GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 821

APÉNDICE III: NORMAS DE USO DEL CORREO ELECTRÓNICO (E-MAIL) NP20

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.02.23 09:29:46 +01'00'

FEBRERO 2018

ÍNDICE

1. OBJETIVO

1. El objetivo de la presente norma es regular el **acceso y utilización del correo electrónico (e-mail)** por parte de los usuarios de los Sistemas de Información de la <<ENTIDAD>>, desde las distintas sedes de la <<ENTIDAD>> o a través de ellas, 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.

   La presente Normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. Este documento se considera de uso interno de la <<ENTIDAD>> y, por tanto, no podrá ser divulgado salvo autorización de la <<ENTIDAD>>.

2. ÁMBITO DE APLICACIÓN

3. Esta Norma es de aplicación a todo el ámbito de actuación de la <<ENTIDAD>>, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la <<ENTIDAD>>.

4. La presente Norma **será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la <<ENTIDAD>>,** incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la <<ENTIDAD>>.

3. VIGENCIA

5. La presente Norma ha sido aprobada por la <<U/OC>> de la <<ENTIDAD>>, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la <<ENTIDAD>> 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.

6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la <<ENTIDAD>>.

7. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

4. REVISIÓN Y EVALUACIÓN

8. La gestión de esta Normativa corresponde a la <<U/OC>>, 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.

9. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la <<U/OC>> revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> de la <<ENTIDAD>>.

10. 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, organización general, etc.

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

5. REFERENCIAS

12. *<<En este epígrafe se deben incluir aquellas referencias documentales que vengan a apoyar o completar esta Norma o que hubieren sido consideradas en su redacción.*

***Internas**:*

- ----
- ----
-

***Externas**:*

(Por ejemplo:

- *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*
- *UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.*
- *UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.*
- *ISO/IEC 9001:2000 Sistemas de gestión de la calidad.*
- *Documentos y Guías CCN-STIC.*
- *Etc.>>*

6. NORMAS PREVIAS

13. Las presentes "Normas de Uso del Correo Electrónico (e-mail) en la <<ENTIDAD>>" complementa, en sus aspectos específicos, a la "NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>>"[1], por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

7. NORMATIVA

14. El correo electrónico (e-mail) es un servicio de red para permitir a los usuarios de la <<ENTIDAD>> enviar y recibir mensajes. 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.

[1] Se recomienda que el organismo disponga de una Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>>, del tipo descrito en el documento CCN STIC – 821 - NG00.

15. En este sentido, la medida de seguridad [mp.per.2] del ENS señala:

> **Deberes y obligaciones [mp.per.2].**
>
> 1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.
>
> a) Se especificarán las medidas disciplinarias a que haya lugar.
>
> b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
>
> c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.
>
> 2. En caso de personal contratado a través de un tercero:
>
> a) Se establecerán los deberes y obligaciones del personal.
>
> b) Se establecerán los deberes y obligaciones de cada parte.
>
> c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

16. A continuación, se incluye un conjunto de normas que tienen como objetivo reducir el riesgo en el uso del correo electrónico:

- **Utilizar el correo electrónico exclusivamente para propósitos profesionales.** Gran parte de los mensajes de correo electrónico no deseados que llegan a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo. Utilizar el correo electrónico únicamente para fines profesionales reduce la posibilidad de ataque.

  Existen numerosos proveedores de servicios de Internet que proporcionan cuentas de correo electrónico gratuitas (gmail, yahoo, hotmail, etc.) que los usuarios pueden configurar y usar en sus ordenadores privados, fuera de las dependencias de la <<ENTIDAD>> y de su perímetro de seguridad.

- **Usar contraseñas seguras**[2]**.** Para limitar la posibilidad de un acceso no autorizado a las cuentas de correo electrónico, es conveniente utilizar contraseñas robustas.
- **No 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.

- **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

[2] Véase: Normas de Creación y Uso de Contraseñas CCN-STIC 821 - NP40.

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.

- **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.
- **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 a la <<U/OC>>.
- **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 a la <<ENTIDAD>>.

  En cualquier caso, nunca debe responderse a los mismos.
- **Utilizar mecanismos de cifrado de la información.** Los mensajes que contengan información sensible, confidencial o protegida deben cifrarse. <<U/OC>> pondrá a disposición de los usuarios que lo precisen el acceso a la aplicación necesaria para el cifrado de información.
- **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.

  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).
- **Desactivar la *vista previa***. Utilizar la *vista previa* para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos.
- **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.

- **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.
- **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.
- **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.

  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.).
- **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.
- **No utilizar el correo electrónico como espacio de almacenamiento.** La capacidad de espacio en los servidores de correo de la <<ENTIDAD>> 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.
- 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.

- Además de lo anterior, cualquier información sensible, confidencial o protegida que permanezca almacenada en el servidor de correo podría ser accedida por un atacante, lo que aconseja su borrado.

17. Además de lo anterior, cualquier información sensible, confidencial o protegida que permanezca almacenada en el servidor de correo podría ser accedida por un atacante, lo que aconseja su borrado.

8. PREVENCIÓN CONTRA SPAM

18. 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.

19. Además de las medidas técnicas de prevención y eliminación de spam ya instaladas en la <<ENTIDAD>> a través de la <<U/OC>>, 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 <<ENTIDAD>> a personas de confianza y del entorno profesional.
- Se debe evitar introducir la dirección de correo de la <<ENTIDAD>> 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.

20. La <<ENTIDAD>> 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, deberá:

- 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 <<U/OC>> inmediatamente, (por ejemplo, a través de la <<herramienta de Atención a Usuarios>>).

9. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

21. Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la <<ENTIDAD>> deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma, debiendo suscribirla.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la <<ENTIDAD>>/empleado de la <<EMPRESA>>*], como usuario de recursos informáticos y sistemas de información de la <<ENTIDAD>>, declara haber leído y comprendido las Normas de Uso del Correo Electrónico (e-mail) de la <<ENTIDAD>> (*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 la <<ENTIDAD>>: <<*Nombre y Apellidos*>>

DNI número: _____

Número de Registro de Personal: _____