



Resolución Directoral

Miraflores, 28 de Diciembre de 2020.

VISTO:

El Expediente Nº 20-014846-001 que contiene el Informe Nº 153-2020-OEI-HEJCU emitido por la Jefa de la Oficina de Estadística e Informática, quien, a su vez remite el Informe Técnico Nº 0265-2020-ET.INFORMATICA-OEI-HEJCU emitido por el Jefe de Equipo de Informática y Telecomunicaciones de la citada oficina y el Informe Nº141-2020-OEPP-HEJCU emitido por el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento y Presupuesto, quien, a su vez remite el Informe Nº066-2020-EOM-OEPP-HEJCU emitido por la Coordinadora del Equipo de Organización y Modernización de la citada oficina del Hospital de Emergencias José Casimiro Ulloa; y,

CONSIDERANDO:

Que, el numeral VI del Título Preliminar de la Ley Nº 26842 - Ley General de Salud, establece que es responsabilidad del Estado promover las condiciones que garanticen una adecuada cobertura de prestaciones de salud a la población, en términos socialmente aceptables de seguridad, oportunidad y calidad.

Que, a través de la Resolución Ministerial Nº 004-2016-PCM, se prueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Que, mediante Resolución Ministerial Nº 850-2016-MINSA se aprueba el documento denominado "Normas para la Elaboración de Documentos Normativos del Ministerio de Salud", el cual tiene como objeto 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 y explícitos para la emisión de los documentos normativos.

Que, mediante Resolución Ministerial Nº 119-2017-MINSA se aprobó la Directiva Administrativa Nº 229-MINSA/2017/0GTI "Directiva Administrativa para el Uso de Servicios Informáticos del Ministerio de Salud", con el objetivo de establecer los lineamientos y responsabilidades que deben cumplir los usuarios para el correcto uso de los servicios informáticos.

Que, mediante Informe Nº 153-2020-OEI-HEJCU, de fecha 17 de diciembre de 2020, la Jefa de la Oficina de Estadística e Informática remite el Informe Técnico Nº 0265-2020-ET.INFORMATICA-OEI-HEJCU emitido por el Jefe de Equipo de Informática y Telecomunicaciones de la citada oficina, quien, a su vez, remite la Directiva Administrativa Nº 001-2020-OEI-HEJCU: Lineamientos para regular el acceso, asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa para su aprobación.



Que, la citada Directiva tiene como finalidad normar el acceso y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa preservando y garantizando la seguridad, confidencialidad e integridad de la información almacenada en los sistemas informáticos a través de un uso racional de los recursos informáticos.

Que, con Informe N° 141-2020-OEPP-HEJCU, de fecha 21 de diciembre de 2020, el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento y Presupuesto remite el Informe N° 066-2020-OEM-OEPP-HEJCU suscrito por la Coordinadora del Equipo de Organización y Modernización de la citada oficina, quien emite opinión técnica favorable respecto de la estructura de la Directiva Administrativa N° 001-2020-OEI-HEJCU: Lineamientos para regular el acceso, asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa.

Que, conforme a lo señalado en los párrafos precedentes y de la revisión de la Directiva Administrativa N° 001-2020-OEI-HEJCU: Lineamientos para regular el acceso, asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa, se verificó que la misma cumple con la normatividad vigente, por lo tanto, resulta necesario su aprobación a través de la resolución correspondiente.

Que, estando a lo señalado en los párrafos precedentes y contando con el visado de la Jefa de la Oficina de Estadística e Informática, del Director Ejecutivo de la Oficina Ejecutiva de Planeamiento y Presupuesto y del Jefe de la Oficina de Asesoría Jurídica del Hospital de Emergencias José Casimiro Ulloa.

De conformidad con lo dispuesto en el literal d) del artículo 11 del Reglamento de Organización y Funciones del Hospital de Emergencias José Casimiro Ulloa, aprobado por Resolución Ministerial N° 767-2006/MINSA, y de la Resolución Ministerial N° 1040-2019-MINSA y la Resolución Viceministerial N° 001-2020-SA-/DVMPAS.

