Nº 006-2015-HCH/DG

MINISTERIO DE SALUD
INSTITUTO DE GESTION DE SERVICIOS DE SALUD
HOSPITAL CAYETANO HEREDIA

REPÚBLICA DEL PERÚ

RESOLUCIÓN DIRECTORAL

Lima, 16 de enero de 2015

Visto el Memorando Nº 435 - 2014-II-OEI/HNCH, con el informe Nº 042-OEI-UI-2014-HNCH, de la Unidad de Informática, con el proyecto de la Directiva Administrativa Nº 001-2015-OEI-UI-HCH-V.01 "Mejores Prácticas para la Gestión de Recursos y Servicios de Tecnologías de Información y Comunicaciones - TIC´s" del Hospital Cayetano Heredia;

CONSIDERANDO:

Que, con el Memorando Nº 435 – 2014-II-OEI/HNCH, el Jefe de la Oficina de Estadística e informática remite el informe Nº 042-OEI-UI-2014-HNCH, de la Unidad de Informática, con el proyecto de la Directiva Administrativa Nº 001-2015-OEI-UI-HCH-V.01 "Mejores Prácticas para la Gestión de Recursos y Servicios de Tecnologías de Información y Comunicaciones - TIC´s", solicitando su aprobación mediante Resolución Directoral;

Que, mediante el Decreto Supremo Nº 024-2005-PCM se aprobó el Reglamento de la Ley 28612 Ley que norma el uso, adquisición y adecuación del software en el Administración Pública, tiene por objeto establecer las medidas que permitan a la Administración Pública la contratación de licencias de software y servicios informáticos en condiciones de neutralidad, vigencia tecnológica, libre concurrencia y trato justo e igualitario de proveedores;

Que, la Ley Nº 27269 Ley de firmas y Certificados digitales fue reglamentado mediante el Decreto Supremo Nº 019-2002-JUS, la presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.;

Que, la Ley Nº 30096 Ley de delitos Informáticos modificado por la Ley 30171, La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia;

Que, mediante Resolución Ministerial Nº 526-2011/MINSA, del 11 de julio, se aprobó las Norma para la Elaboración de Documentos Normativos del Ministerio de Salud, la cual tiene como objetivo establecer disposiciones relacionadas con los procesos de planificación, formulación o actualización, aprobación, difusión, implementación y evaluación de los documentos Normativos, así como estandarizar los elementos conceptuales, estructurales y metodológicos más relevantes, del mismo modo como, establecer la aplicación de procesos transparentes y explícitos para la emisión de los documentos normativos, también para brindar a las instancias reguladoras del Ministerio de Salud una herramienta que facilite el desarrollo de las funciones normativas;

Que, el Literal f) del artículo 3º del Reglamento de Organización y Funciones del Hospital Nacional Cayetano Heredia, aprobado con Resolución Ministerial N° 216-2007/MINSA, establece como una de las funciones generales del Hospital mejorar continuamente la calidad, productividad, eficiencia y eficacia de la atención a la salud, estableciendo las normas y los parámetros necesarios, así como generando una cultura organizacional con valores y actitudes hacia la satisfacción de las necesidades y expectativas del paciente y su entorno familiar;

16 ENE 2015
3766

Que, atendiendo a los fundamentos expuestos, resulta necesario aprobar la Directiva Administrativa de Informática denominada "Mejores Prácticas para la Gestión de Recursos y Servicios de Tecnologías de información y Comunicaciones - TIC´s" del Hospital Cayetano Heredia, para lo cual debe expedirse el proyecto de la Resolución Directoral correspondiente;

Estando a lo solicitado por el Jefe de la oficina Estadística e Informática y a lo informado por la Oficina de Asesoría Jurídica mediante Informe Nº 28-2015-OAJ-HCH, para que se apruebe la Directiva Administrativa Propuesta;

Con las visaciones de los Jefes de las Oficinas de Estadística e Informática y Asesoría Jurídica; y,

De conformidad con las facultades previstas en el Reglamento de Organización y Funciones del Hospital Nacional Cayetano Heredia, aprobado por Resolución Ministerial N° 216-2007/MINSA;

SE RESUELVE:

Artículo Primero.- Aprobar la Directiva Administrativa Nº 001-2015-OEI-UI-HCH-V.01, "Mejores Prácticas para la Gestión de Recursos y Servicios de Tecnologías de Información y Comunicaciones - TIC´s" del Hospital Cayetano Heredia, el cual se adjunta con sus anexos y forman parte de la presente Resolución.

Artículo Segundo.- Encargar a la Unidad de Informática el seguimiento, evaluación y aplicación de la presente Directiva Administrativa en el Hospital Cayetano Heredia.

Artículo Tercero.- Disponer que la Jefa de la Oficina de Comunicaciones efectúe la publicación de la presente Resolución en la página web del Hospital.

Regístrese y Comuníquese.

MINISTERIO DE SALUD
INSTITUTO DE GESTIÓN DE SERVICIOS DE SALUD
HOSPITAL CAYETANO HEREDIA
DR. LUIS EDGARDO DULANTO MONTEVERDE
DIRECTOR GENERAL
C.M.P. 14270

16 ENE 2015

LED/MRC/GV/PDRG/pdrg
OEI
OAJ
OCOM

Directiva Administrativa N° 001-2015-OEI-UI-HCH: V.01

Mejores Prácticas para la Gestión de Recursos y Servicios de Tecnologías de Información y Comunicaciones – TIC´s

1. OBJETIVO

Establecer los procedimientos, disposiciones y responsabilidades para regular la administración, control, utilización además de la seguridad de los Recursos y Servicios de Tecnologías de Información y Comunicaciones en el Hospital Cayetano Heredia (en adelante HCH).

2. FINALIDAD

Normar los procedimientos para la administración, control, utilización demás de la seguridad de los Recursos y Servicios de Tecnologías de Información y Comunicaciones, optimizando y garantizando su correcta aplicación en el desarrollo de las funciones de las direcciones, oficinas, departamentos así como los servicios del HCH a nivel interno y externo.

3. BASE LEGAL

- Ley N° 27657 Ley Del Ministerio De Salud
- Ley Nº 27658 Ley Marco De Modernización De La Gestión Del Estado
- Decreto Legislativo Nº 604 - Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Decreto Supremo Nº 043-2001-PCM - Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Decreto Supremo N°067-2003-PCM: Aprueban Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N°066-2003-PCM: Fusionan la Sub jefatura de Informática del Instituto Nacional de Estadística e Informática - INEI y la Presidencia del Consejo de Ministros, a través de su Secretaría de Gestión Pública
- Decreto Supremo N°081-2013-PCM: Mediante el cual se Aprueba la Política Nacional de Gobierno Electrónico 2013-2017
- Resolución Ministerial N°246-2007-PCM Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI.
- Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición"
- Resolución Ministerial N° 216-2007/MINSA Aprueba el Reglamento de Organización y Funciones del Hospital Cayetano Heredia.
- Resolución Directoral Nº 089-2009-SA-HNCH/DG Aprueban el Manual de Organización y Funciones de la Oficina de Estadística e Informática del HCH
- Ley Nº 27444 - Ley del Procedimiento Administrativo General.

HOSPITAL NACIONAL CAYETANO HEREDIA

HOSPITAL NACIONAL CAYETANO HEREDIA V° B° UNIDAD DE INFORMÁTICA

- Ley Nº 27269 - Ley de Firmas y Certificados Digitales.
- Decreto Supremo N°019-2002-JUS - Reglamento de la Ley de Firmas y Certificados Digitales.
- Ley N°28612 Ley que Norma el uso, Adquisición y Adecuación del Software en la Administración Pública.
- Decreto Supremo N°024-2005-PCM Aprueba el Reglamento de la Ley N°28612.
- Resolución Ministerial N°139-2004-PCM Aprueban "Guía Técnica sobre Evaluación de Software para la Administración Pública"
- Ley N°30096 Ley de Delitos Informáticos.
- Ley N°30171 Ley que modifica la Ley N°30096, Ley de Delitos Informáticos.

