Comisión Nacional de Prevención de Riesgo
y Atención de Emergencias
PRESIDENCIA

CIRCULAR
CNE-PRE-CIR-006-2019

PARA: Srs. Directores
Srs. Jefaturas de Unidad.
Funcionarios

DE: Sr. Alexander Solís Delgado, Presidente CNE

ALEXANDER SOLIS DELGADO (FIRMA)
Firmado digitalmente por ALEXANDER SOLIS DELGADO (FIRMA)
Fecha: 2019.10.29 09:50:38 -06'00'

FECHA: 28 de octubre, 2019

ASUNTO: Directrices para el buen uso de las Tecnologías de Información en la CNE

Con el fin de promover sanas prácticas que contribuyan a mejorar el uso y aprovechamiento de las Tecnologías de Información, como herramientas para el desempeño de las tareas y actividades que les son encomendadas a los funcionarios de la CNE en su quehacer diario, el Comité de Tecnologías de Información y la Unidad de Tecnologías de Información, elaboraron el documento "Directrices para el buen uso de las Tecnologías de Información en la CNE", el cual se adjunta.

Por lo anterior, se solicita la implementación de dichas normas a partir de la fecha de recepción de esta circular.

Saludos cordiales,

A.S.D.

🗁: Archivo

ASD/jgv

CNE-UTI-DIR-001-19

DIRECTRICES PARA EL BUEN USO DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LA CNE

VERSION 1.0

ELABORADO POR:

UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN

JUNIO, 2019

TABLA DE CONTENIDO

CAPÍTULO 1: ASPECTOS GENERALES

1.1 Objeto de las Directrices

Incorporar en la gestión de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias, un conjunto de acciones que permitan preservar las características de confiabilidad, integridad, confidencialidad, disponibilidad y privacidad de la información institucional, de conformidad al numeral 1.4 de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), con el fin de promover sanas prácticas que contribuyan a mejorar el uso y aprovechamiento de las Tecnologías de Información, como herramientas para el desempeño de las tareas y actividades que les son encomendadas a los funcionarios de la CNE en su quehacer diario.

1.2 Ámbito de aplicación

El ámbito de aplicación de las presentes directrices es institucional y atañe a todos los funcionarios de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (en adelante CNE) y personal en labores temporales, salvo en aquellos casos que señalen una responsabilidad particular para algunas unidades.

CAPÍTULO 2: ACERCA DE LOS USUARIOS Y CONTRASEÑAS

2.1 Administración de usuarios

a. La Unidad de Tecnologías de Información de la CNE (en adelante UTI) será la entidad encargada de la administración de los recursos de Tecnologías de Información y Comunicaciones (en adelante TIC) de la institución.

b. Todos los usuarios de recursos TIC de la CNE requieren de una identidad intransferible, compuesta por un código de usuario y una contraseña secreta, que cumpla con los requisitos mínimos establecidos por la UTI (ver apartado 2.2 “Sobre Administración de Contraseñas”), o bien, un certificado digital reconocido por la CNE. Para el sistema de impresión aplica un código compuesto por la combinación de 4 dígitos numéricos.

c. El usuario es el responsable de todas las acciones que se realicen con la identidad que le fue asignada, salvo en los casos en que se demuestre que ese mecanismo de identificación ha sido vulnerado, y que ello no responda a una falta de cuidado de su parte.

d. La Unidad de Desarrollo Humano (en adelante UDH) reportará oportunamente a las jefaturas respectivas y a la UTI, todos los ingresos, egresos o cambios de personal, con el fin de mantener un registro actualizado de los usuarios de los recursos TIC. Esto con el fin de crear, deshabilitar, reactivar o eliminar usuarios según corresponda.

e. Los directores y/o jefes inmediatos definirán los roles y privilegios que aplican a los diferentes usuarios de los sistemas, aplicaciones y/o servicios tecnológicos de la CNE. Mediante estos roles se establecerá la segregación de funciones y la delegación de acciones. La UTI implementará estos roles y privilegios conforme a lo que los directores y/o jefes inmediatos soliciten.

f. Una vez que la UDH haya realizado la notificación respectiva y posterior a la solicitud de la jefatura solicitante, la UTI dispondrá de al menos 24 horas para proceder con las acciones requeridas.

g. Es responsabilidad de cada director y/o jefatura inmediata solicitar a los responsables de la administración de recursos TIC, el otorgar, suspender y revocar los privilegios sobre el uso de estos recursos para los usuarios a su cargo.

h. Cuando proceda, la UTI, en coordinación con el jerarca inmediato, actuará de oficio con el comunicado que la Unidad de Desarrollo Humano emita, con relación a la suspensión o eliminación de privilegios a un usuario determinado, sobre el uso de los recursos TIC.

i. Cuando proceda, la UTI deberá eliminar o cambiar la contraseña de todos los usuarios que estén preinstalados en los equipos TIC que se adquieran.

