de conectar un cliente de correo. El sistema es accesible mediante un cliente Outlook o el correo web.

5. Protección ante virus y correo no deseado.

Las estafetas de correo de la universidad analizan todo el tráfico entrante y saliente y rechazan la emisión o recepción de mensajes infectados o no deseados.

Para el control de estas políticas se aplican una serie de filtros que evalúan la legalidad del mensaje. Dichos filtros actúan sobre los parámetros que definen la comunicación. Existen **tres bloques o niveles** de filtrado.

En el caso de los dominios centrales el correo pasa en un **primer nivel de filtrado** por la Plataforma de Correo Unificada de RedIris, que realiza un filtrado de virus, reputación IP y contenido de Spam de primer nivel. El sistema rechaza el correo dirigido a direcciones inexistentes.
Los mensajes con virus son eliminados, los mensajes identificados como spam son rechazados y los mensajes identificados como con alta probabilidad de que sea spam son marcados en el asunto como [Posible Spam].

A continuación tanto el correo central como el departamental pasa por un **segundo nivel de filtrado** consistente en la verificación de:

Servidor origen El sistema rechaza todos los mensajes que provienen de servidores que,

- Estén registrados en alguna de las listas negras utilizadas por el servidor de correo entrante.
- Excedan el límite de conexiones simultáneas autorizadas
- Su IP no esté dada de alta en DNS.
- Durante la comunicación (comando HELO), no se identifiquen con un nombre que este dado de alta en DNS y esté bien formado (FQDN)

Dirección del remitente El sistema rechaza los mensajes en los que,

- El dominio del remitente no sea un dominio de correo registrado en DNS.
- Siendo un correo remitido por un servidor externo a la Universidad de Cantabria, el dominio del remitente sea un dominio interno de la universidad.
- Siendo un correo remitido por un servidor interno a la Universidad de Cantabria, el dominio del remitente sea un dominio externo de la universidad.

Dirección del destinatario El sistema rechaza los mensajes en los que,

- El dominio del destinatario no sea un dominio de correo registrado en DNS.
- Siendo un correo remitido por un servidor externo a la Universidad de Cantabria, el dominio del destinatario no sea de la Universidad de Cantabria.
- La dirección de destino sea una dirección de correo definida exclusivamente para uso interno de la Universidad de Cantabria

Para evitar posibles rechazos de correos recibidos, debido a esporádicas inclusiones de los servidores origen en las listas negras, se define una relación de servidores confiables desde los cuales se permite la recepción de correos destinados a la Universidad de Cantabria

Los mensajes que finalmente pasan todos estos filtros son procesados por otro conjunto de filtros que tratan de eliminar los mensajes reconocidos como spam y los virus que puedan ser recibidos en dichos

mensajes. Los mensajes con virus con eliminados.

Por último, en este nivel, se aplica un filtro heurístico a los mensajes restante que añade una marca de "[Posible Spam]" a aquellos mensajes que se interpreta que puedan tratarse de spam.

En el caso del Correo UC para personal, el correo pasa por un **tercer nivel de filtrado** consistente en el análisis de los mensajes mediante cinco motores antivirus distintos a los usados previamente, la comprobación de la reputación del origen IP mediante otras listas negras y un filtrado de análisis de contenidos.
Los mensajes con virus son eliminados, los mensajes identificados como spam son rechazados y los mensajes identificados como con alta probabilidad de que sean spam son colocados en una carpeta de cada buzón llamada "Correo no deseado".

6. Responsable del servicio.

El responsable del mantenimiento del servicio de correo electrónico hospedado en los servidores centrales de la universidad es el SdeI de la Universidad de Cantabria.

Es responsabilidad del SdeI:

- La apertura, administración y cierre de buzones.
- El mantenimiento de los servidores.
- La realización de copias de seguridad periódicas de los buzones.

Aunque se disponen de las direcciones técnicas de contacto abuse@unican.es y Postmaster@unican.es, los usuarios deberán contactar con el SdeI para cualquier cuestión relacionada con el servicio de la forma habitual a través de Atención a Usuarios (soporte@unican.es).

6.1. Garantía de entrega.

Aunque en un tanto por ciento muy elevado de los casos los mensajes de correo electrónico llegan a su destino rápidamente, en ningún caso el servicio de correo garantiza la entrega de un mensaje. Numerosas circunstancias pueden impedir la recepción de un mensaje: desde caídas imprevistas en las líneas de comunicaciones, límites de almacenamiento en los buzones del usuario receptor, rechazo del mensaje por virus, spam, etc...

Por lo tanto, el hecho de enviar un mensaje no supone la certeza de que este ha sido recibido por el usuario. Además el hecho de que un usuario reciba un mensaje en su buzón no debe tomarse como garantía de que dicho mensaje ha sido leído y entendido en su totalidad.

No se debe considerar al correo electrónico como un medio certificado de notificación o envío de información. En ningún caso se debe utilizar el correo electrónico para notificaciones de carácter urgente.

6.2. Privacidad del correo.

El servicio de correo electrónico proporcionado por la institución debe ser utilizado únicamente para fines profesionales relacionados con la actividad desempeñada en la misma de acuerdo a lo establecido en el "Reglamento de uso de recursos TIC de la Universidad de Cantabria", no obstante se respeta, como principio general, la privacidad de los usuarios. Nunca se realizarán monitorizaciones o inspecciones de los contenidos de los buzones personales sin el consentimiento del propietario del buzón, salvo en los casos detallados más adelante.