4. ALCANCE

La presente Directiva es de cumplimiento obligatorio para todos los servidores y funcionarios del Hospital Cayetano Heredia, así como para el personal contratado que presta servicios o desempeñe actividades (independientemente del régimen laboral al que se encuentra sujeto).

5. DEFINICIONES

5.1. Tecnologías de la Información: Conjunto de recursos y servicios desarrollados para gestionar información.

5.2. Infraestructura Tecnológica: Conjunto de elementos de Hardware, Software y comunicaciones que soportan los servicios informáticos.

5.3. Recursos Informáticos: Bienes tangibles (Equipos) y lógicos (Carpetas) que permiten el acceso o distribución de la información.

5.4. Servicios Informáticos: Servicios brindados a través del uso de la Infraestructura Tecnológica que permiten la gestión de información, asistencia y soporte a los Usuarios.

5.5. Software Propietario: Software de Código Cerrado cuya licencia no permite su modificación y/o redistribución.

5.6. Software Libre: Software de Código Abierto cuya licencia permite su uso irrestricto, modificación y/o redistribución libre.

5.7. Sistema Operativo: Software de base que permite al Usuario interactuar con el hardware o equipo de cómputo.

5.8. Aplicativos: Son software propietarios o libres que aplican a una solución o uso en particular. (Herramientas de Ofimática, Navegadores, etc.)

5.9. Sistemas Informáticos: Son los sistemas desarrollados o cedidos en uso a través de los cuales se gestiona la información.

5.10. Usuario: Toda persona que hace uso de los recursos informáticos.

5.11. Cuenta de Usuario: Permite identificar al trabajador por medio de una identidad en el dominio institucional, le permite acceder a la red de domino y asignarle los permisos y/o accesos a los recursos y servicios informáticos.

5.12. Cuenta de Correo: Es la cuenta de correo electrónico institucional asignada a la Cuenta de Usuario para intercambio de información o mensajes dentro o fuera de la institución.

5.13. Riesgos: Combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.

5.14. Amenazas: Actividad del Usuario o condición peligrosa que puede ocasionar incidencias o eventos sobre los recursos o servicios informáticos. La amenaza se determina en función de la intensidad y la frecuencia de incidentes o eventos.

5.15. Vulnerabilidades: Son las características y las circunstancias de un sistema o equipo que los hacen susceptibles a los efectos de una amenaza.

5.16. Permisos: Los permisos son reglas asociadas a los objetos de un equipo o red, como archivos y carpetas. Determinan si se puede obtener acceso a un recurso u objeto y lo que se puede hacer con él.

5.17. Accesos: Se obtiene a través de los permisos para trabajar con recursos u objetos.

5.18. Reproducción: Acción de copiar archivos o información con la finalidad de editarla, reutilizarla o distribuirla.

5.19. Copia: Acción de copiar un archivo o información.

5.20. Descarga: Todo acción de bajar archivos o información a través del uso del internet.

5.21. Carga de archivos: Toda acción de subida de archivos a través del uso del internet.

5.22. Respaldo: Copia de archivos o información con la finalidad de protegerlos y mantener operativos los recursos o servicios.

5.23. Evaluación: Acciones de análisis de

5.24. Asignación: La evaluación es la determinación del valor en función de criterios basados en un conjunto de normas.

5.25. Red de datos: Conjunto de elementos que permiten la interconectividad entre equipos a través de una interface de enlace.

5.26. Dominio: Es el ámbito de confianza dentro del cual los equipos de cómputo, identidades y objetos son administrados a través de cuentas de usuario a las cuales se les asignan permisos y privilegios.

5.27. Soporte: Actividad de Asistencia de los servicios informáticos.

5.28. Puertos: Todo punto de acceso a través del cual se pueden conectar dispositivos y/o accesorios a una computadora. (USB, RJ45, Serial, Paralelo, etc.)

5.29. Periféricos: Dispositivos complementarios de una Computadora. (Teclado, Mouse, Monitor, Parlantes, Etc.)

5.30. Dispositivos Externos: Dispositivos que se conectan a través de los puertos de un equipo de cómputo.

6. DISPOSICIONES GENERALES

6.1. RED DE SERVICIOS DE TECNOLOGIAS DE LA INFORMACION

En concordancia con sus fines misionales y lo previsto en su plan estratégico. El HCH, reconoce y valora la información como un activo de importante valor para la organización, cuyo adecuado tratamiento requiere, entre otros, de una red o conjunto de servicios de soporte tecnológico para garantizar, de manera integral, estructurada y eficaz, su utilización,

interconectividad y control apropiados, independientemente de la forma escrita, electrónica u otra que adopte, previniendo riesgos de amenazas y vulnerabilidades.
En tal sentido, conforme a sus atribuciones y disponibilidad respectiva, El HCH proporciona Recursos y Servicios de Tecnologías de Información y Comunicaciones – TIC´s (Computadoras, internet, correo electrónico y sistemas informáticos) a sus usuarios, que le pueda ser útil para el mejor desempeño de sus labores.

6.2. SUJECION A POLITICAS Y NORMAS DE APLICACION

El suministro, utilización, interconectividad y control de los Recursos y Servicios de Tecnologías de Información y Comunicaciones – TIC´s (Computadoras, internet, correo electrónico y sistemas informáticos), así como cuando se asignen para uso de otros órganos del Sistema Nacional de Salud (en adelante SNS), debe sujetarse a las políticas y normas institucionales aprobadas sobre protección o salvaguarda de activos, seguridad de la información, control de accesos y otras aplicables al uso de sistemas o tecnologías de la información y comunicación, así como a la normativa de control interno aplicable sobre el particular.
Asimismo, es deber del usuario respetar la propiedad intelectual y licencias de software, por lo que está impedido de utilizar, copiar, redistribuir programas o recursos para los cuales no exista una licencia de software o autorización de uso válido. De igual forma los archivos, documentos y/o proyectos que se desarrollen en la institución son propiedad de la misma, y no pueden ser divulgados, reproducidos, negociados, o utilizados ni parcial o totalmente para fines ajenos a los propios de su naturaleza, es responsabilidad de los Usuarios la custodia de toda información de carácter confidencial, la misma que deberá estar respaldada. Los Usuarios que incurran en estos actos serán sancionados de acuerdo a la normatividad vigente.

6.3. ASIGNACIÓN DE RECURSOS Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – TIC´S (COMPUTADORAS, INTERNET, CORREO ELECTRONICO Y SISTEMAS INFORMÁTICOS)

Es facultad del HCH, de acuerdo a los recursos, necesidades y capacidad disponible, asignar a cada Usuario, los Recursos y Servicios de Tecnologías de Información y Comunicaciones – TIC´S (Computadoras, Internet, Correo Electrónico y sistemas informáticos) dentro de la red institucional.
Para el efecto los Directores o Jefes de las Oficinas o Servicios deberán realizar el requerimiento correspondiente a la Unidad Funcional de Informática, sustentando las actividades y labores que se realizaran a través del uso del recurso o servicio solicitado. (Formato de Solicitud de Recursos y Servicios de TICS´s)
Sólo podrán usarse los recursos y servicios que hayan sido previamente solicitados y autorizados por la Unidad Funcional de Informática quien realizara la evaluación correspondiente e informara la aprobación o desaprobación de la solicitud, indicando los motivos y los recursos o servicios asignados.

6.4. UTILIZACION EXCLUSIVA PARA FINES INSTITUCIONALES

Los Recursos y Servicios de Tecnologías de Información y Comunicaciones – TIC´S, así como otros accesos asignados a los usuarios, deben ser utilizados exclusivamente en el cumplimiento de sus labores institucionales.