En uso de sus atribuciones y facultades conferidas;

SE RESUELVE:

ARTÍCULO 1.- APROBAR la Directiva Administrativa N° 001-2020-OEI-HEJCU: Lineamientos para regular el acceso, asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa, la misma que, como anexo, forma parte integrante de la presente resolución.

ARTÍCULO 2.- ENCARGAR a la Oficina de Estadística e Informática la ejecución de las acciones correspondientes para la difusión, implementación, aplicación y supervisión de la directiva administrativa aprobada.

ARTÍCULO 3.- ENCARGAR a la Oficina de Comunicaciones la publicación de la presente resolución en el portal *web* institucional de la entidad (www.hejcu.gob.pe).

Regístrese, comuníquese y cúmplase

LPE/VDP/CAOS/LCD/ysm

Distribución:

- Dirección General
- Dirección Médica
- Of. Administración
- Of. Estadística e Informática
- Of. Planeamiento y Presupuesto
- Of. de Asesoría Jurídica
- Of. de Comunicaciones
- Archivo

MINISTERIO DE SALUD
Hospital de Emergencias "José Casimiro Ulloa"

Dr. LUIS JULIO PANCORVO ESCALA
Director General (e)
CMP. 9633 RNE. 2547



PERÚ

Ministerio de Salud

Hospital de Emergencias
"José Casimiro Ulloa"

Of. Estadística e Informática
Eq. Trabajo de Informática

HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA

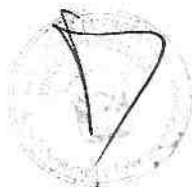


DOCUMENTO TECNICO:

**DIRECTIVA ADMINISTRATIVA Nº 001-2020-OEI-HEJCU
LINEAMIENTOS PARA REGULAR EL ACCESO, ASIGNACION DE
PRIVILEGIOS Y USO ADECUADO DE LOS SISTEMAS Y RECURSOS
INFORMATICOS EN EL HOSPITAL DE EMERGENCIAS
JOSE CASIMIRO ULLOA**

**OFICINA DE ESTADISTICA E INFORMATICA
AREA DE INFORMATICA**

2020





PERÚ

Ministerio de Salud

Hospital de Emergencias
"José Casimiro Ulloa"

Of. Estadística e Informática
Eq. Trabajo de Informática

DIRECTIVA ADMINISTRATIVA Nº 001-2020-OEI-HEJCU
LINEAMIENTOS PARA REGULAR EL ACCESO, ASIGNACION DE PRIVILEGIOS Y USO
ADECUADO DE LOS SISTEMAS Y RECURSOS INFORMATICOS
EN EL HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA

I. FINALIDAD

Normar el acceso y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa preservando y garantizando la seguridad, confidencialidad e integridad de la información almacenada en los sistemas informáticos a través de un uso racional de los recursos informáticos de los usuarios.

II. OBJETIVO

El presente documento tiene por objeto definir los procedimientos aplicables a la gestión de accesos y privilegios sobre el uso de los recursos de red puestos a disposición de los usuarios de los servicios tecnológicos del Hospital de Emergencias José Casimiro Ulloa.

III. AMBITO DE APLICACION

Este procedimiento será de aplicación a todo el personal del Hospital de Emergencias José Casimiro Ulloa, independientemente del régimen laboral o vínculo contractual al que se encuentren sujetos, a los que se les asigne y autorice el acceso y uso de los sistemas, recursos y servicios informáticos.