2.2 Sobre la administración de contraseñas

a. La UTI debe definir y administrar los lineamientos para la asignación, mantenimiento y revocación de las contraseñas.

b. Las contraseñas deben ser robustas, en tanto la tecnología lo permita, lo que implica que cumplan con las siguientes características:

- Debe contener al menos 8 caracteres siendo estos a escoger entre tres de las siguientes categorías: mayúsculas, minúsculas, números y símbolos especiales. **Ej: C0m1$10n**
- No podrá contener partes de la identidad, nombres o apellidos del usuario.
- Se deberá cambiar cada 90 días.
- No se podrán repetir las tres contraseñas anteriores.
- Otras que implemente y divulgue la UTI

c. Cuando proceda, estas contraseñas deben expirar periódicamente según los criterios definidos por la UTI.

d. Cuando proceda, la UTI dispondrá de la tecnología necesaria para el almacenamiento y transmisión encriptada de las contraseñas de los recursos TIC.

e. Cuando se requiera acceder un sistema de información y no se encuentre el funcionario que cuenta con el perfil para realizar tareas específicas en éste, la jefatura podrá solicitar a la UTI la asignación temporal de los permisos necesarios a quien designe y autorice. Es responsabilidad de la jefatura notificar a la UTI en el momento que ya no se requieran más esos permisos, para que se proceda a revocarlos.

CAPÍTULO 3. SEGURIDAD DE LA INFORMACIÓN

3.1 Control de amenazas

a. Todas las computadoras y cuando aplique en otros dispositivos (teléfonos inteligentes, tabletas, etc.), deben contar con un programa antivirus activo, actualizado y aprobado por la UTI.

b. La UTI es la responsable de colocar a disposición de los funcionarios de la CNE, las versiones actualizadas del programa de antivirus utilizado en la institución.

c. Es responsabilidad del usuario vigilar que la versión de su antivirus se encuentre actualizada y operando, de conformidad al procedimiento para tal fin dispuesto en la intranet. En caso contrario deberá informar a la UTI para proceder con la debida corrección. Además, es responsabilidad del usuario informar a la UTI en el momento de detectar algún virus o un comportamiento anormal sobre el equipo en uso.

d. La UTI debe monitorear permanentemente la existencia de programas maliciosos como lo son troyanos, gusanos, adware, ransomware, y proceder a aplicar las medidas preventivas y correctivas para minimizar el riesgo de contaminación de los equipos institucionales.

e. La UTI, mediante dispositivos o programas de validación, eliminará o pondrá en cuarentena aquellos correos electrónicos detectados como sospechosos, que entren o salgan de la CNE.

f. La UTI es la responsable, mediante la utilización de dispositivos especializados, de detectar y bloquear ataques o accesos no autorizados a equipos o redes definidas.

g. La UTI gestionará ante los proveedores de servicio correspondientes, la solución a problemas que no haya sido posible solventar mediante la infraestructura tecnológica en uso.

h. La UTI definirá las políticas para la conexión de dispositivos no autorizados a los equipos de la CNE (Device Control[1]), a la red interna (Network Access Control[2]) y/o la implementación de un sistema de prevención para la fuga o perdida de datos (Data Lost Prevention[3]).

[1] Device Control: control de dispositivos o equipos
[2] Network Access Control: Control de acceso a la red
[3] Data Lost Prevention: Prevención de la perdida de datos

3.2 Cifrado de información.

a. Cuando se tenga información de carácter confidencial o sensible dentro de una estación de trabajo o en un dispositivo de almacenamiento externo, el usuario deberá proceder a cifrarla utilizando las herramientas que la UTI ponga a su disposición.

CAPÍTULO 4: INFRAESTRUCTURA TECNOLÓGICA

4.1 Sobre la asignación, uso y cuidado de los equipos

a. Todos los equipos TIC propiedad de la CNE son bienes públicos destinados exclusivamente para satisfacer el cometido público que corresponde a la Institución.

b. Cada equipo tendrá asignado un responsable, quien es el encargado de velar por su adecuado registro, identificación, manejo eficiente y control, de conformidad a los lineamientos que para tal fin dicta el Reglamento para el registro y control de bienes de la administración central, así como la Unidad de Proveeduría Institucional, encargada del control y fiscalización de activos.

c. Para que la UTI proceda con la asignación de equipos se deberá cumplir previamente con lo establecido en el Capítulo 2: ACERCA DE LOS USUARIOS Y CONTRASEÑAS, Numeral 2.1: Administración de usuarios, incisos d, e y f.