Asimismo la información contenida en las computadoras, los mensajes de correo electrónico, proyectos, así como aquella obtenida o consultada mediante el uso de internet y los sistemas informáticos de la institución, deben utilizarse debida y directamente en las funciones o actividades institucionales a cargo de los respectivos usuarios.

En ningún caso dicha información puede ser divulgada, reproducida, negociada, o utilizada ni parcial o totalmente para fines ajenos a las funciones del HCH. Es responsabilidad de los Usuarios la custodia de toda información de carácter confidencial, la misma que deberá estar respaldada.

6.5. CUENTAS DE USUARIO Y CLAVES DE ACCESO

Las cuentas, contraseñas o claves de acceso asignadas al usuario son de carácter personal, confidencial, intransferible e irrenunciable. Su utilización es responsabilidad del usuario correspondiente.

El usuario no debe utilizar la cuenta de otra persona, intentar apoderarse de claves de acceso de otros usuarios, ni intentar burlar los sistemas de seguridad bajo ningún motivo, este tipo de actos es sancionable de acuerdo a la normatividad vigente.

Aquel usuario afectado o que advierta una incorrecta utilización de sus contraseñas o claves, deberá informar a la Unidad Funcional de Informática o quienes hagan sus veces, para que adopten las medidas correspondientes.

6.6. AUTORIZACIÓN Y SUPERVISION DE PERMISOS Y/O ACCESOS

La Unidad Funcional de Informática es responsable de brindar los permisos y/o accesos solicitados por los Directores o Jefes de la Unidad Orgánica donde labore el usuario, previa evaluación y de acuerdo a las actividades o funciones que realice el mismo, a su vez supervisara su correcto uso y solicitudes de baja las que deberán ser solicitadas oportunamente.

Son responsables solidarios de la custodia de estos permisos y/o accesos el Usuario y los Directores o Jefes Inmediatos de la Unidad Orgánica solicitante en su ámbito de competencia, por lo cual deben solicitar la baja de los mismos, cuando el usuario ya no los requiera o sea removido de su cargo (Formato de Solicitud de Recursos y Servicios de TICS´s). Los Actos ilícitos que un usuario pueda cometer por el uso indebido de estas atribuciones son causal de sanción para los responsables solidarios de acuerdo a la normativa vigente.

Los accesos a los Jefes de OCI son autorizados por la Dirección o Jefatura de la unidad orgánica de Gestión de Órganos de Control Institucional o el que haga sus veces, en base a la política de seguridad institucional y el reglamento de seguridad, debiendo supervisar el correcto uso de los servicios dados.

6.7. EQUIPOS EXTERNOS A LA INSTITUCION

El ingreso al HCH de equipamiento informático que no sea de propiedad institucional, debe ser autorizado por la Jefatura de Seguridad Interna, o el que haga sus veces en coordinación con la Unidad Funcional de Informática y de acuerdo al tiempo de permanencia de estos con la Unidad de Patrimonio, debiendo evaluarse los riesgos que afecten la seguridad de la información del HCH y las medidas para mitigarlos.

El Acceso o Permanencia de los equipos externos en la Institución es autorizado previa solicitud con 48 horas de anticipación al ingreso del mismo, salvo casos de personal de otras instituciones que de acuerdo a sus actividades (Supervisión, Visita Técnica, etc.) así lo requiera, en cuyo caso la Jefatura de Seguridad Interna deberá coordinar con la Unidad de Informática su acceso inmediato. Cuales quiera de los casos la solicitud deberá indicar si los aparatos requieren utilizar recursos informáticos del HCH (Red institucional y/o Internet). El Acceso o Permanencia es solicitado por el Director o Jefe de la Unidad Orgánica donde labora el propietario (Usuario) y/o donde se realizaran las actividades por parte de personal de otras instituciones utilizando el Formato de Acceso y/o Permanencia de Equipos Externos.

Los equipos externos solo tendrán soporte a las aplicaciones y red institucional según corresponda y de acuerdo a lo autorizado, los propietarios son únicos responsables por la cautela y cuidado de sus equipos en ningún caso el HCH se hará cargo del soporte técnico, daños internos propios de los equipos o pérdida de los mismos.

6.8. OBLIGACIÓN DE CAUTELA

La unidad orgánica responsable de Tecnologías de la Información, la unidad orgánica encargada de Seguridad Interna y el Órgano de Control Institucional, así como los Director o Jefes de las respectivas unidades orgánicas usuarias, cautelarán y adoptarán las acciones necesarias para el cumplimiento de las disposiciones de esta directiva por las personas comprendidas en su alcance, conforme al correspondiente ámbito de su competencia funcional.

6.9. RESERVA DE SERVICIOS.

La Unidad informática dentro de sus atribuciones y responsabilidades de acuerdo a la Normatividad vigente, siempre respetando la confidencialidad de los Usuarios. Se reserva la atribución de bloquear servicios, permisos y/o accesos, siempre que el resultado de la supervisión o monitoreo demuestre un riesgo potencial o vulnere la seguridad de la información del HCH, sin solicitud previa e informando a la Dirección o Jefatura de donde se hayan detectado y registrado los hechos, indicando el riesgo o vulnerabilidad registrado, los equipos o recursos afectados, las cuentas utilizadas, las consecuencias y las correspondientes sanciones de acuerdo a la normatividad vigente.

7. DISPOSICIONES ESPECIFICAS

7.1. USO DE LAS COMPUTADORAS

7.1.1. ASIGNACIÓN DE EQUIPOS.

De acuerdo a la prioridad, evaluación o necesidad de la Unidad Orgánica solicitante en la que labore o presta servicios el usuario y según las tareas o labores que le sean encomendadas, considerando la disponibilidad de equipos informáticos o de comunicaciones, la Unidad Funcional de Informática es responsable de asignar los recursos adecuadamente, informando a la Oficina de Administración para que la Oficina de Logística a través de la Unidad Patrimonio haga entrega de los equipos asignados como corresponda, registrándolos y asignándoles un código patrimonial. El usuario al cual se le asigna el bien firmará el documento respectivo en señal de recibido, quedándose con una copia.

7.1.2. DISPOSICIONES PARA EL ADECUADO USO DE LAS COMPUTADORAS

El usuario debe cuidar y dar un uso apropiado y correcto, a los equipos de procesamiento de información asignados, evitando su deterioro e incorrecta utilización.

En concordancia con dicha obligación, sin constituir una lista limitativa, el usuario se encuentra prohibido de:

a. Colocar adhesivos en las computadoras.
b. Ingerir alimentos sobre las computadoras, así como colocar o manipular líquidos en su cercanía o sobre las computadoras.
c. Rociar sobre las computadoras líquidos para el ambiente u otros que la dañen.
d. Descargar, copiar y guardar: juegos, música, videos musicales, o de entrenamiento, material pornográfico u otro tipo de información no autorizada.
e. Fumar cerca de las computadoras.
f. Colocar o apilar documentos y otros objetos sobre las computadoras o en ubicaciones que obstruyan o impidan su adecuada ventilación y uso.
g. Ubicar Unidad Central de Procesamiento (CPU) en una posición distinta a su diseño original (horizontal o vertical).
h. Conectar artefactos eléctricos sobre la línea eléctrica estabilizada de uso exclusivo para las computadoras, o sobre los estabilizadores de corriente.
i. No compartir para artefactos electrodomésticos (Horno microondas, hervidores, Frio bares, ventiladores u otros) o cargadores de celular, los tomacorrientes asignados para los equipos de cómputo utilizando adaptadores múltiples, supresores de picos u otro dispositivo de expansión de corriente.
j. Trasladar computadoras a otra área, sin la autorización de su Director o jefe de la unidad orgánica, del Departamento de Logística a través de la Unidad de Patrimonio y de la Jefatura de la Unidad Informática o quien haga sus veces.
k. Cambiar el fondo de escritorio institucional.
l. Instalar en las computadoras, programas informáticos sin autorización.

