GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 821

APÉNDICE IV: NORMAS PARA TRABAJAR FUERA DE LAS INSTALACIONES DE LA ENTIDAD NP30

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 09:30:38 +01'00'

FEBRERO 2018

ÍNDICE

1. OBJETIVO

1. El objetivo de la presente norma es **regular el trabajo del personal de la <<ENTIDAD>> cuando desarrolle su actividad profesional fuera de los edificios, dependencias o instalaciones de la <<ENTIDAD>>**.

> 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 de la <<ENTIDAD>> o adscrito a él que, de manera permanente o eventual, desarrolle su trabajo fuera de sus instalaciones.

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 para trabajar fuera de las instalaciones de 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 trabajo fuera de las instalaciones de la <<ENTIDAD>> comprende tanto el teletrabajo habitual y permanente de los usuarios desplazados, como el trabajo ocasional, usando, en ambos casos, dispositivos de computación y comunicación (usualmente: ordenador portátil, *tablet*, teléfono móvil, etc.). Este modo de trabajo comprende también las conexiones remotas realizadas desde Congresos o sesiones de formación, alojamientos o, incluso, llamadas telefónicas de contenido profesional que sean realizadas o atendidas en áreas públicas.

15. El trabajo fuera de las instalaciones de la <<ENTIDAD>> conlleva el riesgo de trabajar en lugares desprotegidos, esto es, sin las barreras de seguridad físicas y lógicas implementadas en sus instalaciones. Fuera de este perímetro de seguridad

[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.

aumentan las vulnerabilidades y la probabilidad de materialización de las amenazas, lo que hace necesario adoptar medidas de seguridad adicionales.

16. Se incluyen seguidamente un conjunto de normas de obligado cumplimiento, que tienen como objetivo el reducir el riesgo cuando se trabaja fuera de las instalaciones de la <<ENTIDAD>>.

- **Uso personal y profesional**. Los dispositivos móviles de computación y comunicación asignados al usuario de la <<ENTIDAD>>, son para su uso exclusivo y solamente pueden ser utilizados para fines profesionales. No pueden prestarse a terceros salvo autorización expresa de la <<U/OC>>, que incluirá en todo caso la definición de las condiciones de uso.
- **Necesidad de Autorización**. La salida fuera de las dependencias de la <<ENTIDAD>> de documentación, equipos y dispositivos informáticos y de comunicaciones precisa autorización previa de la <<U/OC>>.

  Asimismo, es necesaria la correspondiente autorización para utilizar equipos personales del usuario en el tratamiento de la información de la organización o en el acceso a recursos o sistemas de información de la <<ENTIDAD>>.
- **Copias de seguridad**. Regularmente, debe realizarse copia de seguridad de la información contenida en los dispositivos móviles. Análogamente, es necesario adoptar las medidas adecuadas para la protección de dichas copias.
- **Uso de los canales de comunicación establecidos**. La transmisión de información y el acceso remoto se realizará únicamente a través de los canales establecidos, siguiendo los procedimientos y requisitos definidos para ello y adoptando las siguientes precauciones:
  - En caso de utilizar contraseñas en la autenticación, estas deben ser robustas[2].
  - Cerrar siempre la sesión al terminar el trabajo.
  - Cifrar la información sensible, confidencial o protegida que vaya a ser transmitida a través de correo electrónico o cualquier otro canal que no proporcione la confidencialidad adecuada.
- **Vigilancia permanente**. La documentación y los dispositivos móviles deben estar vigilados y bajo control para evitar extravíos o hurtos que comprometan la información almacenada en ellos o que pueda extraerse de ellos. En los desplazamientos en avión, este tipo de equipamiento no debe facturarse y deberá viajar siempre con el usuario.
- **Evitar el acceso no autorizado**. El trabajo en lugares públicos debe realizarse con la mayor cautela y precaución, evitando que personas no autorizadas vean o escuchen información interna a la organización.
- En relación con el **acceso remoto (vía web)**, deben adoptarse las siguientes cautelas:

[2] Ver Norma de Creación y Uso de Contraseñas NP40, en esta misma Guía.

- Los navegadores utilizados para el acceso 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 las características de recordar contraseñas en 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.

- **Transporte seguro**. La documentación y equipos que salgan de las instalaciones de la <<ENTIDAD>> se deberá transportar de manera segura, evitando proporcionar información sobre el contenido en los mismos y utilizando, en su caso, maletines de seguridad que eviten el acceso no autorizado.
- **Utilización de candados**. Es obligatorio el uso de candados y/o cables de seguridad para los dispositivos de computación que deban permanecer desatendidos fuera de las instalaciones de la <<ENTIDAD>>.
- **Mantenimiento de los equipos**. Los equipos se mantendrán de acuerdo con las especificaciones técnicas de uso, almacenamiento, transporte, etc., proporcionadas por el fabricante. En particular, se evitará su uso en condiciones de temperatura o humedad inadecuadas, o en entornos que lo desaconsejen (mesas con alimentos y líquidos, entornos sucios, etc.).
- **Revisión periódica de los equipos.** Al menos, dos veces al año, para verificar la ausencia de sw dañino.
- **Normativa interna**. Durante la actividad profesional fuera de las instalaciones de la <<ENTIDAD>> se seguirán las normas, procedimientos y recomendaciones internas existentes, atendiendo de manera especial a las siguientes:
  - Las contraseñas deberán ser robustas y renovarse periódicamente o cuando se sospeche que pueden estar comprometidas.
  - El almacenamiento de la información en soportes electrónicos (CDs, DVDs, memorias USB, etc.), debe caracterizarse por no ser accesible para usuarios no autorizados. Para ello, es necesario aplicar claves de acceso o algoritmos de cifrado cuando la naturaleza de la información así lo aconseje.
  - No desactivar las herramientas de seguridad habilitadas en los dispositivos móviles (ordenadores portátiles, móviles, tablets, etc.) y comprobar que se mantienen actualizadas.
  - No descargar ni instalar contenidos no autorizados en los equipos (tonos de teléfono, aplicaciones para tablets o móviles, etc.).

8. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

17. 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 para trabajar fuera de las instalaciones 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: _____