IV. BASE LEGAL

- TUO de la Ley N° 27444, Ley de Procedimientos Administrativos General.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de seguridad de la Información. Requisitos. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Ley N° 29733 - Ley de Protección de datos personales
- Decreto Supremo N° 003-2013-JUS, aprueban Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales
- Resolución Directoral N° 295-2017-DG-HEJCU, que aprueba el Manual de Organización y Funciones del Hospital de Emergencias - 2017 "José Casimiro Ulloa"





PERÚ

Ministerio de Salud

Hospital de Emergencias
"José Casimiro Ulloa"

Of. Estadística e Informática
Eq. Trabajo de Informática

V. DISPOSICIONES GENERALES

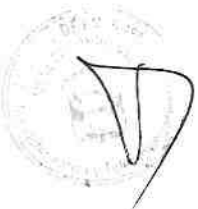
- Los sistemas, recursos y servicios informáticos deberán ser utilizados por los usuarios para las actividades directamente relacionadas con el cumplimiento de sus funciones. Ningún usuario deberá descargar música, videos, juegos o cualquier otro programa procedente de Internet ni instalarlos o copiarlos de cualquier fuente, ni acceder a lugares que incluyan material pornográfico o material en perjuicio de terceros o de la institución.
- El usuario deberá utilizar la cuenta que le ha sido asignada para tener acceso a los sistemas, servicios de red, Internet y/o correo electrónico y será de su responsabilidad proteger y no olvidar su contraseña.
- Los jefes de las Oficinas Administrativas y/o Departamentos Asistenciales podrán solicitar a la Oficina de Estadística e Informática, un backup en forma digital de la información contenida en los equipos asignados a su personal.
- La información contenida en las computadoras no podrá reproducirse o utilizarse para fines ajenos a las funciones del usuario en la institución.
- Los usuarios son responsables exclusivos de la información obtenida de Internet, del contenido de los mensajes enviados a través de Internet, para dichos efectos deberán extremar medidas de seguridad a fin de que otras personas no hagan uso o se adueñen de su usuario y/o password.
- Ante cualquier contravención a la presente Directiva que se detecte, el Área de Informática comunicará a la jefatura de la Oficina de Estadística e Informática quien a su vez informará al jefe inmediato del usuario infractor a efectos de que se tomen las medidas correctivas y administrativas pertinentes.
- Los servicios de red que se proporcionarán a los usuarios podrán ser todos o algunos de los que se detallan a continuación:
 - Acceso a los servicios de aplicaciones y sistemas de información.
 - Acceso a los servicios de red de datos.
 - Acceso a los servicios de Internet.
 - Acceso a los servicios de correo electrónico.
 - Acceso a los lectores de dispositivos externos.



VI. DISPOSICIONES ESPECIFICAS

1. GESTIÓN DE ACCESOS Y PRIVILEGIOS A LOS SISTEMAS DE INFORMACIÓN

- El usuario que requiera tener acceso a algún sistema de información deberá conocer y aceptar las normas de uso de los sistemas de información, los cuales serán otorgados únicamente por el personal del Área de Informática.



1.1 Registro de Usuarios



PERÚ

Ministerio de Salud

Hospital de Emergencias
"José Casimiro Ulloa"

Of. Estadística e Informática
Eq. Trabajo de Informática

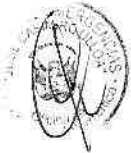
Los jefes de los trabajadores que se incorporen al Hospital de Emergencias José Casimiro Ulloa y que tengan la necesidad de acceder a los sistemas informáticos proporcionarán los siguientes datos:

- Nombres y Apellidos
- N° de DNI
- N° de CMP (en caso corresponda)

1.2 Proceso de Alta de Usuarios

En el momento en el que el trabajador se incorpore a su puesto de trabajo en el área correspondiente, su jefe solicitará la necesidad de acceso al o los sistemas informáticos definiendo los niveles de acceso requerido.

- Definición del proceso
 - a. Nombre:
Proceso de alta de Accesos.
 - b. Propósito:
Proceso soporte que tiene por objetivo el correcto desarrollo de la solicitud de accesos informáticos para los nuevos trabajadores de cada Unidad Orgánica del Hospital de Emergencias José Casimiro Ulloa.
 - c. Responsables del proceso:
Los responsables del cumplimiento de este proceso son las jefaturas de las Oficinas Administrativas, Jefes de Departamentos Asistenciales, Oficina de Estadística e Informática y el Área de Informática.
 - d. Descripción del proceso:
 1. El jefe de la Oficina Administrativa o Departamento Asistencial remitirá un documento de solicitud (memorándum) a la Oficina de Estadística e Informática, en el cual solicitará los accesos requeridos para su personal según las funciones que le sean asignadas.
 2. La jefatura de la Oficina de Estadística e Informática una vez que reciba el documento de solicitud de accesos, lo derivará al Área de Informática para la ejecución de lo solicitado.
 3. El Área de Informática registrará y dará el alta al usuario en los sistemas informáticos requeridos por su jefatura. Posteriormente comunica a su jefatura inmediata la atención de la solicitud.





