UNIVERSIDAD D SEVILLA

# Normas de Seguridad

## Normativa de uso aceptable y seguridad básica del Correo Institucional de la Universidad de Sevilla

# Índice

# 1. Introducción

Este documento define las normas de uso y seguridad que deben seguir todos los usuarios que dispongan de una cuenta de correo corporativa en la Universidad de Sevilla (en adelante US). Las normas han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos destinados a dicho Servicio.

# 2. Objeto

El objeto de la presente normativa es regular el acceso y utilización del correo electrónico (*e-mail*) por parte de los usuarios de los Sistemas de Información de la US, desde los distintos Campus o cualquier ubicación posible, posibilitando la homogeneización de criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

# 3. Ámbito de aplicación

La presente normativa será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, pertenezca a la comunidad universitaria, incluyendo el personal de organizaciones externas cuando sean usuarios o posean acceso al Servicio de Correo de la US.

En particular, las normas contenidas en este documento serán de aplicación para todos los usuarios que dispongan de un buzón de correo corporativo o hagan uso de buzones en estafetas secundarias de correo de la US.

Los usuarios serán informados de esta Normativa de uso aceptable y seguridad básica y aceptarán que el Servicio de Informática y Comunicaciones (en adelante, SIC) sea el garante del cumplimiento de las mismas. Así mismo podrán proponer al órgano pertinente las modificaciones a este documento que consideren oportunas para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos

y finalidades del correo institucional. Los usuarios serán puntualmente informados de cualquier modificación que fuera preciso introducir.

# 4. Vigencia

La presente normativa ha sido aprobada por la Comisión de Seguridad de la US con fecha 16 de diciembre de 2016, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos que la US pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la US. Las versiones anteriores quedan anuladas por la última versión de esta normativa.

# 5. Revisión y evaluación

La gestión de esta normativa corresponde al SIC, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario, para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Cuando las circunstancias así lo aconsejen, el SIC revisará la presente normativa, que se someterá, de haber modificaciones, a la aprobación de la Comisión de Seguridad de la US.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica y organización general o cualquier otra cuestión que pueda provocarla.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

# 6. Referencias

La presente normativa se fundamenta en la legislación vigente en materia de seguridad de las Tecnologías de la Información y las Comunicaciones de ámbito europeo, estatal y autonómico, así como en las normas y procedimientos internos que resulten de aplicación a la Universidad en el marco de la Política de Seguridad de la Información.

# 7. Términos y condiciones de acceso y uso

Estos Términos y condiciones de acceso y uso regulan el uso del sistema de correo de la US.

## 7.1. Registro del usuario

El acceso y utilización del correo electrónico de la US por parte del usuario requiere de la existencia de un buzón de correo para el mismo. Este espacio depende directamente de la creación del Usuario Virtual de la US (UVUS). La información sobre estos servicios se encuentra accesible vía Web a través de la página del Servicio de Informática y Comunicaciones (en adelante SIC) de la US (http://sic.us.es).

La utilización de los sistemas de estafetas primarias por parte de las estafetas secundarias definidas depende de la viabilidad y coordinación entre los responsables de las mismas y el SIC.

El usuario se compromete a usar sus claves de acceso (nombre de usuario y contraseña) de acuerdo con las restricciones que aparecen en este documento.

## 7.2. Condiciones de uso

Para garantizar y optimizar el mejor funcionamiento del correo electrónico institucional se hace necesaria una serie de compromisos entre los usuarios y los responsables del Servicio de Correo Electrónico.

El SIC, como responsable de este servicio, debe asegurar:

- La disponibilidad del correo electrónico de la US conforme a los compromisos adquiridos de conformidad con el Acuerdo de Nivel de Servicio (SLA).
- La salvaguardia de la información almacenada en los buzones de correo electrónico.

Los compromisos por parte de los usuarios del correo electrónico de la US son los siguientes:

- Hacer un uso aceptable del correo de la US, respetando los fines para los que ha sido creado y utilizando correctamente los recursos que se le suministran.
- Evitar la interrupción de los servicios que ofrece.
- Evitar situaciones que afecten a la seguridad del correo y de sus usuarios
- Cumplir las normas de seguridad definidas en el presente documento.
- Comunicar los problemas que surjan al Servicio de Atención de Usuarios del SIC para su resolución.

## 7.3. Uso aceptable

Los usuarios del Correo electrónico de la US utilizarán el mismo para:

- La comunicación con otros usuarios, siempre que se trate de información cuyo contenido sea de investigación, académico, educacional o necesario para el desempeño de la función administrativa.

En general los usuarios del correo de la US deberán utilizar eficientemente el servicio con el fin de evitar perjuicios al resto de usuarios.

## 7.4. Uso no aceptable

El Correo Institucional de la US no debe usarse para:

- Difundir mensajes con contenidos contrarios a los principios enunciados en los Estatutos de la US: mensajes con contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o que actúen en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
- Enviar información que viole los derechos de propiedad intelectual, la LOPD o cualquier otra legislación vigente.
- Enviar información que cause cualquier tipo de molestia a otros usuarios, incluida la información difamatoria de cualquier tipo, ya sea contra entidades o personas.

