Centro Informático Científico de Andalucía
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

JUNTA DE ANDALUCIA

NORMAS DE SEGURIDAD INFORMÁTICA

CENTRO INFORMÁTICO CIENTÍFICO DE ANDALUCÍA

NS01 – CORREO ELECTRÓNICO

Fecha: 22 agosto 2019

Índice de contenido

1. OBJETIVO

1. El presente documento constituye la norma de seguridad del CICA en cuanto al uso del correo electrónico corporativo, y forma parte del conjunto de normas de seguridad del CICA, "NS00 CICA – GENERAL".

2. USO DEL CORREO ELECTRÓNICO CORPORATIVO

2. El Centro Informático Científico de Andalucía (CICA) ofrece el servicio de correo electrónico a la comunidad universitaria e investigadora de Andalucía, así como a aquellas instituciones o asociaciones que estén acogidas bajo un acuerdo de servicio en nuestro centro.
3. El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.
4. Junto con los mensajes también pueden ser enviados ficheros adjuntos. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.
5. Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos.
6. Por ello, se dictan las siguientes normas de uso:

2.1. NORMAS GENERALES

7. Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.
8. Se harán copias de seguridad diarias de los buzones de usuario/usuaria, manteniendo un histórico mínimo de una semana y máximo de un mes. No obstante, es responsabilidad del usuario/usuaria hacer copia de los mensajes importantes en su medio local y personal.
9. El tamaño máximo que puede tener un mensaje es de 20 Megabytes. Debe tenerse en cuenta que el envío a cuentas externas pueden impedir el trasiego de mensajes de este volumen e impedir que dicho mensaje llegue su destinatario.
10. Se utilizarán contraseñas seguras para el acceso al correo (ver Norma "NS03 CICA - CONTRASEÑAS").
11. Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por el CICA.
12. El correo corporativo deberá utilizarse única y exclusivamente, para la realización de las funciones encomendadas al personal, quedando totalmente prohibido el uso privado del mismo.
13. Se deberá notificar al CSU cualquier tipo de anomalía detectada, así como los correos no deseados (spam) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas.
14. Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse

ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia al CSU.

15. Es importante revisar la barra de direcciones antes de enviar un mensaje. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información. Cuando se responde a un mensaje es importante revisar las direcciones que aparecen en el campo Con Copia (CC). Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.
16. No se deben enviar o reenviar correos de forma masiva. Si se envía por necesidad un correo a un conjunto de destinatarios, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Copia Oculta (CCO o BCC), evitando su visibilidad a todos los receptores del mensaje.
17. No enviar mensajes en cadena. Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe notificar la incidencia al CSU.
18. No responder a mensajes de Spam. La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envían a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa al CICA.

    En cualquier caso, nunca debe responderse a los mismos.
19. Utilizar mecanismos de cifrado de la información. Los mensajes que contengan información sensible, confidencial o protegida deben cifrarse. El Área de Seguridad pondrá a disposición de los usuarios que lo precisen el acceso a la aplicación necesaria para el cifrado de información.
20. Asegurar la identidad del remitente antes de abrir un mensaje. Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) del usuario atacado. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información sensible, confidencial o protegida a petición de un correo del que no se puede asegurar la identidad del remitente debe rechazarse.
21. Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).
22. Desactivar la vista previa. Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos.
23. Limitar el uso de HTML. El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute.

24. Utilizar herramientas de análisis contra código dañino. La utilización de herramientas tales como antivirus y cortafuegos ayuda a detectar el código malicioso y a mitigar sus efectos. Por ello, debe configurarse el antivirus con la opción de analizar el correo electrónico entrante.
25. No abrir correos basura ni correos sospechosos. Aun cuando un mensaje no deseado hubiera traspasado el filtro contra spam, no debe abrirse, debiendo reportarse el correspondiente incidente de seguridad. Es conveniente borrar los correos sospechosos o, al menos, situarlos (sin abrir) en una zona de cuarentena.
26. No ejecutar archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso.
27. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).
28. Informar de correos con virus, sin reenviarlos. Si el usuario detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente de seguridad y no reenviarlo, para evitar su posible propagación.
29. No utilizar el correo electrónico como espacio de almacenamiento. La capacidad de espacio en los servidores de correo del CICA es limitada. Cuando una cuenta se satura puede ser que se restrinjan por parte del servidor los privilegios de envío y/o recepción de mensajes o que se realice un borrado, más o menos selectivo, de los mensajes almacenados. Por todo ello, se recomienda conservar únicamente los mensajes imprescindibles y revisar periódicamente aquellos que hubieren quedado obsoletos.
30. En relación con el acceso remoto (vía web) al correo electrónico, deben adoptarse las siguientes cautelas:
    - Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
    - Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
    - Desactivar la interpretación de contenidos remotos a la hora de leer mensajes de correo vía webmail.
    - Desactivar las características de recordar contraseñas para el navegador.
    - Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
    - Salvo autorización expresa, está prohibida la instalación de addons para el navegador.
31. Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones, de conformidad con lo dispuesto en el art. 23. Registro de actividad, del ENS.