m. Modificar los parámetros o configuración de las computadoras, así como el software y/o sistema informático instalado en ellas.
n. Abrir las computadoras, así como, extraer o cambiar componentes.
o. Dejar prendidos los equipos asignados o desbloqueados cuando el usuario se retira o suspenda sus labores.
p. Establecer conexiones remotas entre la computadora asignada o no, con cualquier otro equipo informático ajeno a la Institucí6n, salvo con autorizaci6n de su Director o Jefe de Unidad Orgánica a la cual pertenece y del Jefe de Informática o quien haga sus veces y la supervisión del personal de soporte.
q. Ingresar y usar equipamiento informático ajeno a la institución, sin la autorización de la Dirección o Unidad orgánica competente usuaria o destinataria, ni la que corresponde a la unidad orgánica responsable de la Seguridad Interna a través del personal encargado o el que haga sus veces.
r. Encriptar carpetas y/o archivos sin la autorización de su Dirección o jefatura de la unidad orgánica a la que pertenece y sin el apoyo técnico de la Unidad Informática o quien haga sus veces. Es responsabilidad de la Oficina o de la unidad orgánica que autoriza, guardar la clave de encriptación y de la custodia diligente y confidencial de dichos mecanismos así como cualquier daño perjuicio que eventualmente pudiera ocasionar.
s. Distribuir información utilizando carpetas compartidas que no estén aprobadas y supervisadas por la Unidad Funcional de Informática.
t. Revisar los dispositivos externo (USB, Disco Externo) con el Antivirus antes de acceder a visualizar las carpetas para evitar la infección del equipo.
u. Dejar la sesión abierta, pues esto representa un riesgo potencial para el usuario. Ya que personas ajenas podrían apoderarse de su cuenta.
v. Otras acciones o conductas que sobre la materia se establezcan en el Reglamento interno de Trabajo.

7.1.3.COMPETENCIA SOBRE ACCIONES EN COMPUTADORAS

La Oficina de estadística e Informática a través de la Unidad Funcional de Informática o quien haga sus veces, es responsable de realizar las acciones señaladas en los incisos l), m), n) y p) del numeral 7.1.2, de acuerdo al diagnóstico o necesidad del equipo.
El personal de las Oficinas, Unidades o Servicios, deberá solicitar el soporte correspondiente, toda vez que tenga problemas con el equipo asignado.

Es responsabilidad de la Unidad Funcional de Informática tener un control de cambios respecto a las configuraciones y/o cambios en los componentes de los equipos, inventario actualizado de los mismos y un plan de mantenimiento preventivo anual.

7.1.4.ACCESO A LOS PUERTOS PERIFÉRICOS DEL EQUIPO.

La Oficina de estadística e Informática a través de la Unidad Funcional de Informática o quien haga sus veces, otorgará al usuario, derechos de acceso a los puertos periféricos (memorias USB, Discos duros externos, unidades de CD, DVD, etc.) según los tipos que a continuación se detallan, los que serán compatibles con las labores que este desarrolla y serán regulados por el director o jefe de la oficina, unidad o servicio en la cual labora.

a. Sin acceso: Bloquea el uso de todos los puertos de comunicación del equipo.

b. Sólo lectura: Permite el uso sólo para "lectura" de los dispositivos conectados a los puertos de comunicación del equipo. Esta será la configuración por defecto

c. Total: Permite la lectura y escritura en los dispositivos conectados en los puertos de comunicación del equipo.

El usuario con acceso a dispositivos portátiles deberá previamente ejecutar el antivirus y revisarlo antes del uso de la información que contenga éste.

7.2. ACCESO A LOS EQUIPOS Y RED DE DATOS

Para el acceso a los equipos y la red de datos, los Directores o Jefes de Unidad deberán enviar con anticipación la relación del personal nuevo o que ya labora en dicha Oficina, Unidad o Servicio a la Oficina de Estadística e Informática que a través de la Unidad de Informática generara las cuentas de usuario y otorgara los acceso correspondientes de acuerdo a las actividades que realice e indique dicha nomina, previa evaluación. (Formato de Solicitud de Recursos y Servicios de TICS´s)

7.2.1.CUENTA DE USUARIO PARA ACCESO AL EQUIPO Y RED DE DATOS.

El nombre de la cuenta de usuario para cada trabajador está formado de acuerdo al siguiente estándar:

a. El primer nombre del usuario unido con (.) al apellido paterno ligado a la inicial del apellido materno.
b. En caso de existir dos construcciones similares el criterio alternativo será el primer nombre del usuario seguido de la inicial del segundo nombre unido con (.) al apellido paterno ligado a la inicial del apellido materno.

Ejemplo: Si el nombre y apellidos del Trabajador son Pepito Pepón Rodriguez su cuenta usuario de red será pepito.peponr

De mantenerse una semejanza el administrador determinara el formato de la cuenta tomando como referencia los dos criterios anteriores.

7.2.2.ACCESO A LA RED DE DATOS Y RECURSOS COMPARTIDOS.

Los accesos a la red de datos del HCH son otorgados a solicitud de los Directores o Jefes de Unidad de acuerdo a las actividades que desempeñe el usuario y son evaluados por la Oficina de Estadística e Informática.

Los accesos son entregados de acuerdo a los siguientes criterios:

a. Sin Acceso: El usuario no tiene acceso ningún recurso compartido del HCH.
b. Acceso a Sistemas Hospitalarios: El usuario tiene acceso a Recursos Compartidos correspondientes a los sistemas Hospitalarios.
c. Acceso a Sistemas Administrativos: El usuario tiene acceso a Recursos Compartidos correspondientes a los Sistemas Administrativos
d. Acceso a Recursos Compartidos: El usuario dispone de accesos a carpetas compartidas personales o grupales y de Escáner, de acuerdo a las actividades que desempeñe, a solicitud de los Directores o Jefes de Unidad y previa evaluación de la Oficina de Estadística e Informática
e. Acceso a Equipos de Impresión: El usuario dispone de acceso a los equipos de impresión en Red.

7.2.3.USO DE LA RED DE DATOS Y RECURSOS COMPARTIDOS.

El uso de la red de datos y los recursos compartidos son exclusivamente para fines institucionales, los recursos compartidos para la utilización de sistemas informáticos son únicamente para acceso a los mismos y no deberán ser utilizados como carpetas compartidas para colocar información personal, fotos, juegos o documentos.

Para el caso de archivos, documentos compartidos o buzones de Escáner en red, los Directores o Jefes de Unidad deberán solicitar este espacio sustentando su necesidad especificando si serán carpetas personales o grupales e indicando los permisos correspondientes para cada usuario según el siguiente detalle:

a. Lectura: Los usuarios asignados pueden visualizar y hacer una copia local de los archivos compartidos.
b. Lectura y Escritura: Los usuarios asignados pueden visualizar, copiar y colocar archivos en el recurso compartido.
c. Buzón de Escáner: Los usuarios asignados disponen de una carpeta para digitalizar imágenes de documentos, los archivos digitalizados no pueden ser borrados por los usuarios.
d. Carpetas Personales: El usuario puede leer, escribir hacer copias locales y colocar archivos en este recurso compartido.

7.2.4. CUENTAS DE USUARIO TEMPORAL.

En el caso de que sea necesaria la creación de una cuenta de carácter temporal por temas contractuales, los Directores o Jefes de Unidad deberán solicitar la creación de una cuenta temporal indicando los datos del usuario, actividades que desempeñara y el equipo que utilizara, pues el uso de esta cuenta está restringido a un equipo determinado. Al finalizar las actividades correspondientes se deberá informar a la Unidad Funcional de Informática para la baja respectiva.

Los Directores o Jefes de las Unidades Orgánicas que soliciten y reciban accesos de tipo temporal, son responsables directos de la custodia de los accesos y el buen uso del mismo, dentro de su ámbito de competencia.