d. La UTI evaluará la solicitud, buscará y preparará, de conformidad a la disponibilidad de equipo, el adecuado para el nuevo colaborador y programará su asignación. Para esto dispondrá de un máximo de tres días hábiles. En caso de no contar con equipo disponible, se informará a la jefatura respectiva para buscar una alternativa de solución.
En caso de ingresos masivos de funcionarios (5 o más), es responsabilidad de la jefatura y/o Dirección que está gestionando el proceso, notificar a la UTI con al menos 7 días de anticipación, para verificar la disponibilidad de equipos.

e. El día de la asignación del equipo, el nuevo colaborador recibirá una breve inducción acerca de las herramientas que tendrá disponibles para la ejecución de sus tareas diarias, así como sus credenciales de acceso.

f. El usuario será el responsable de apagar o bloquear el computador a su cargo cuando no esté en su puesto de trabajo, para evitar cualquier uso no autorizado del equipo.

g. Las computadoras portátiles, en ausencia del responsable, deben estar debidamente aseguradas con el respectivo candado de seguridad.

4.2 Control y Gestión de la Plataforma Tecnológica.

a. La UTI tiene la potestad de desconectar aquellos equipos que representan un riesgo sobre el resto de la plataforma tecnológica de la CNE.

b. Solo personal técnico de la UTI o cualquier otro debidamente autorizado por los responsables correspondientes, puede revisar, configurar y dar soporte a los equipos de cómputo y a la plataforma tecnológica institucional.

c. Todos los programas instalados en los equipos de cómputo propiedad de la CNE deben haber sido autorizados previamente por la UTI, la cual llevará un registro formal de los mismos.

d. Los usuarios no podrán copiar ni traspasar a terceros, licencias de software o desarrollos realizados por y para la CNE.

e. La UTI podrá utilizar herramientas para la elaboración de inventarios remotos del software instalado en los equipos de la CNE, para detectar y eliminar cualquier programa no autorizado.

f. Para acceder a la información almacenada en las computadoras de uso de los funcionarios, la UTI procederá de acuerdo con lo establecido por la normativa legal vigente.

g. Si por motivos de trabajo un funcionario requiere que se le instale algún programa particular no propiedad de la CNE, se aplicará el procedimiento definido por la UTI para estas situaciones y disponible en la intranet.

4.3 Servidores institucionales

a) Los servidores y las estaciones de trabajo se deben ubicar en redes independientes entre sí y la comunicación entre ellos debe controlarla un componente con funciones de seguridad incorporadas.

b) Las contraseñas de los servidores institucionales y cualquier otro equipo que lo requiera, deben ser registradas y almacenadas por la UTI en un dispositivo de acceso restringido bajo llave, al cual tendrá acceso en caso de ser necesario, el jefe de la Unidad de Tecnologías de Información, o en su ausencia, el Director Ejecutivo de la CNE o quien éste designe.

c) Se prohíbe el uso de los protocolos TELNET y FTP, salvo en los casos en que se amerite, previa autorización por parte de la jefatura de la UTI.

d) Cualquier servicio, puerto o aplicación no utilizados en la plataforma tecnológica en producción, debe ser deshabilitado por el responsable técnico respectivo.

e) Ningún servidor con una dirección IP privada bajo el protocolo IPv4 debe estar accesible directamente desde Internet.

f) Por ninguna circunstancia un usuario debe, sin autorización expresa de la UTI, utilizar el equipo a cargo como servidor de servicios adicionales (FTP, Telnet, WWW, carpetas compartidas o servidor de Chat).

g) La UTI será la responsable de la coordinación con el proveedor de servicios de Internet (I.S.P., Internet Service Provider) o con la autoridad latinoamericana de asignación de direcciones (LACNIC), para la solicitud de direcciones IP públicas.

h) La UTI es la responsable de la coordinación con la autoridad encargada de administrar y proveer nombres de dominio a nivel nacional (NIC Costa Rica), para cualquier aspecto relacionado con el dominio de la CNE y sus derivados (subdominios).

i) Todos los servidores institucionales ubicados en las instalaciones físicas de la CNE, deben estar en zonas de acceso físico restringido, manteniendo control y registro de quienes ingresan y/o los acceden.

j) Todos los cuartos de comunicaciones o lugares donde se almacenen datos electrónicos sensibles deberán contar con un control de acceso físico restringido, manteniendo control y registro de quienes ingresan y/o los acceden.

4.4 Control ambiental del centro de cómputo

a) Con relación al centro de cómputo, la UTI coordinará con la Unidad de Servicios Generales (en adelante la USG) la implementación de los controles de acceso, las instalaciones eléctricas, UPS[4], las condiciones ambientales, las alarmas y dispositivos contra incendio, necesarios para garantizar su integridad. Igualmente coordinará lo que corresponda para los cuartos de comunicaciones (espacios destinados para ubicar los equipos de comunicaciones de la red de voz y datos institucional).

b) Además, la USG es la responsable del monitoreo y correcta operación del(los) aire(s) acondicionado(s) y de los dispositivos para extinción de incendios (en conjunto con el encargado del área de salud ocupacional) en el centro de cómputo, conforme a los procedimientos que se establezcan para tales efectos.