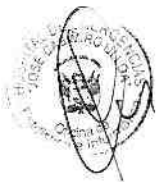
1.3 Proceso de Baja de Usuarios

En el momento en el que el trabajador deje de laborar en el Área o el Hospital de Emergencias José Casimiro Ulloa su Jefe informará acerca de este suceso para proceder con la baja de los accesos proporcionados.

Los jefes de los trabajadores que son rotados de Área o son cesados del deberán ser dados de baja y se les deberá quitar los accesos proporcionados. Deberán proporcionar los siguientes datos:

- Nombres y Apellidos
- N° de DNI
- Área en la que trabajó
- Fecha de baja del trabajador

- Definición del proceso
 - a. Nombre
Proceso de baja de accesos.
 - b. Propósito
Proceso soporte que tiene por objetivo el correcto desarrollo de la solicitud de retiro de accesos informáticos para los trabajadores rotados o cesados.
 - c. Responsable del proceso
Los responsables del cumplimiento de este proceso son las jefaturas de las Oficinas Administrativas, Jefes de Departamentos Asistenciales, Oficina de Estadística e Informática y el Área de Informática.
 - d. Descripción del proceso de Retiro de Accesos
 1. El jefe de la Oficina Administrativa o Departamento Asistencial remitirá un documento de solicitud (memorándum) a la Oficina de Estadística e Informática, en el cual en el cual comunicará que su personal será cambiado a otra oficina o que será cesado para que se proceda con las restricciones de los accesos proporcionados.
 2. La Jefatura de la Oficina de Estadística e Informática una vez que reciba el documento de solicitud de retiro de accesos del Jefe de la Oficina Administrativa o Departamento Asistencial, lo derivará al Área de Informática para su ejecución.
 3. El Área de Informática recibe la solicitud y ejecutará las acciones pertinentes para dar de baja al usuario de los sistemas según lo indicado en





PERÚ

Ministerio de Salud

Hospital de Emergencias
"José Casimiro Ulloa"

Of. Estadística e Informática
Eq. Trabajo de Informática

el documento. Posteriormente comunica a su jefatura la atención de la solicitud.

1.4 Autenticación mediante contraseñas

- Alta y baja de contraseñas

Las gestiones asociadas a la creación o eliminación de contraseñas son responsabilidad de los administradores del sistema (Área de Informática).

- Sustitución de contraseñas

El cambio de contraseñas podrá obedecer a:

1. Cumplimiento del periodo de rotación.
2. Cambio de contraseña decidido por el usuario.
3. Cambio de contraseña por olvido, pérdida o sospecha de haber sido comprometida la seguridad de la anterior.
4. Cambio de una contraseña por defecto.

2. GESTIÓN DE ACCESOS Y PRIVILEGIOS A LOS SERVICIOS DE RED DE DATOS

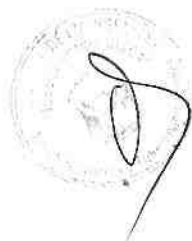
Los servicios de red serán utilizados por los usuarios para obtener servicios complementarios en sus equipos de cómputo pudiendo tener acceso a ficheros, antivirus y/o servicios de impresión.

- 2.1 El acceso a los servicios deberá ser solicitado por el jefe del usuario solicitante.
- 2.2 Para la creación del usuario (login) se utilizará la primera letra del primer nombre, seguido del apellido paterno, seguido de la primera letra de su apellido materno. Se considerará la letra inicial del segundo apellido materno y a su vez la segunda letra del apellido paterno, si fuese necesario.
- 2.3 La comunicación de las contraseñas se realizará de forma personal o vía anexo telefónico, la misma que deberá ser cambiada inmediatamente por el usuario.