7.2.5. BAJA O INABILITACIÓN DE LAS CUENTAS DE USUARIO.

La Oficina de Recursos Humanos o la Oficina encargada de las contrataciones de personal deberán informar a la Oficina de Estadística e Informática para dar de baja a los usuarios que ya no laboren en la institución o que sean destacados en cuyo caso la cuenta solo es deshabilitada.
Es responsabilidad de ambas oficinas si dichas cuentas no son dadas de baja o deshabilitadas a su tiempo y fueran usadas para fines ilícitos.
La baja o inhabilitación de las cuentas implica que el usuario ya no tienes acceso a ningún servicio informático ni equipo del HCH.
Son responsables solidarios de la custodia de los permisos y/o accesos el Usuario y los Directores o Jefes Inmediatos de la Unidad Orgánica solicitante en su ámbito de competencia, por lo cual deben solicitar la baja de los mismos, cuando el usuario ya no los requiera o sea removido de su cargo (Formato de Solicitud de Recursos y Servicios de TICS´s). Los Actos ilícitos que un usuario pueda cometer por el uso indebido de estas atribuciones son causales de sanción para los responsables solidarios de acuerdo a la normativa vigente.

7.3. USO DEL SERVICIO DE INTERNET

7.3.1.ASIGNACIÓN DE ACCESO A INTERNET.

La Oficina de estadística e Informática a través de la Unidad Funcional de Informática o quien haga sus veces, otorgará al usuario, derechos de acceso a internet según los tipos que a continuación se detallan, los que serán compatibles a las labores que desarrolla el usuario. Esta asignación de acceso a internet, se tramitará de acuerdo al numeral 6.3.3 "Autorización de acceso".

7.3.2.TIPOS DE ACCESOS

Los tipos de acceso a internet asignados son:
a. Sin Internet: Usuario sin acceso a internet, que es considerado tipo de acceso por defecto.
b. Internet Normal: Acceso a páginas de internet con temas relacionados a:
Páginas de gobierno y banca local, Traducción web y correo web institucional.
c. Internet Avanzado: Acceso a internet con los mismos temas del tipo "Internet Normal" y adicionalmente temas relacionados de:
Correo electrónico basado en web (diferente al institucional), Grupos de noticias y foros de mensajes.
d. Internet VIP: Acceso a internet con los mismos temas del tipo "Internet Avanzado" y adicionalmente temas relacionados a:

Mensajería instantánea (web), Intercambio de archivos, radio y TV por internet, telefonía internet, Redes sociales.

Los Directores o Jefes podrán solicitar el cambio del tipo de acceso para Sí y para los Usuarios dentro de ámbito de competencia, con solicitud previa que sustente los motivos de dicho cambio, la aprobación o desaprobación será informada por la Unidad Funcional de Informática luego de la evaluación correspondiente.

7.3.3.AUTORIZACIÓN DE ACCESO.

El acceso al servicio de Internet para los usuarios, se dará de acuerdo al siguiente detalle:

a. El " Internet Normal" será autorizado por el Jefe de la Oficina, Unidad o servicio a la cual pertenezca cada usuario.

b. El " Internet Avanzado", será autorizado por el Jefe de la Unidad o Servicio a la que pertenece el usuario y visado por el respectivo Director o Jefe de la Oficina o departamento o nivel jerárquico superior equivalente, al que reporte dicha unidad, este será el acceso por defecto que tendrán los Jefes de la Unidades o servicios.

c. El " Internet VIP", será autorizado por el respectivo Director, o nivel jerárquico superior equivalente, al que reporte la Oficina o Departamento a la cual pertenezca el usuario.

Cualquier cambio del tipo de acceso a Internet Avanzado e Internet VIP será propuesto por el Director o Jefe de la Oficina o Departamento a la cual pertenece el usuario y aprobado por la Oficina de Estadística e Informática.

7.3.4.DISPOSICIONES PARA LA CORRECTA UTILIZACIÓN DEL INTERNET

Para utilizar correctamente los servicios de internet, el usuario debe observar las disposiciones siguientes:

a. Podrá utilizar programas de mensajería instantánea (ejecutables que se instalan en la computadora), sólo si cuentan con la previa autorización de la Dirección o nivel equivalente del cual depende la opinión técnica favorable de la Oficina de Estadística Informática a través de la Unidad Informática o quien haga sus veces.

b. Podrá descargar programas informáticos previamente autorizados por el Director o Jefe o Jefe de la unidad orgánica en la que labora o presta servicios el usuario y adicionalmente con la opinión técnica favorable de la Oficina de Estadística e Informática a través de la Unidad de Informática. El personal técnico de esta unidad orgánica es el autorizado para su instalación.

c. Podrá descargar archivos (Documentos de diferentes formatos) que sean necesarios para el desarrollo de las labores encomendadas y que no atenten contra la integridad de la información del HCH.

d. Podrá subir archivos (Documentos de diferentes formatos) siempre sean necesarios para cumplir con el desarrollo de sus actividades y que no atenten contra la integridad de la información del HCH.

e. Podrá utilizar los privilegios de internet en estricta sujeción al acceso autorizado y necesario para el desarrollo de sus labores institucionales.

f. Son responsables solidarios el usuario y los Directores o Jefes de las Unidades Organizas correspondientes dentro de su ámbito de competencia, por la custodia de los accesos, los archivos subidos o descargados y el buen uso del servicio de internet.

7.3.5.ACCIONES SUJETAS A LA RESPONSABILIDAD O DEL USUARIO

Cada usuario es responsable de las acciones efectuadas respecto al uso de los servicios de internet y del contenido de las páginas o enlaces a las que acceda desde la computadora o cuenta asignada comprendiendo las consecuencias o efectos que se deriven de las mismas y las sanciones según la normativa vigente.

Los Directores o Jefes de las Unidades Orgánicas donde laboren los Usuarios son responsables solidarios de la custodia de los accesos a internet, de los archivos subidos o descargados y el buen uso del mismo, dentro de su ámbito de competencia.

7.3.6.ACCESO A PERSONAS AJENAS A LA INSTITUCIÓN.

Se podrán otorgar derechos de acceso a personas ajenas a la institución siempre y cuando se cuente con la autorización y justificación respectiva del Director o Jefe de la unidad orgánica con el visado del correspondiente Director, Jefe de Unidad o nivel equivalente al que reporte.

Estos derechos tendrán una vigencia no mayor a noventa (90) días calendario y podrán ser renovados por periodos máximos similares.

Los Directores o Jefes de las Unidades Orgánicas que soliciten y reciban accesos para personas ajenas a la institución, son responsables directos de la custodia de los accesos a internet y el buen uso del mismo, dentro de su ámbito de competencia.

7.4. SISTEMAS INFORMÁTICOS.

Los sistemas informáticos forman parte de los Servicios que soportan los diferentes procesos asistenciales y administrativos del HCH. Estos sistemas son otorgados en sesión de uso por entidades del Estado, adquiridos a terceros o desarrollados por la Unidad Funcional de Informática a solicitud expresa de los Jefes de Departamentos y Servicios Asistenciales (F003-HCH-DIRE-001-2014-OEI-UI: Formato de Solicitud de Software) o de los Jefes de las Direcciones u Oficinas Administrativas, con la finalidad de mejorar la atención a pacientes y/o procesos administrativos.

7.4.1.SISTEMAS INFORMATICOS ASISTENCIALES.

Son los sistemas desarrollados por la Unidad Funcional de Informática de acuerdo a los requerimientos de los Directores y/o Jefes de las Unidades Orgánicas del HCH, que soportan los procesos de atención al paciente (Historia Clínica Electrónica, Citas,

citas en Línea), así como los sistemas de terceros que permiten el tratamiento de análisis clínicos y diagnóstico por imágenes.

7.4.2.SISTEMAS INFORMATICOS ADMINISTRATIVOS.