4.5 Acerca de la infraestructura física

a) Toda obra civil que afecte directamente la red de datos institucional (intervención del cableado estructurado: modificación, instalación, traslado, eliminación de puntos de red, etc.) deberá ser coordinada anticipadamente con la UTI, con el fin de evaluar su impacto, determinar las implicaciones y/o definir los requerimientos.

4.6 Acceso a las redes Institucionales

a) Solamente en situaciones calificadas, a solicitud de la jefatura respectiva y con la autorización y coordinación de la UTI, se permitirá conectar a la red institucional un equipo que no pertenezca a la CNE. Para estos casos la UTI deberá llevar un registro del equipo y garantizar que cumpla con las políticas de seguridad tecnológica establecidas institucionalmente. En caso de ser necesario, la UTI tiene la potestad de realizar la conexión de estos equipos en una red separada del resto de la plataforma y controlada en forma independiente por el firewall Institucional.

[4] UPS: del inglés “Uninterruptible Power Supply” cuyo significado en español es “Sistema de Alimentación ininterrumpida.

b) Los equipos que se encuentren conectados a la red institucional, permanentemente o en forma temporal, deben contar, cuando aplique, con el programa antivirus y con un firewall personal debidamente instalado. Cualquier anomalía reportada por estos programas debe notificarse de inmediato a la UTI, para las acciones correspondientes.

c) El uso compartido de carpetas o dispositivos de almacenamiento bajo el sistema operativo Windows incrementa las posibilidades de que se presenten contagios masivos de virus a nivel Institucional. Utilizar estos mecanismos para compartir información institucional es responsabilidad de los usuarios. Se recomienda recurrir a las herramientas disponibles a través de la Plataforma de Gestión Documental (SharePoint) o los servicios de almacenamiento que se brindan en la nube como OneDrive o Nextcloud.

d) La UTI implementará los procedimientos o tecnología necesaria para validar la integridad de aquellos equipos que se conecten a las redes de datos institucionales, considerando, cuando el equipo lo permita, al menos la presencia de un antivirus debidamente actualizado.

4.7 Conexiones inalámbricas internas

a) La UTI administrará las conexiones inalámbricas establecidas a nivel institucional y podrá delegar, utilizando mecanismos seguros, la opción de otorgar acceso a secciones de la red inalámbrica institucional.

b) Las conexiones de tipo WLAN (Wireless LAN o red LAN inalámbrica) serán tratadas bajo los esquemas de seguridad y conectividad establecidos por la UTI.

c) Solamente con autorización de la UTI se podrán poner en operación equipos de acceso del tipo “ACCESS POINT” dentro de las instalaciones de la CNE, sean estos conectados a la red institucional o no.

d) El acceso a la red Invitados-CNE será restringido y de uso exclusivo para fines laborales.

e) El mecanismo de acceso a la red de Invitados-CNE será el que la UTI, con la aprobación de la Dirección Ejecutiva y/o Presidencia Ejecutiva de la CNE determine: uso de tiquetes, excepciones por direccionamiento físico, etc. y deberá ser solicitado por la jefatura y/o Dirección correspondiente mediante correo electrónico u oficio dirigido a la Unidad de Tecnologías de Información. La UTI se reserva el derecho de elevar la aprobación de las solicitudes a la Dirección Ejecutiva y/o Presidencia Ejecutiva.

CAPÍTULO 5: SOBRE EL USO DE INTERNET, CORREO ELECTRÓNICO Y HERRAMIENTAS COLABORATIVAS

5.1 Servicios de acceso a Internet.

a. La UTI es la responsable de la administración de los servicios de acceso a Internet de la CNE.

b. La UTI debe dar seguimiento al uso que se dé al servicio de acceso a Internet. Ante una solicitud formal de una jefatura, se emitirán informes de los sitios visitados por los funcionarios a su cargo, así como el tiempo de navegación reportado por la herramienta de monitoreo y de acuerdo con la disponibilidad de almacenamiento de esta información.

c. La UTI implementará los mecanismos necesarios para bloquear los accesos no permitidos a la Internet o que pongan en riesgo la seguridad de los recursos TIC.

d. La UTI administrará el ancho de banda asignado a los diferentes protocolos o aplicaciones que se accedan en la Internet, con el fin de garantizar un tiempo de respuesta aceptable para clientes internos o externos.

e. Todos los accesos desde sitios externos a cualquiera de los servicios que la CNE ponga a disposición de los usuarios, deben estar controlados por el sistema de seguridad institucional.