Para elegir una contraseña, se recomienda lo siguiente:

- Difícil de adivinar
- Tener la cantidad de al menos seis caracteres.
- Tener caracteres de letras, dígitos y/o signos de puntuación.
- No coincidir con el nombre de la cuenta o login, número de DNI, placa del automóvil o palabras escritas al revés.
- Evitar usar el mismo password para dos sistemas distintos.

- 2.4 El usuario podrá cambiar su contraseña de inicio de sesión por motivos de seguridad solicitándolo al Área de Informática.



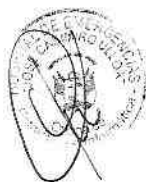


3. GESTIÓN DE ACCESOS Y PRIVILEGIOS PARA EL USO DEL INTERNET

- 3.1 El Área de Informática administrará los permisos de acceso a los servicios de Internet para todos los usuarios del Hospital de Emergencias José Casimiro Ulloa. Se estableció Niveles de Acceso a los Servicios de Internet según el cargo y función que realice el usuario. Ver Anexo N° 1.
- 3.2 El usuario solo deberá acceder a los servicios de Internet únicamente a sitios relacionados con sus funciones laborales.
- 3.3 Todo archivo adjunto descargado desde las páginas Web será examinado por el antivirus (el cual estará debidamente actualizado) que los usuarios tienen instalados en su equipo de Cómputo.
 - a. El no realizar esta acción puede poner en riesgo la información del Hospital de Emergencias José Casimiro Ulloa ya que pueden provocar que ingrese a la red informática archivos con virus o con códigos malicioso los cuales pueden borrar o alterar información de archivos, consumir recursos del equipo y acceso no autorizado a archivos.
 - b. El virus se puede extender por los equipos informáticos y producir cortes o instantes prolongados de inactividad y pérdidas de datos muy graves.
- 3.4 El usuario es responsable por cualquier información obtenida desde Internet.

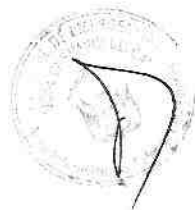
4. GESTIÓN DE ACCESOS PARA EL USO DE CORREO ELECTRÓNICO INSTITUCIONAL

- 4.1 El acceso al Servicio de Correo Electrónico, se otorga a los Jefes de Oficinas Administrativas, Jefes de Departamentos Asistenciales y/o a los Encargados o Responsables de un Área o Equipo de Trabajo.
- 4.2 Este acceso es entregado por el Área de Informática previa Solicitud de los usuarios mencionados que por la naturaleza de sus funciones requieran del uso del servicio, para lo cual el Área de Informática no procederá sin la autorización del Jefe inmediato o Director.
- 4.3 Las cuentas de correo institucionales son únicas, confidenciales y personales por lo tanto no deben ser compartidas y toda acción que se realice con ellas, es responsabilidad del usuario titular.
- 4.4 En salvaguarda de la cuenta del correo electrónico y uso indebido de la misma, el Jefe o Director del área tiene la obligación de solicitar la anulación de la cuenta de correo electrónico del personal que ya no mantiene vínculo laboral con la entidad
- 4.5 El uso del correo electrónico institucional, queda delimitado única y exclusivamente para las comunicaciones relacionadas a la función que desempeñan las personas autorizadas