Los sistemas informáticos administrativos también son desarrollados por la Unidad Funcional de Informática, sin embargo existen sistemas cedidos en uso por Instituciones del Estado como el Ministerio de Salud-MINSA, Ministerio de Economía y Finanzas-MEF, Oficina Nacional de Gobierno Electrónico-ONGEI, Etc.) y que son necesarios para el desarrollo de Estadísticas e Indicadores, así como para las labores administrativas correspondientes.

7.4.3.ACCESO A LOS SISTEMAS INFORMÁTICOS HOSPITALRIOS Y/O ADMINISTRATIVOS.

Para el acceso a los sistemas informáticos del HCH son otorgados a solicitud de los Directores o Jefes de Unidad de acuerdo al as actividades desempeñadas por el usuario y previa aprobación de la Oficina de Estadística e Informática.
Los usuarios y claves de acceso a los sistemas son el primer paso para que el usuario tenga los permisos correspondientes a nivel de acceso a la red de datos y recursos compartidos.
Los accesos a los sistemas de Tramite y Hospitalarios se solicitan directamente a la Oficina de Estadística e Informática.
Para los sistemas administrativos como SIGA o SIAF se solicitan a las Oficinas de Logística y Economía respectivamente
Para el caso de los sistemas de diagnóstico, serán solicitados directamente a los departamentos correspondientes (Anatomía Patológica y/o Diagnostico por Imágenes)
Las Oficinas o Departamentos que administren o generen usuarios, deberán informar a la Oficina de Estadística e Informática la creación de estos y de esta forma se dará el acceso a los recursos correspondientes.

7.4.4.SOFTWARE DE TERCEROS

Son los software desarrollados por proveedores especializados a nivel de servicios informáticos, servicios asistenciales (Historia Clínica, Laboratorio, Diagnóstico por Imágenes, Ecografía, electrocardiogramas, etc.) y Servicios Administrativos y/o Generales.

7.4.4.1. NEUTRALIDAD TECNOLOGICA

De acuerdo a la normativa vigente no se deberá adquirir ningún soporte físico (hardware) que obligue a utilizar solo determinado tipo de software o que de alguna manera limite su autonomía informática. En caso de no existir soportes físicos (hardware), que permitan el uso de software de diferentes

tipos, la Unidad Funcional de Informática deberá Certificar esta condición y emitir el informe técnico de evaluación correspondiente.

7.4.4.2. SOLUCIONES TECNOLÓGICAS.

Cuando se trate de soluciones tecnológicas que requieran soporte de hardware y Software para su funcionamiento; como equipos Biomédicos, PLC (Controlador Lógico Programable) o de otra índole, el Servicio o Unidad solicitante deberá hacer llegar a la Unidad Funcional de Informática los requerimientos correspondientes y/o las especificaciones técnicas de la solución requerida (Hardware y Software), sin ser excluyentes una de la otra, con la finalidad de que dicha Unidad emita el informe técnico de evaluación correspondiente.

La Unidad Funcional de Informática no aceptara ninguna solución tecnológica de software o hardware que no haya sido verificada e informada oportunamente, dado que la Ley 28612 (Art. 7) y su reglamento establecen claramente las responsabilidades administrativas, penales y civiles por su incumplimiento.

7.4.4.3. INFORME TÉCNICO DE EVALUACIÓN

La Unidad Funcional de Informática dentro de sus funciones y atribuciones, podrá solicitar información complementaria a las Oficinas solicitantes o representantes de las soluciones ofertadas, quienes deberán responder oportunamente en un plazo no mayor de 72 horas mediante documento, que exprese de forma clara, especifica y sin obviar, desestimar u ocultar información de la solución.

Los informes técnicos de evaluación deberán ser emitidos de acuerdo a la normatividad vigente, considerando las guías establecidas para el caso y en un plazo no mayor a 15 días hábiles el cual podrá ampliarse según la complejidad de la evaluación.

7.5. USO DEL SERVICIO DE CORREO ELECTRÓNICO

7.5.1.ASIGNACION DEL SERVICIO CORREO ELECTRONICO Y MENSAJERIA INSTANTANEA

La unidad orgánica a la que pertenece el usuario, solicitará a la Oficina de Estadística e Informática, el acceso al servicio de correo electrónico y mensajería instantánea según los tipos de acceso que se establecen en la presente directiva y acorde con las labores que desempeñará el usuario.

7.5.2.CUENTA DE CORREO

La cuenta de correo electrónico institucional de cada usuario es la misma de la cuenta de acceso a la red ligada al dominio del HCH (@hospitalcayetano.gob.pe), es decir si el Usuarios es pepito.peponr la cuenta de correo es pepito.peponr@hospitalcayetano.gob.pe, para todos los casos se aplica el mismo criterio.

7.5.3.TIPOS DE ACCESO

Los tipos de cuentas de correo electrónico, desde los cuales se pueden enviar o recibir mensajes, podrán ser de tres (3) tipos:

a. Correo Tipo 1.- Es el correo electrónico desde el cual se puede enviar o recibir mensajes con archivos adjuntos dentro de la institución; además puede recibir mensajes con archivos adjuntos desde correos externos. La capacidad de envió y/o recepción de archivos adjuntos es de 2 MB (Megabytes) y cuenta con el servicio de mensajería instantánea a nivel interno. Este es el correo por defecto.
b. Correo Tipo 2. - Es el correo electrónico desde el cual se puede enviar o recibir mensajes con archivos adjuntos tanto dentro como fuera de la institución. La capacidad de envió y/o recepción de archivos adjuntos es de 5 MB (Megabytes) y cuenta con el servicio de mensajería instantánea a nivel interno.
c. Correo Tipo 3.- Es el correo electrónico desde el cual se puede enviar o recibir mensajes con archivos adjuntos tanto dentro como fuera de la institución. La capacidad de envió y/o recepción de archivos adjuntos es de 20 MB (Megabytes) y cuenta con el servicio de mensajería interno y externo (vía web). Este tipo está destinado para Directores y funcionarios.

Si por alguna razón alguno de los tipos de usuarios requiere mayor capacidad de envió o recepción de archivos adjuntos o el cambio de tipo de usuario, este requerimiento será remitido a la Oficina de Estadística e Informática con el refrendo del Jefe de Oficina o Servicio donde labora el usuario.

7.5.4.ASIGNACIÓN DE CUENTAS CON CARÁCTER TEMPORAL

De ser necesaria la creación de cuentas con propósitos específicos de comunicación derivados de contratos temporales o provisionales, congresos, eventos y proyectos de diversa índole; estas cuentas tendrán una fecha de caducidad y se desactivarán automáticamente a su término. La vigencia de estas cuentas de correo electrónico no será mayor a treinta (30) días y podrán renovarse por periodos máximos similares a solicitud del Director o Jefe de la unidad orgánica responsable y con el visado del Director o Jefe respectivo.

7.5.5.ASIGANCIÓN DE CUENTAS DE CARÁCTER INSTITUCIONAL O INTERINSTITUCIONAL

Las cuentas de carácter institucional o que se utilicen para fines de información interinstitucional serán asignadas a las Oficina o Unidades que hayan solicitado estas cuentas, quienes cautelaran, aseguraran y supervisaran su correcto uso.

7.5.6.USO INSTITUCIONAL DEL SERVICIO

El correo electrónico es un servicio de comunicación e intercambio de información sólo de carácter institucional, por lo que no es un servicio de difusión indiscriminado de información. En tal sentido, constituye obligación del usuario cautelar y asegurar, en el ámbito de su competencia y responsabilidad, que el uso del citado servicio responda a las funciones y fines inherentes al HCH.
La Oficina de Estadística e Informática a través de la Unidad de Informática o quien haga sus veces.
El contenido y documentación remitida por el correo electrónico institucional es responsabilidad del usuario.