- Fines privados comerciales no autorizados por la US.
- El desarrollo de actividades que produzcan:
  - La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
  - La destrucción, modificación o apropiación indebida de la información de otros usuarios.
  - La violación de la privacidad e intimidad de otros usuarios.
  - El uso y obtención de cuentas ajenas.

## 7.5. Aceptación y compromiso de cumplimiento

El uso del correo electrónico de la US implica el conocimiento y plena aceptación de las advertencias legales y condiciones vigentes en cada momento en que el usuario acceda al mismo y que se especifican en este documento.

Cualquier usuario que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta del correo corporativo de la Universidad de Sevilla.

# 8. Desarrollo de la normativa

El correo electrónico es un servicio de red que permite a los usuarios de la US enviar y recibir mensajes y, en ocasiones, estos pueden incluir ficheros adjuntos. Las características peculiares de este medio de comunicación (universalidad, bajo coste o anonimato) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

## 8.1. Enunciado de las normas generales

A fin de reducir riesgos en el uso del correo electrónico, el usuario de este servicio deberá cumplir las normas que se incluyen a continuación:

- Utilizar el correo electrónico para propósitos profesionales.

- Utilizar el correo electrónico para comunicaciones interpersonales: en ningún momento debe usarse como un medio de difusión masiva e indiscriminada de información.
- Usar protocolos seguros en los clientes de correo (SSL o TLS) para la conexión a los buzones.
- Utilizar protocolos seguros en las conexiones por SMTP para envío de correo autenticado y cifrado.
- Usar contraseñas seguras conforme a la política de contraseñas de la US.
- No ceder el uso de las cuentas de correo a terceros: las cuentas de correo son personales e intransferibles ya que esto provoca la suplantación de identidad y el acceso a información confidencial.
- No responder a mensajes de SPAM
- Utilizar mecanismos de cifrado de la información cuando los mensajes contengan información sensible, confidencial o protegida.
- No ejecutar archivos adjuntos sin analizarlos previamente con la herramienta corporativa contra código malicioso (antivirus).
- No reenviar correos en los que se haya detectado virus o código malicioso para evitar su posible propagación: todo incidente de seguridad se notificará a través del Servicio de Atención a Usuarios SOS sin reenviar el correo.
- No responder a solicitudes que pidan el usuario y/o contraseña.
- No manipular las cabeceras del correo electrónico saliente.
- Respetar el contenido de las leyes y demás disposiciones que sean de aplicación con especial atención al cumplimiento de la Ley Orgánica 15/1999 de Protección de Datos Personales (LOPD).

Además de las anteriores normas, se recomienda:

- No utilizar el correo electrónico como espacio de almacenamiento.
- Asegurar la identidad del remitente antes de abrir un mensaje: con carácter general, si no se conoce el remitente de un correo, y/o el asunto del mismo es extraño a pesar de haber traspasado el filtro de SPAM, se recomienda borrar el mensaje o situarlo en cuarentena hasta disponer de más datos, especialmente si contiene ficheros adjuntos.
- Revisar la barra de direcciones antes de enviar un mensaje para comprobar que no hay destinatarios erróneos y evitar una brecha en la confidencialidad de la información.
- Desactivar la visualización HTML de los mensajes: esto ayuda a evitar que el código malicioso se ejecute.

- Usar las listas de distribución para la difusión de la información, evitando el envío de documentos pesados a través de las mismas, para lo cual se recomienda usar enlaces a páginas web.
- Usar el campo Copia Oculta (CCO o BCC) para evitar la visibilidad de direcciones de correo a todos los receptores de un mensaje cuando el usuario tenga necesidad de enviarlo a un conjunto de destinatarios.
- Mantener actualizados los sistemas operativos de equipos, los sistemas operativos de dispositivos móviles y los clientes pesados de escritorio a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
- Ante cualquier incidencia que pueda surgir y afecte al normal comportamiento del servicio de correo, contactará con el Servicio de Atención de Usuarios del SIC.

Recomendaciones para acceso al correo vía web:

- Mantener actualizados los navegadores a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
- Cerrar la conexión al servidor una vez finalizada la sesión web.
- Desactivar la característica “recordar contraseñas” en el navegador.
- Activar en el navegador la opción de borrado automático de la información sensible al cerrar: histórico de navegación, caché, *cookies*, contraseñas, sesiones autenticadas, etc.
- No instalar *addons* (extensiones) para el navegador que puedan alterar el normal funcionamiento del acceso web al correo.

## 8.2. Normas específicas de uso de estafetas secundarias

La Universidad de Sevilla permite el uso de Estafetas Secundarias de correo siempre y cuando tengan razón de ser en cuanto a número de buzones afectados, responsabilidad del servicio, coordinación con el grupo de personas que administran las estafetas primarias de la Universidad de Sevilla y aceptación de la política de correo universitaria.