2.2. PREVENCIÓN CONTRA SPAM

32. El término spam se define como el envío de correos no solicitados, de forma masiva, a direcciones de correo electrónico, constituyendo uno de los problemas de seguridad más habituales con los que se enfrentan las organizaciones. Tales mensajes pueden contener código dañino que, de penetrar en los sistemas de información, podrían llegar a colonizar una institución y propagarse a través de las redes de comunicaciones.

33. Además de las medidas técnicas de prevención y eliminación de spam ya instaladas en el CICA a través del Área responsable de Microinformática, 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 del CICA a personas de confianza y del entorno profesional.
- Se debe evitar introducir la dirección de correo del CICA en foros de noticias o listas de correo a través de Internet, salvo en los casos necesarios y con proveedores de confianza. Muchos ataques de spam se sirven de estas direcciones, introducidas en sitios no seguros.
- Con carácter general, si no se conoce el remitente de un correo, y/o el asunto del mismo es extraño, se recomienda borrar el mensaje (o situarlo en cuarentena hasta disponer de más datos), especialmente si contiene ficheros adjuntos.

34. El CICA dispone de sistemas antispam para la detección y borrado de mensajes identificados como spam. Sin embargo, es posible que dichos sistemas no puedan eliminar la totalidad de estos mensajes. Por este motivo, si el usuario recibe un mensaje de spam seguirá las siguientes instrucciones:

- Si lo reconociera como tal por la dirección o el asunto que contiene, lo borrará inmediatamente (sin abrirlo).
- No responderá nunca.
- No accederá a los enlaces o anexos que pudieran contener.
- Comunicarlo al CSU inmediatamente, a través de los canales establecidos.

2.3. USOS ESPECIALMENTE PROHIBIDOS

35. Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.
- Está terminantemente prohibido suplantar la identidad de un usuario de Internet, correo electrónico o cualquier otra herramienta colaborativa.
- Ceder el uso de las cuentas de correo. Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales -para los que deberá solicitarse y obtenerse la correspondiente

autorización-, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial.

Además de ello, es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios.

- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.
- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.
- Responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.
- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información sensible, confidencial o protegida. El sistema evitará el intercambio de correos de tamaños superiores al límite establecido en los procedimientos y guías técnicas específicas sobre correo electrónico.
- La utilización del correo corporativo para recoger correo de buzones que no pertenezcan al CICA o el reenvío automático del correo corporativo a buzones ajenos a la organización. para ello se necesitará la autorización expresa del Área de Seguridad.

2.4. BAJA EN EL SERVICIO

Las cuentas de correo de CICA pueden encontrarse en estado:

36. Bloqueada, cuando el usuario/usuaria no puede enviar correos desde su cuenta.

    Puede producirse en los siguientes casos:

    - Se sospecha que ha sido interceptada por terceras personas.
    - Ha infringido la ley o norma.
    - El usuario/usuaria ha causado baja en el organismo al cual pertenecía.
    - Se ha detectado envío masivo de correos desde dicha cuenta sin autorización.
    - La última fecha de acceso al correo es superior a 10 meses.

37. Cancelada, cuando la cuenta de correo ha sido eliminada del servidor.

    Una cuenta puede ser eliminada cuando:

    - El usuario/usuaria así lo pida desde la propia dirección de correo.
    - Transcurridos 3 meses en estado bloqueada el usuario

2.5. RECOMENDACIONES ADICIONALES

38. Asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.
39. Evitar, en la medida de lo posible, el uso ineficiente en los envíos de correo: agrupar los envíos a

múltiples destinatarios en un solo mensaje, evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos (ya que incrementan innecesariamente el tamaño y volumen de los mismos), envíos innecesarios, etc.

40. Los buzones de correo se configuran con un tamaño para almacenamiento limitado según el tipo de usuario al que pertenezcan y cuya relación actualizada se encuentra en el procedimiento técnico específico de correo electrónico que se encuentra en el gestor documental del CICA (https://www.cica.es/servicios/colaboracion/servicio-de-correo-electronico-con-dominio-cica-es/). El sistema indicará cuándo se encuentra al límite de su capacidad, tras el cual no se permitirá enviar y recibir correos.

2.6. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

41. Todos los usuarios de los recursos informáticos y/o Sistemas de Información del CICA deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa de uso del Correo Electrónico (e-mail) Corporativo, debiendo suscribirla.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [personal del CICA/ empleado de la <<EMPRESA>>], como usuario de recursos informáticos y sistemas de información del CICA, declara haber leído y comprendido la Normativa de uso del Correo Electrónico (e-mail) Corporativo del CICA (versión x) y se compromete, bajo su responsabilidad, a su cumplimiento.

<<En _____, a _____ de _____ de 20__>>

Organismo:	
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Por el CICA: _____

DNI número: _____

Número de Registro de Personal: _____