7.5.7.DISPOSICIONES PARA EL CORRECTO USO OEL CORREO ELECTRONICO

En concordancia con su obligación de dar correcto uso a los servicios de correo electrónico brindados por el HCH, los usuarios deben cumplir con las siguientes disposiciones:

a. No facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.
b. No utilizar el correo electrónico institucional con fines ajenos a la institución.
c. No participar en la propagación de mensajes encadenados o similares.
d. No distribuir mensajes con contenidos impropios y/o lesivos a la moral o que afecten la imagen de terceros o de la Institución u otras entidades públicas.
e. No falsificar las cuentas de correo electrónico.
f. No enviar mensajes a grupos de discusión (listas de distribución, listas de correo y/o cadena de mensajes newsgroups que comprometan la información de la institución o violen las disposiciones legales vigentes.
g. No inscribirse en listas de correos no relacionadas directamente con su trabajo.
h. No utilizar la cuenta de correo para suscribirse o inscribirse en foros, redes sociales o servicios a fines que no tengan relación directa con las actividades que desempeña.
i. No difundir contenidos inadecuados.
j. No facilitar ni efectuar difusión masiva no autorizada,
k. No propiciar ni incurrir en actos o ataques con el objeto de imposibilitar o dificultar el servicio, mediante "mail bombing" o envió de desproporcionada cantidad de archivos con el propósito de saturar el buzón del correo del destinatario.

l. No enviar mensajes de correo electrónico al personal de la Institución como a terceros ajenos, en los que se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a controversias, problemas, funcionamiento, políticas, personas o cualquier otra situación o asunto interno del HCH, que puedan poner en entredicho la reputación o imagen institucional, aunque la información divulgada no sea de naturaleza confidencial.

m. No facilitar la recolección de direcciones electrónicas o la comercialización de bases de datos de direcciones de correo electrónico.

n. No realizar manipulaciones técnicas sobre el campo del "Asunto" a fin de evitar los sistemas y programas de bloqueo o filtro.

o. No acceder o utilizar una cuenta de correo electrónico institucional diferente a la asignada salvo permisos específicos de "envió por otro" en cuyo caso se solicitara a la Oficina de Estadística e Informática los permisos correspondientes.

7.5.8.OBSERVANCIA DE BUENAS PRACTICAS

Con la finalidad de contribuir a la mejor utilización y mantenimiento del servicio de correo electrónico, el usuario debe dar observancia a las siguientes recomendaciones:

a. Lectura de Mensajes Recibidos

- Debe leer los mensajes recibidos de manera frecuente, preferentemente cotidiana.
- Debe depurar permanentemente aquellos mensajes innecesarios, permitiendo mantener espacio disponible.
- Debe abstenerse de abrir correos electrónicos sospechosos o de dudosa procedencia, aún si conociera al remitente, teniendo especial cuidado en los mensajes remitidos en otros idiomas.

b. Correos No deseados u Ofensivos

Si recibe un mensaje que se considere no deseado u ofensivo a su persona o a cualquier otra persona, deberá comunicar este hecho al correo electrónico soporte.correo@hospitalcayetano.gob.pe, con el fin de que se tomen las acciones que correspondan al caso. No debe retransmitirlo a otros usuarios.

c. Envió de Correo

- Debe utilizar siempre el campo "asunto" para resumir el tema del mensaje indicando en letras mayúsculas las iniciales de la Oficina y/o departamento unido con (-) a la Unidad o Servicio desde donde se emite el correo, seguido de (:) y el Asunto materia del correo.
- Debe expresar las ideas completas, con palabras y signos de puntuación adecuados, revisando el texto y los destinatarios a fin de corregir posibles errores de ortografía, sintaxis, forma o fondo.

- Debe enviar mensajes debidamente formateados y evitar el uso generalizado de letras mayúsculas.
- Debe evitar el uso indiscriminado de tabuladores, para no generar la introducción de caracteres invalidas en el mensaje.
- Debe evitar el uso indiscriminado de la opción de "Acuse de recibo", a menos que sea absolutamente necesario en relación a la importancia de la comunicación.
- Debe evitar el envío de mensajes a personas que no conoce, a menos que sea por un asunto oficial que los involucre.
- Debe evitar el envío de mensajes a listas globales.
- Debe escribir el nombre de la persona a la que va dirigido el mensaje, así como el nombre del remitente.
- No debe enviar mensajes a grupos de usuarios al cual no pertenece o no está autorizado para su envío.
- En caso se ausente de la institución por vacaciones, licencias u otro motivo, debe habilitar la opción de respuesta automática de "fuera de oficina", que consigne además fecha de retomo y funcionario alterno de contacto, para que el remitente pueda derivar su comunicación a otras instancias.
- Utilice la firma de correo cuando envié o responda uno.

d. Vigencia de los Mensajes
   - En caso sea necesario mantener un mensaje en forma permanente, debe almacenar o archivar el mismo en carpetas personales de su computadora.
   - LISTAS DE CORREOS
   - Al enviar un mensaje a una lista o grupo de usuarios, debe revisar que el mensaje sea remitido a los destinatarios correctos.
   - Debe evitar él envió de archivos adjuntos a grupos de usuarios.

7.5.9. GRUPOS DE CORREO ELECTRÓNICO O CORREOS TEMATICOS

La creación, asignación o eliminación de los grupos de correo electrónico o correos temáticos, será solicitada por la Dirección o Jefatura de la unidad orgánica correspondiente y aprobada por la Dirección General a través de la Oficina de Comunicaciones.

El Director o Jefe o Jefe de la unidad orgánica solicitante, será el responsable de controlar que los correos electrónicos se mantengan actualizados

7.5.10. USO DE LA MODALIDAD DE COMUNICACIÓN INSTANTANEA

El usuario podrá hacer uso de la comunicación instantánea (Chat Interno), sólo para casos exclusivamente necesarios que se vinculen directamente al cumplimiento de las labores encomendadas.

Este servicio se habilita o suspende a solicitud del Director o Jefe de la unidad orgánica correspondiente.

7.5.11. CORREOS DIRIGIDOS A OTRAS INSTITUCIONES O A TERCERAS PERSONAS.

Los mensajes de correos electrónicos dirigidos a personas o instituciones que no pertenezcan al HCH tendrán los siguientes detalles:

a. En la Cabecera del Mensaje deberá incluir la imagen correspondiente emitida por el MINSA.
b. Al final del texto del correo deberá incluir la Firma de Correo.

Pepito Pepón Rodriguez
Astrónomo
C.A.P.: 99999
Departamento de Astronomía
Av. Honorio Delgado N° 262 Urb. Ingeniería-Lima 31
(511) 444-5555 Anexo 999
pepito.peponr@hospitalcayetano.gob.pe

c. En el pie de página deberá incluir el siguiente párrafo:

"Este mensaje electrónico y sus documentos adjuntos, sólo son para conocimiento y uso de la(s) persona(s) y/o Institución a quien va dirigido. Si usted no es el destinatario(s), agradeceremos se abstenga de copiarlos, divulgarlos o usarlos, así como agradeceremos comunique este error a la siguiente dirección: soporte.correo@hospitalcayetano.gob.pe y borre de su equipo este mensaje y los documentos adjuntos en caso contengan alguno. La lectura de este mensaje presupone que usted comprende y acepta los términos de este".

d. Adicionalmente coloque en el pie de página el siguiente párrafo:

"Imprima este mensaje o su adjunto solo si es indispensable, la ecoeficiencia se logra con el aporte de todos"

7.5.12. CORREOS QUE CONTENGAN COMUNICADOS INSTITUCIONALES

Los correos que contengan comunicados institucionales internos son aprobados por la Dirección General, antes de ser remitidos a la unidad orgánica encargada de Comunicaciones para su difusión. La unidad orgánica de origen es responsable del contenido del mismo, de igual forma la Unidad de Comunicaciones es responsable solidario del contenido aprobado y difundido. La Unidad Funcional de Informática se encarga de dar a aprobación para la distribución masiva a través de correo institucional. Para el envío masivo se utilizará la cuenta hnch.informa@hospitalcayetano.gob.pe.