5.2 Accesos alternos desde la CNE hacia Internet.

a. Salvo excepciones autorizadas por la UTI, no se permitirá que ningún equipo se conecte desde la Comisión a otra red externa, utilizando cualquier dispositivo no autorizado de comunicación (datacard, módems, access point) que así lo permita.

b. Por ninguna circunstancia un equipo conectado a la red de la CNE podrá estar conectado, a la misma vez, a una red externa no autorizada.

c. Cuando se requiera de un acceso conmutado o de banda ancha a Internet, desde puntos externos a la CNE, la UTI gestionará el servicio en coordinación con el proceso de comunicaciones. La administración de la cuenta es responsabilidad de la unidad o funcionario solicitante y su uso es exclusivamente para asuntos laborales.

5.3 Uso del correo electrónico

a. El servicio de correo electrónico institucional es el medio de comunicación electrónico oficial de la CNE y está destinado a satisfacer el cometido público que corresponde a la Comisión y las necesidades de comunicación electrónica de los funcionarios, por lo cual, no debe ser utilizado para el registro en redes sociales, para la recepción de información personal o para uso en foros que no tienen que ver con el quehacer institucional, es decir, su uso es estrictamente para fines laborales.

b. A solicitud de la jefatura inmediata y previa oficialización del nombramiento por parte de la Unidad de la Unidad de Desarrollo Humano, la UTI asignará una cuenta de correo electrónico para uso exclusivo de los funcionarios de la CNE, y la mantendrá activa en tanto se encuentren laborando en la Institución. Una vez que se pierda esta condición de funcionario de la CNE, la Unidad de Desarrollo Humano informará a la UTI, la cual procederá a desactivar la cuenta y a partir de ese momento el servidor de correo empezará a emitir alertas de imposibilidad de entrega de un correo a dicha cuenta. Con la desactivación de la cuenta se eliminan todos los correos que al momento tenga almacenados, sin que exista posibilidad de recuperarlos ni responsabilidad alguna para la custodia de los mismos, por la Unidad de Tecnologías de Información.

c. La información contenida en los buzones de correo electrónico de cada funcionario es privada y pertenece al usuario titular de la cuenta. Toda comunicación emitida o recibida por un funcionario desde la cuenta de correo electrónico es de su responsabilidad. Este deberá velar por no comprometer la imagen ni la credibilidad de la CNE con las comunicaciones que realice.

d. Todo colaborador deberá utilizar una fotografía asociada a su perfil de correo electrónico que permita identificarlo como funcionario de la CNE, cumpliendo con los esquemas de presentación personal y de vestimenta dispuestos en la normativa interna de la Institución, libro de marca, o disposiciones que al respecto emita la Unidad de Desarrollo Humano.

e. La UTI deberá disponer de la tecnología apropiada para que los mensajes entre usuarios internos cuenten con autenticidad, integridad y seguridad.

f. Cuando un funcionario no se encuentre laborando por más de dos días hábiles consecutivos (sea por vacaciones, incapacidad, permisos, etc.), deberá programar en su correo electrónico un mensaje de respuesta automática indicando que no se encuentra laborando, e incluyendo en el mensaje la fecha en que regresa.

g. Se entenderá como correo masivo aquél que sea enviado de forma general o impersonal a un grupo de cuentas. En tales casos, los destinatarios de los correos y/o el nombre del grupo al que se envían, se deben incluir en el campo CCO (Con Copia Oculta) del mensaje de correo, esto con el fin de que no se den respuestas masivas a estos correos electrónicos y como medida de protección de las direcciones de correo.

h. El envío de correos masivos al grupo de cuentas "funcionarios" sólo será permitido a aquellos usuarios que la UTI autorice, previa valoración del caso y con el V°B° del Director(a) de área, de la Dirección Ejecutiva y/o de la Presidencia Ejecutiva.

i. En el caso de que algún funcionario no autorizado desee enviar un correo al grupo funcionarios, deberá gestionarlo ante la UTI, previa autorización, del Director(a) de área, de la Dirección Ejecutiva y/o de la Presidencia Ejecutiva. La UTI procederá a realizar el envío a través de la cuenta denominada "Comunicados".

j. La UTI podrá implementar cuentas de correo impersonales (por ejemplo primerosimpactos@cne.go.cr) dependiendo de la conveniencia institucional, previa valoración del caso y con la autorización del correspondiente Director(a) de área, Dirección Ejecutiva y/o de la Presidencia Ejecutiva. La gestión de estas cuentas será responsabilidad de quien la solicita. De no autorizarse una cuenta impersonal la UTI podrá crear direcciones de correo que operen hacia un grupo de cuentas (grupos de distribución), de manera tal que dicho grupo reciba o envíe mensajes utilizando la dirección de correo asignada. Para la atención de estos casos él o los interesados deberán plantear una solicitud formal ante la jefatura de la UTI, con el V°B° del superior inmediato.

k. La información contenida en los buzones de correo de los funcionarios será responsabilidad del titular.

l. Cada funcionario dispondrá de un máximo de 5GB de almacenamiento en su correo electrónico. Con el fin de evitar problemas con el envío y/o recepción de correo al llenarse el buzón, se recomienda utilizar archivos del tipo ".pst". Para esto podrá revisar el procedimiento disponible en la intranet o solicitar el apoyo directamente a la UTI.