- 4.6 El usuario es el responsable directo del contenido de la información que remite y recibe a través del correo electrónico asignado.
 - 4.7 El usuario debe abstenerse de abrir correos de dudosa procedencia con la finalidad de evitar posibles infecciones por virus informático.
 - 4.8 El usuario es responsable de generar copias de respaldo de los correos para lo cual podrá solicitar el apoyo del Área de Informática.
 - 4.9 Queda prohibido utilizar correo electrónico institucional, para enviar o reenviar mensajes en forma de cadenas, la remisión de correos de contenido pornográfico, ya sea en forma de imágenes, video, audio o textos constituyendo falta grave para el usuario, en caso de detectar este uso el Área de Informática elevará el Informe correspondiente para aplicar las sanciones pertinentes.
5. GESTIÓN DE ACCESOS Y PRIVILEGIOS PARA EL USO DE LECTOR DE DISPOSITIVOS EXTERNOS
- 5.1 El Área de Informática bloqueará el acceso a los puertos de conexión de los dispositivos externos de los usuarios. Esta acción será realizada previa coordinación y autorización del jefe de la Unidad Orgánica.
 - 5.2 Queda prohibido el uso de dispositivos externos que permitan la copia total o parcial de la información perteneciente a la Institución, como: quemadores de CD's / DVD's, memoria USB, etc. Sólo se podrán utilizar en casos excepcionales debidamente justificados y autorizados por el director o jefe de la unidad orgánica, y serán utilizados bajo responsabilidad del solicitante y de la persona que autoriza.
 - 5.3 Está prohibido que un usuario acceda a la información contenida en unidades de almacenamiento (medios magnéticos, electrónicos, ópticos, digitales, etc.) que no le hayan sido asignados ni autorizados por su jefe.
 - 5.4 El Área de Informática, por la naturaleza de sus funciones podrá contar y utilizar dichos dispositivos, los mismos que deben ser monitoreados por el Jefe de dicha Área.
6. PROHIBICIONES PARA EL USUARIO
- 6.1 Almacenar información personal como: música, videos, imágenes, etc.
 - 6.2 Iniciar sesión con la cuenta asignada en un equipo de cómputo diferente al que le fue asignado.
 - 6.3 Usar los servicios de Internet para actividades lucrativas o comerciales de carácter individual.
 - 6.4 Suplantar la cuenta de otro usuario.





PERÚ

Ministerio de Salud

Hospital de Emergencias
"José Casimiro Ulloa"

Of. Estadística e Informática
Eq. Trabajo de Informática

- 6.5 Utilizar los recursos informáticos para obtener acceso no autorizado a otros equipos y Servidores.
- 6.6 Utilizar los servicios de internet para ejecutar juegos, emisoras radiales, TV en línea, videos en línea, salvo casos relacionados a capacitaciones, conferencias en línea o videos descriptivos relacionados a sus funciones.
- 6.7 Guardar información en la red que infrinja los derechos de los demás.
- 6.8 Violar o intentar violar los sistemas de seguridad de los equipos de cómputo y sistemas informáticos a las cuales se tenga acceso.
- 6.9 Modificar el estado de la configuración de Red de las computadoras, cambiando la configuración de red realizada por el Área de Informática.

VII. RESPONSABILIDAD

7.1 Responsabilidad de los Jefe de Departamentos y/o Oficinas:

7.1.1 Aprobar los accesos de asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el hospital de emergencias José Casimiro Ulloa.

7.2 Responsabilidad del Oficial de Seguridad de la Información:

7.2.1 Realizar el Inventario de activos de información, Propiedad de los activos de información, Uso adecuado de los activos de información en la diferentes Oficinas y departamentos en el HEJCU.

7.2.2 Aprobar los accesos de asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el hospital de emergencias José Casimiro Ulloa

7.3 Responsabilidades del Área de Informática:

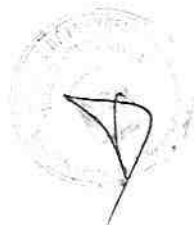
7.3.1 Adoptar, proponer y/o coordinar las medidas pertinentes, a fin de garantizar la integridad de la información y el correcto funcionamiento de los equipos de cómputo y de los servicios de red.

7.3.2 Realizar la actualización de los equipos de cómputo, a fin de conservar e incrementar la calidad del servicio que prestan.

7.3.3 Proveer de la infraestructura de seguridad adecuada en atención a los requerimientos específicos de cada área.

7.3.4 Proporcionar el servicio de acceso remoto a personal autorizado y establecer las medidas pertinentes para salvaguardar la integridad de la información.