A esto respecto se ha de tener en cuenta que la información pública de cabecera de los mensajes y por tanto el tráfico de correo de la organización es registrado y monitorizado de acuerdo a las necesidades del servicio y a las obligaciones legales existentes.

Podrá denegarse el acceso a los servicios de correo electrónico y cancelar un buzón personal:

- Cuando haya requerimientos legales.
- Cuando haya sospechas fundadas de violación de la normativa interna de la institución.
- Cuando por circunstancias de emergencia, donde no actuar pudiera repercutir gravemente en el

servicio general a la comunidad.

Además se podrá inspeccionar y monitorizar el contenido de un buzón personal:

- Cuando haya requerimientos legales.
- Cuando se requiera para salvaguardar los intereses de la organización y en caso de cese, fallecimiento o incapacidad del propietario del buzón. En este caso se realizará siguiendo el procedimiento que determine la asesoría jurídica de la universidad con el fin de preservar los derechos legales del propietario.

Los buzones comunes e institucionales no tienen carácter privado y sus contenidos pertenecen siempre a la institución.
Su contenido podrá ser inspeccionado y monitorizado a petición del responsable de la unidad a la que está asignado el buzón común o a petición de los órganos de gobierno de la UC.

6.3. Ficheros de registro de correo (logs).

Los ficheros de log se guardarán de acuerdo con la política de conservación de los ficheros de traza, la cual garantiza su almacenamiento siguiendo lo indicado por la ley.

6.4. Abuso del servicio de correo.

Tal y como recoge la "Normativa de uso de recursos TIC de la Universidad de Cantabria", esta explícitamente prohibido el uso de cualquier recurso de TIC para la realización de algún tipo de Abuso de Correo Electrónico. Son ejemplos del mismo:

Difusión de contenido inadecuado. Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos).
Difusión a través de canales no autorizados. Uso no autorizado de una estafeta ajena para reenviar correo propio.
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 como mensajes encadenados, publicidad.
Ataques con objeto de imposibilitar o dificultar el servicio. Dirigido a un usuario o al propio sistema de correo.

Los administradores de sistemas tomarán las medidas necesarias para evitar que sus sistemas sean puedan ser usados para estas prácticas.

7. Anexos.

7.1. Descripción técnica del servicio de correo.

El servicio de correo de la Universidad de Cantabria se compone de,

Para el enrutamiento del todo el correo:

- Dos estafetas de primer nivel que son las encargadas de encaminar todo el tráfico de correo externo de Universidad, tanto el entrante como el saliente. Estos dos servidores aplican los filtros de segundo nivel antes de entregar los correos a los servidores a los que van destinados los mensajes. En el caso del tráfico de entrada del correo central estos servidores reciben los mensajes de la Plataforma Unificada de Correo de RedIris que realiza el primer nivel de filtrado.

Para el servicio central oficial:

- Dos servidores en balanceo para el acceso cliente y enrutamiento del correo del personal.
- Un clúster de correo colaborativo para el alojamiento de los buzones del personal. Los contenidos de los buzones se alojan en bases de datos que están replicadas de forma instantánea entre dos cabinas de almacenamiento situadas en CPDs distintos.

Para los servicios departamentales:

- Estafetas secundarias gestionadas por los propios departamentos.

7.2. Dominios de correo registrados.

7.2.1. Centrales.

Dependientes del SdeI de la Universidad de Cantabria.

- alumnos.unican.es
- gestion.unican.es
- unican.es
- postgrado.unican.es
- listas.unican.es

7.2.2. Departamentales.

Hospedados en servidores de correo departamentales.

- atc.unican.es
- dicom.unican.es
- frescor.org
- gtas.dicom.unican.es
- ifca.unican.es
- teisa.unican.es
- tlmat.unican.es

7.3. Encaminamiento de los mensajes.

En base a la información citada en el punto 6.2 las estafetas primarias de la universidad encaminan los mensajes a los servidores tal y como se muestra en el [Cuadro 3].

Dominio	Servidor
unican.es gestion.unican.es	correo.unican.es
alumnos.unican.es postgrado.unican.es	correo.alumnos.unican.es
listas.unican.es	Sir002.unican.es
atc.unican.es dicom.unican.es frescor.org gtas.dicom.unican.es ifca.unican.es teisa.unican.es tlmat.unican.es	Servidores Departamentales

Cuadro 3: Enrutamiento de dominios.

6.4. Configuración de clientes de correo.

La información específica sobre la configuración de los diferentes clientes de correo se encuentra publicada en la página web del SdeI en la sección dedicada al área de soporte.
Tal y como se especifica en el punto 3.3 el personal dispone de un sistema de configuración automática de clientes.

Los datos básicos para configurar los clientes de correo en los diferentes colectivos se muestran en los [cuadros 4, 5 y 6]

Servidor entrante//saliente	Nombre usuario	Direcciones de correo
correo.unican.es (*)	usuario	usuario@unican.es
		nombre.apellido@unican.es

Cuadro 4: Personal Docente e Investigador.

Servidor entrante//saliente	Nombre usuario	Direcciones de correo
correo.unican.es (*)	usuario	usuario@gestion.unican.es
		nombre.apellido@unican.es

Cuadro 5: Personal de Administración y Servicios.

(*) Para facilitar la movilidad entre dentro y fuera de la UC y mejorar la seguridad, los clientes deben utilizar el puerto 587 de los servidores salientes usando SMTP SSL-AUTH