5.4 Uso de herramientas colaborativas

a. Las herramientas colaborativas básicas asociadas a la cuenta de correo electrónico que se asignan a cada funcionario incluyen: una herramienta para el manejo de calendarios, colaboración y gestión documental (SharePoint), un espacio de almacenamiento en la nube para la gestión de documentos con sus aplicaciones de ofimática (OneDrive y Office Online),

una herramienta de mensajería instantánea (Skype Empresarial y Teams) y un perfil de red social (Yammer).
Debido a que todas estas herramientas están asociadas a la cuenta de correo, éstas también son desactivadas al momento que una persona pierde la condición de funcionario de la CNE.

b. El personal de la CNE deberá utilizar sólo las herramientas colaborativas aprobadas institucionalmente (de uso local o en la nube), conforme a lo que para tales efectos disponga la UTI.

c. Para utilizar alguna herramienta colaborativa, de uso local o en la nube, distinta a las aprobadas institucionalmente, el funcionario deberá plantear la solicitud a la jefatura de la UTI, debidamente avalada por el nivel de jefatura que corresponda, indicando el uso que se dará a la herramienta y la justificación de por qué se requiere. La UTI, una vez que valore la solicitud, aprobará o no el uso de la herramienta para el funcionario que la pidió, y de aprobarla será por un tiempo limitado.

d. Los espacios de almacenamiento dispuestos en servidores de la CNE o en la nube, deberán ser utilizados exclusivamente para archivos relacionados con las labores que le son encomendadas al funcionario. Cuando la persona deje de ser funcionario de la CNE, deberá proceder de previo a trasladar todos los archivos de interés institucional a su superior inmediato, quien tendrá que velar por el cumplimiento de esta disposición.

e. Las comunicaciones que sean realizadas mediante la herramienta de mensajería instantánea son privadas y pertenecen al usuario titular de la cuenta. Al momento de desactivar la cuenta, los registros de dichas comunicaciones serán eliminados automáticamente.

f. Los registros contenidos en la herramienta de calendario pertenecen al usuario titular de la cuenta y al momento de desactivarla, dichos registros serán eliminados automáticamente.

h. El uso de sitios web colaborativos deberá hacerse en apoyo a las labores que se realizan en la institución y no con fines personales.

5.5 Plataforma de Gestión Documental

a. La UTI pondrá a disposición de cada Dirección, Unidad o Proceso un sitio en la plataforma de gestión documental Microsoft SharePoint, donde deberán almacenar y registrar todos los documentos y demás información, en formato electrónico, que surjan como parte de la gestión institucional.

b. Las jefaturas y/o encargados de procesos serán los responsables de definir y/o designar a los administradores de los sitios en SharePoint (máximo 2 por unidad o proceso), quienes tendrán a cargo la gestión de los documentos: crear bibliotecas y listas, así como otorgar o denegar accesos a los usuarios.

c. La Unidad de Tecnologías de Información impartirá talleres de actualización, presenciales o a través de la plataforma virtual, a los nuevos funcionarios y/o a los administradores de sitio, previa coordinación con la Unidad de Desarrollo Humano (Área de Capacitación) y según los requerimientos y necesidades institucionales.

CAPÍTULO 6: DESARROLLO DE PROYECTOS DE TIC.

a. Todo desarrollo de Proyectos de TIC debe ser realizado en coordinación con la UTI.

b. Todo desarrollo de proyectos de TIC debe cumplir con las directrices que para estos efectos emita la Unidad de Tecnologías de Información. Estas directrices deben ser revisadas y actualizadas periódicamente por la UTI.

c. Todo desarrollo de proyectos de TIC que se realice para la CNE debe estar alineado con el Plan Estratégico de Tecnologías de Información, Plan Estratégico Institucional, Plan Anual Operativo y al Plan de Compras aprobado y vigente.

CAPÍTULO 7: GESTIÓN DE LA INFORMACIÓN INSTITUCIONAL.