7.5.13. USO DE CORREOS POR PERSONAL AJENO A LA INSTITUCIÓN.

Previa autorización y bajo responsabilidad del Director o Jefe de la unidad orgánica, el personal ajeno a la institución podrá acceder a su correo personal a través de Internet. La autorización deberá señalar el plazo máximo de acceso, el cual no podrá ser mayor a 90 días renovables por periodos máximos similares. Asimismo, se debe incorporar en el contrato una cláusula de confidencialidad.

8. SANCIONES

El no cumplimiento de los puntos expresados en la presente directiva será sancionado conforme a la falta y/o hecho de acuerdo a la normativa vigente, el Código de Ética, la Ley de Delitos Informáticos y la Ley del Procedimiento Administrativo General.

9. DISPOSICIONES FINALES

9.1. CLAUSULA CONTRACTUAL

En la Contratación de servicios no personales, consultoría o asesoría para el HCH, se deberá incluir una cláusula de cumplimiento de la presente directiva, donde a la vez se detalle los recursos y servicios informáticos que serán necesarios para el desarrollo de las actividades materia del contrato.

El Director o Jefe donde desarrolla actividades el personal contratado es responsable solidario dentro de su ámbito de competencia, por los acciones irregulares o ilícitas que el dicho usuario pueda ejercer sobre los recursos y servicios asignados.

9.2. RESPONSABILIDAD.

El incumplimiento de lo establecido en la presente Directiva por parte del Usuario y los responsables solidarios dentro de su ámbito de competencia, constituye una falta disciplinaria, aplicándose lo dispuesto en las Normas correspondientes. En el caso del usuario sujeto a modalidad contractual, el incumplimiento de la presente Directiva podrá ser causal de resolución de contrato.

9.3. EXCEPCIONES Y CASOS ESPECIALES

Toda excepción o caso especial relacionado con la seguridad de la información será tramitado a la Oficina de Estadística e Informática o a la que haga sus veces quien a través de la Unidad Funcional de Informática realizara las evaluaciones correspondientes y emitirá el informe correspondiente aprobando o desaprobando estas excepciones o casos.

9.4. VIGENCIA

La presente Directiva rige a partir del día siguiente a la fecha de su aprobación con Resolución Directoral.

Anexos

Anexos N° 01

F001-HCH-DIRE-001-2014-OEI-UI: Formato de Solicitud de Recursos y Servicios de TICS´s

Formato de Solicitud de Recursos y Servicios de TICS´s

N° Caso _____ Fecha Reg. _____ Hora Reg. _____

Antención: Diurna ☐ Nocturna ☐ Reten ☐

Unidad Organica _____ Área _____

Usuario _____ Cuenta _____

Jefe Inmediato _____ Cargo _____

Solicitud: _____

Sustento: _____

_____

_____

Personal Asiganado _____ Derivado a _____

1. Tipo de Recurso o Servicio

Cuenta de Usuario [1] Cuenta de Correo [2] Permisos de Acceso [3] Cuenta de Ml [4]

Acceso a Internet [5] Acceso a Red Social [6] Acceso Correo Publicos [7]

Recurso Compartido [8] Acceso a Recur. Compartido [9] Acceso a Red Inal./Alamb. [10]

Acceso a Sist. Hospitalarios [11] Acceso a Sist. Administrativos [12] Otros [13]

Equipo PC Escritorio [14] Equipo Computo Laptop [15] Equipo de Scaner / Impresora [16]

Creacion o Modificación de Sistemas [17] Generar Reportes de Sistemas [18]

( ) _____

2. Vigencia: Temporal ☐ Permanente ☐ Externos (Contratos) ☐ Prueba ☐

3. Datos del Equipo

Cod. Patrimonio	Serie	Marca	Modelo	Observ. (19)

(19) _____

4. Atención

Procedimiento: Creación de Cuenta ☐ Acceso a Servicios o Recursos ☐

Asignación de Equipo Informático ☐ Acceso a Sistemas Informáticos ☐

Creación de Módulo o Reporte de Sistemas ☐

Nombre del Módulo o Reporte: _____

Versión Final del Sistema: _____

Nombre del Usuario _____

Cuenta del Usuario _____

Observaciones: _____

5. Cierre del Caso Fecha _____ Hora _____

FIRMA Y SELLO DEL USUARIO

FIRMA Y SELLO DEL JEFE INMEDIATO

HOSPITAL NACIONAL CAYETANO HEREDIA OFICINA DE ASESORIA JURIDICA

HOSPITAL NACIONAL CAYETANO HEREDIA V°B° UNIDAD DE INFORMATICA

Anexos N° 02

F002-HCH-DIRE-001-2014-OEI-UI: Formato de Acceso o Permanencia de Equipos Externos

Formato de Acceso o Permanencia de Equipos Externos

N° Caso _____ Fecha Reg. _____ Hora Reg. _____

Antención: Diurna ☐ Nocturna ☐ Reten ☐

Unidad Organica _____ Área _____

Usuario _____

Correo: _____ Teléfono: _____

Jefe Inmediato _____ Cargo _____

Hora de Ingreso _____

1. Tipo de Equipo

Computadora de Escritorio o Portatil [1] Equipo de Impresión o Escaneo [2]

Equipo de Red [3] Equipo Servidor [4] Antena o Torre [5] Monitor [6]

Equipo de Almacenamiento [7] Otros Equipos Informáticos [8]

( ) _____

2. Área a donde se Dirige

Oficina / Servicio: _____

Jefe de la Oficina o Servicio: _____

Motivo del Ingreso: _____

_____

3. Vigencia: Temporal ☐ Permanente ☐

4. Datos del Equipo

Cod. Patrimonio	Serie	Marca	Modelo

Observaciones: _____

FIRMA Y SELLO DEL PROPIETARIO

FIRMA Y SELLO DEL JEFE INMEDIATO

HOSPITAL NACIONAL CAYETANO HEREDIA V°B° R.O.A.L. DE MEDICINA

HOSPITAL NACIONAL CAYETANO HEREDIA V°B° UNIDAD DE INFORMATICA

Anexos N° 03

F003-HCH-DIRE-001-2014-OEI-UI: Formato de Servicio de Mesa de Ayuda

Formato del Servicio de Mesa de Ayuda

N° Caso _____ Fecha Reg. _____ Hora Reg. _____

Antención: Diurna [ ] Nocturna [ ] Reten [ ]

Unidad Organica _____ Área _____

Usuario _____ Cuenta _____

Incidencia / Falla / Actividad: _____

1. Servicio Técnico

Personal Asiganado _____ Derivado a _____

CPU [1] Monitor [2] Periferico [3] Estabilizador [4] Impresora [5]

Software [6] Red [7] Asistencia [8] Evaluación [9] Domino [10]

Mantenimiento [11] Traslado / Instalación [12] Garantía [13] Otros [14]

Sistemas Hospitalarios [15] Sistemas Administrativos [16] Correo [17] Inventario [18]

( ) _____

2. Datos del Equipo / Situación

Cod. Patrimonio	**Serie**	**Marca**	**Modelo**	**Estado** (11)

(11) _____

3. Analisis Técnico

Diagnostico: _____

Solución: _____

Modo de Atención: En Sitio [ ] Internamiento [ ]

Procedimiento: Verifiación de Cta. [1] Instalación de HW [2] Otros [3]

Re-Instalación SW [4] Garantia [4] Informe [6] Cableado Estructurado [7]

( ) _____

Requerimientos: _____

_____

_____

_____

Observaciones: _____

4. Cierre del Caso Fecha _____ Hora _____

FIRMA Y SELLO DEL USUARIO

FIRMA Y SELLO DEL PERS. ASIGNADO