## 8.3. Normas específicas de prevención contra correo basura (SPAM)

Además de las medidas técnicas de prevención y eliminación de SPAM ya instaladas en la US a través del SIC, se detallan seguidamente las normas que todo usuario deberá seguir para hacer frente a este problema:

- Con carácter general, sólo se proporcionará la dirección de correo electrónico profesional de la US a personas de confianza y del entorno profesional.
- Se debe evitar introducir la dirección de correo de la US en foros de noticias o listas de correo a través de Internet, salvo en los casos necesarios y con proveedores de confianza.
- Si a pesar de las medidas de prevención instaladas el usuario recibe un mensaje de SPAM:
  - No accederá a los enlaces o adjuntos que pudieran contener.
  - Lo comunicará al SIC a través del Servicio de Atención a Usuarios SOS inmediatamente.

# 9. Responsabilidades

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, cuando se detecten envíos masivos o cualquier otra actividad abusiva que pudiera perjudicar el correcto funcionamiento del Servicio de Correo, o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC procederá, dependiendo de la gravedad y reiteración del incidente, a aplicar una de estas medidas:

### Suspensión temporal del buzón de correo de un usuario

Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de nuestra institución o implique a la US en algún tipo de responsabilidad que conlleve perjuicio para sus usuarios. La acción a tomar y la duración de la misma dependerán de la incidencia, si bien, como medida de precaución se procederá a deshabilitar la cuenta del usuario, no permitiendo el acceso al correo universitario.

### Suspensión temporal del acceso de la estafeta secundaria al puerto 25 de mail.us.es

Se tomará esta medida cuando se produzca un mal uso del servicio que ofrece la estafeta secundaria de correo.

### Suspensión indefinida del usuario o la estafeta secundaria

Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por el cauce adecuado.

En todos los casos el servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable de la cuenta de correo o estafeta secundaria garanticen un uso aceptable en el futuro.

### Exención de responsabilidades de la US por los contenidos

La Universidad de Sevilla no se hace responsable del contenido de los mensajes enviados por los usuarios a través de cualquiera de las formas de utilización del correo universitario. En cualquier caso, la Universidad de Sevilla se compromete a actuar con diligencia para evitar cualquier uso indebido del servicio.

## Apéndice: Lenguaje de género

Esta normativa ha sido redactada con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.

# ANEXO: Acrónimos y glosario de términos

Addons

Extensiones, también llamados *plugins* o complementos: son programas que sólo funcionan anexados a otro y que sirven para incrementar o complementar sus funcionalidades

CCN-Cert

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

ESTAFETAS PRIMARIAS DE CORREO DE LA US

Sistemas que gestionan todo el tráfico de correo entrante y saliente de la US administradas por el SIC.

ESTAFETAS SECUNDARIAS DE CORREO EN LA US:

Sistemas que gestionan subdominios bajo el dominio de correo @us.es. Administradas por el SIC, Centros o Departamentos.

LOPD

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (cualquier información concerniente a personas físicas identificadas o identificables).

MX DE LA US (buzon.us.es)

Mail eXchange record (registro de intercambio de correo). Es un tipo de registro en el Servidor de Nombres, DNS, que especifica cómo debe ser encaminado un correo electrónico en internet. Los registros MX apuntan a los Sistemas que reciben todo el correo dirigido al dominio @us.es y todos los subdominios que dependen de él.

mail.us.es (correo autenticado)

Nombre del servidor de correo de la US: es el sistema de estafetas primarias diseñado para enviar correo autenticado y cifrado, única forma de envío permitida en la US.

RedIris

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

SERVICIO DE INFORMÁTICA Y COMUNICACIONES

Servicio de la Universidad responsable de gestionar el Correo Institucional de la US.

SLA

*Service Level Agreement* o "Acuerdo de Nivel de Servicio" (ANS) en castellano. Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel de calidad de dicho servicio.

SMTP

*Simple Mail Transfer Protocol* o "protocolo para transferencia simple de correo" en castellano. Es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre dispositivos.

SPAM

Correo electrónico masivo no solicitado.

SSL

*Secure Sockets Layer* (capa de puertos seguros) es un protocolo criptográficos que proporciona comunicaciones seguras por red.

TLS

*Transport Layer Security* (seguridad de la capa de transporte) es una versión actualizada y más segura del protocolo SSL.

UVUS

Usuario Virtual de la Universidad de Sevilla.

PORTAL INSTITUCIONAL DE LA US

Página oficial de la Universidad de Sevilla que proporciona el acceso a la mayor parte de los contenidos Web institucionales, académicos y de investigación existentes en la Universidad.

## USUARIOS DE CORREO CORPORATIVO DE LA US

Estudiantes, profesores, investigadores, personal de la administración y servicios, resto de miembros de la Comunidad Universitaria y, en general, cualquier persona externa a la Universidad de Sevilla que disponga de un buzón de correo corporativo en la misma por su relación con la US.