7.1 Gestión responsable de la información institucional

a. La gestión de la información es responsabilidad de todo funcionario de la CNE, por lo que criterios como la calidad y oportunidad de la información deberán ser tomados en consideración por todo el personal, de manera que coadyuven a contar con información confiable que sustente la toma de decisiones.

b. Todos los funcionarios deben hacer un uso correcto de la información que por sus funciones tienen a disposición, sin sacar provecho personal del acceso que se tenga y velando por la protección de la información que esté bajo su responsabilidad directa o sobre la cual tengan acceso.

c. El personal de la CNE deberá valorar la información como un activo institucional, por lo cual deberá custodiarla apropiadamente y protegerla contra usos no autorizados o malintencionados.

d. Todo colaborador deberá mantener absoluta confidencialidad para toda aquella información catalogada como sensible, en atención a la normativa aplicable, y sobre la cual se tenga acceso, de manera directa o indirecta, en el ejercicio de las labores encomendadas como funcionario de la CNE.

7.2 Uso de Certificados de Firma Digital

a. La CNE podrá utilizar la firma digital certificada para todos los documentos electrónicos que emita oficialmente, tanto para la correspondencia interna como externa. Dichos certificados deberán operar al amparo de la Ley No. 8454 Ley de Certificados, Firmas Digitales y Documentos Electrónicos y de su Reglamento.

b. La CNE aplicará la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, emitida por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Dicha política establece el conjunto de reglas generales para el procesamiento de documentos electrónicos firmados digitalmente, tanto para la realización de la firma digital como para la verificación de su validez en cualquier momento en el tiempo.

c. La CNE entregará certificados de firma digital a aquellos funcionarios que requieran firmar documentos electrónicos internos o externos, o cuando el funcionario lo requiera para autenticarse y ejecutar acciones en un sistema automatizado. Para dichos certificados se mantendrá la actualización en tanto la persona tenga la condición de funcionario activo de la CNE.

d. En el caso de los certificados de firma digital que la CNE adquiera y entregue a sus funcionarios, se entiende que el dispositivo seguro (tarjeta inteligente) pasa a formar parte del patrimonio del funcionario y puede ser, por tanto, utilizado también en actuaciones que realice a título personal. En el caso de que el funcionario reciba un dispositivo lector externo de tarjetas inteligentes, éste le pertenece a la CNE y el funcionario deberá devolverlo junto con su equipo de cómputo, cuando deje de ser funcionario activo de la Institución.

e. El funcionario que reciba un certificado de firma digital asume la total responsabilidad sobre las actuaciones que sean realizadas con dicho dispositivo. Lo anterior conforme a Ley No. 8454 Ley de Certificados, Firmas Digitales y Documentos Electrónicos y de su Reglamento.

f. Le corresponderá a las jefaturas de cada unidad indicar de manera justificada a la Unidad de Proveeduría Institucional, la necesidad de entregar o renovar certificados de firma digital a funcionarios de su dependencia, entendiendo que éstos requieren dicho dispositivo para realizar firma de documentos electrónicos oficiales o autenticarse en un sistema automatizado.

g. La Unidad de Proveeduría Institucional gestionará conforme a la disponibilidad presupuestaria, la adquisición y renovación de los certificados de firma digitales que utilizarán los funcionarios en el ejercicio de las labores que les son encomendadas.

h. La Unidad de Proveeduría Institucional mantendrá un registro actualizado de los funcionarios que cuentan con un certificado de firma digital en el cual se lleve control de las fechas de vigencia de estos.

i. El funcionario que recibe un certificado de firma digital por parte de la CNE, deberá responsabilizarse por el cuidado del dispositivo y en caso de pérdida, robo o daño de éste, deberá reponerlo por su propia cuenta, reportando a la Unidad de Proveeduría Institucional dicha situación para que se proceda a corregir el registro de vigencia del certificado de esa persona. Esto igualmente aplica en los casos en que el funcionario olvide la clave de uso del certificado (PIN) y deba obtener un nuevo certificado.

7.3 Manejo de las unidades de almacenamiento.

a. En la estación de trabajo asignada al funcionario, éste podrá crear dentro de la carpeta de Windows llamada DOCUMENTOS, una carpeta llamada PERSONAL, bajo la cual organizará toda aquella información de índole personal que tenga en su equipo. La gestión de esta carpeta es responsabilidad del usuario.

b. Todo dispositivo electrónico de almacenamiento externo (discos duros, unidades magnéticas, unidades usb, grabadoras, etc.) deberá ser debidamente custodiado por el funcionario que lo tenga asignado y será responsable de evitar el acceso indebido a la información que contenga.

c. Cuando proceda, la UTI implementará mecanismos para bloquear la conexión de dispositivos de almacenamiento externo (discos duros, unidades usb, etc.) a las estaciones de trabajo de los funcionarios.

d. Cuando un funcionario tenga asignado un equipo o dispositivo electrónico que almacene datos institucionales (computadoras, discos duros externos, unidades usb, grabadoras, etc.), y deje de utilizarlo (sea que lo devuelva a la UTI o lo traslade a otro funcionario), deberá borrar toda la información institucional que contenga en ese momento. En caso de requerir apoyo de la UTI, deberá solicitarlo en el momento que haga la devolución o el traslado del dispositivo.

e. La UTI, en coordinación con el(la) encargado(a) de activos, deberá garantizar la eliminación oportuna de la información institucional que contengan cualquier equipo o dispositivo electrónico, que vaya a ser desechado o sujeto de donación a otra institución. La UTI, en coordinación con el(la) encargado(a) de activos, deberá garantizar la eliminación oportuna de la información institucional que contenga(n) el(los) equipo(s) o dispositivo(s) electrónico(s), que vaya(n) a ser desechado(s) o sujeto(s) de donación.