7.3.5 Efectuar el monitoreo constante de los servicios informáticos, así como de los sistemas considerados críticos (relacionados con la atención al paciente).





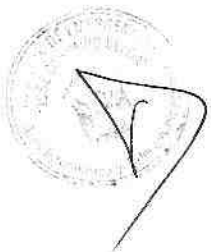
- 7.3.6 Controlar el acceso a la red e Internet, restringiendo el acceso al usuario que contravenga las normas contenidas en la presente Directiva.
- 7.3.7 Implementar herramientas que filtren y limiten los contenidos y servicios que se ofrecen en Internet, los cuales puedan atentar contra la seguridad de la información de los otros usuarios.
- 7.3.8 Mantener instalado software antivirus licenciado en los equipos de cómputo.
- 7.3.9 Implementar políticas de dominio que se ejecutan en los equipos de cómputo a nivel de usuario y equipo. Estas políticas de seguridad se implementarán de acuerdo a las funciones designadas a los usuarios.
- 7.3.10 El Área de Informática de la Oficina de Estadística e Informática se encargará de proponer la actualización de la presente Directiva según se requiera.
- 7.3.11 La Oficina de Estadística e Informática será la responsable de llevar a cabo la difusión e implementación de la presente Directiva.
- 7.3.12 El personal que se encuentra dentro del alcance de la presente Directiva a quienes se les asignó y autorizó el uso de sistemas, recursos y servicios informáticos serán los responsables de velar por el cumplimiento de la presente Directiva.

7.4 SANCIONES

- 7.4.1 Los Directores y Jefes de Oficinas y Departamento son responsables de la aplicación de la presente Directiva Administrativa
- 7.4.2 Los usuarios de los sistemas, recursos y servicios informáticos del Hospital de Emergencias José Casimiro Ulloa, serán responsables por el incumplimiento de lo dispuesto en la presente Directiva, por lo que la entidad se reserva el derecho de evaluar periódicamente su cumplimiento.
- 7.4.3 El personal que transgreda lo dispuesto en la presente Directiva Administrativa será sujeto de sanción de acuerdo a lo dispuesto en las normas vigentes de la Institución.

7.5 REVISIÓN Y EVALUACIÓN

- 7.5.1 La gestión de este Procedimiento corresponde al Oficial de Seguridad de la Información, Jefe de Oficinas y/o Departamentos y personal del Área de Informática, los cuales semestralmente (o con menor periodicidad, si existieran circunstancias que así lo aconsejen) realizarán una revisión periódica de los accesos y privilegios concedidos a los usuarios de los sistemas, recursos y servicios informáticos del Hospital de Emergencias José Casimiro Ulloa. Se adjunta propuesta de Privilegios asignados a los Sistemas, Recursos y Servicios Informáticos del HEJCU (Anexo 2).





7.5.2 La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

VIII. ANEXOS:

Anexo 01:

Niveles de Acceso a los Servicios de Internet según el cargo y función que realice el usuario

Anexo 02:

Privilegios asignados a los sistemas, recursos y servicios informáticos



HOSPITAL DE EMERGENCIAS
"José Casimiro Ulloa"
Ing. Carlos Pachas Suárez



ANEXO N° 01

NIVELES DE PERMISO	CATEGORIA DEL ACCESO O PERMISO
A	ACCESO ALTO Tienen acceso total a Internet excepto a páginas de contenido pornográfico y aquellas que pongan en riesgo la seguridad implementada en el Hospital de Emergencias José Casimiro Ulloa. Directores, Jefes de Oficinas y Departamentos.
C	ACCESO MEDIO Tienen acceso para la navegación a todas las paginas excepto a redes sociales, música y video on line y páginas de contenido pornográfico. USUARIOS
B	ACCESO BAJO Tienen acceso restringido para la navegación limitada a páginas del estado que se encuentren relacionadas con sus funciones. ADMISION, ESTADISTICA
D	SIN ACCESO Se le restringe la salida a Internet, solo puede trabajar con los servicios internos y aplicaciones USUARIOS RESTRINGIDOS