7.4 Respaldo y recuperación de la información

a. Los responsables de los servicios que se ejecuten en los servidores institucionales deben realizar pruebas periódicas para verificar la funcionalidad de los respaldos. La periodicidad de estas pruebas se definirá en coordinación con la jefatura de la UTI.

b. Cada funcionario es el responsable del mantenimiento, custodia y respaldo de la información que mantiene en su estación de trabajo o en el espacio de almacenamiento en la nube que le sea asignado.

7.5 Bases de Datos

a. La administración de las bases de datos institucionales es responsabilidad de la UTI.

b. La información contenida en las bases de datos institucionales no puede ser transferida sin previa autorización por parte del administrador del sistema.

c. La UTI debe velar por la custodia, disponibilidad, integridad y acceso controlado de los datos.

d. El sistema administrador de bases de datos institucional debe tener la posibilidad de generar pistas de auditoría, de acuerdo con los requerimientos de los usuarios.

7.6 Publicación de información institucional.

a. La Unidad de Comunicación Institucional será la encargada de dictar los lineamientos institucionales para emitir criterios o publicar información en representación de la CNE: en sitio web, redes sociales, foros, blogs, o cualquier medio de comunicación electrónico.

b. La publicación de información institucional en el sitio web oficial de la CNE, deberá hacerse conforme a los lineamientos establecidos por la Unidad de Comunicación Institucional.

c. Cuando una Unidad o Dirección requiera colocar un fondo de pantalla alusivo a una campaña de concientización o algún tema de su interés, deberá solicitar la autorización a la Dirección Ejecutiva o Presidencia Ejecutiva. La imagen deberá ser proporcionada por el solicitante, cumpliendo con las siguientes características técnicas:

- Tamaño: 1920 x 1080 pixeles
- Formato: bmp o png
- La imagen debe ser de buena calidad para una mejor experiencia de usuario

La UTI podrá determinar las regulaciones adicionales y las herramientas que estime necesarias para la implementación de estas Directrices.

Estas Directrices entrarán a regir a partir de su comunicación.

Firmado digitalmente por GUSTAVO ADOLFO SANCHEZ COTO (FIRMA)
Fecha: 2019.07.16 14:47:14 -06'00'

Jefatura Unidad de Tecnologías de Información **V°B° Directora Ejecutiva**

GLOSARIO

ACCESS POINT: dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red.

ADWARE: programas que alteran el sistema instalando propaganda o enlaces maliciosos.

ANCHO DE BANDA: cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

ANTIVIRUS: programa que detecta y elimina virus informáticos

CIFRAR: aumentar la seguridad de un archivo mediante la codificación del contenido.

CNE: Comisión Nacional de Prevención de Riesgos y Atención de Emergencias.

DIRECCION IP: etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de red.

ENCRIPTAR: Ocultar o codificar información.

ESTACION DE TRABAJO: equipo(s) de cómputo (portátil o de escritorio) asignado(s) a un colaborador para la ejecución de sus tareas diarias.

FIRMA DIGITAL: mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje, y confirmar su autenticidad.

FIREWALL: elemento de red diseñado para bloquear accesos no autorizados.

FTP: protocolo para la transferencia de archivos.

GUSANO: programa malicioso que tiene la posibilidad de duplicarse y distribuirse por medio del almacenamiento.

IPv4: protocolo de IP versión 4.

LAN: red de área local.

NEXTCLOUD: Servicio privado de alojamiento de archivos en la nube.

ONEDRIVE: Servicio de alojamiento de archivos en la nube.

RANSOMWARE: virus que restringe el acceso de los datos y pide un “rescate” para quitar dicha restricción.

SERVIDOR: Equipo informático encargado de recibir solicitudes, procesarlas y devolver un resultado

SHAREPOINT: Plataforma colaborativa para la gestión documental

TELNET: protocolo de red que permite conectarse a otro equipo

TIC: Tecnologías de Información y Comunicaciones.

TROYANO: programa usado para robar información o alterar el sistema para su control externo.

USG: Unidad de Servicios Generales

UTI: Unidad de Tecnologías de Información

WLAN: red de área local inalámbrica