MINISTERIO DE SALUD
VICEMINISTERIO DE PRESTACIONES
Y ASEGURAMIENTO EN SALUD
HOSPITAL DE EMERGENCIAS
JOSE CASIMIRO ULLOA

N° 049-2021-DG-HEJCU

Resolución Directoral

Miraflores, 26 de febrero de 2021.

VISTO:

El Expediente N° 21-002325-001 que contiene el Informe N° 027-2021-OEI-HEJCU emitido por la Jefa de la Oficina de Estadística e Informática, quien, a su vez remite el Informe Técnico N° 041-2021-ET.INFORMATICA-OEI-HEJCU emitido por el Jefe de Equipo de Informática y Telecomunicaciones de la citada oficina y el Informe N° 027-2021-OEPP-HEJCU emitido por el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento y Presupuesto, quien, a su vez remite el Informe N° 013-2021-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 N° 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 N° 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 N° 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 N° 119-2017-MINSA se aprobó la Directiva Administrativa N° 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 Resolución Directoral N° 310-2020-DG-HEJCU, de fecha 28 de diciembre de 2020, se aprobó 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, mediante Informe N° 027-2021-OEI-HEJCU, de fecha 18 de febrero de 2021, la Jefa de la Oficina de Estadística e Informática informa que el Director General de la Oficina de Tecnologías de la Información de Minsa realizó observaciones de la precitada directiva; por lo que, realizó una nueva versión de la citada directiva con base al Informe Técnico N° 041-2021-ET.INFORMATICA-OEI-HEJCU emitido por el Jefe de Equipo de Informática y Telecomunicaciones de la citada oficina

Que, estando a lo señalado, la Jefa de la Oficina de Estadística e Informática remite la Directiva Administrativa N° 002-2021-OEI-HEJCU: Directiva administrativa que establece el procedimiento para el acceso, asignación de privilegios, uso adecuado de los sistemas de información y demás recursos informáticos del Hospital de Emergencias José Casimiro Ulloa, debidamente visado, para la aprobación mediante acto resolutivo.

Que, la citada Directiva tiene como finalidad contribuir con la adecuada automatización y preservación de la información que se genera en el Hospital de Emergencias José Casimiro Ulloa; y, como objetivo establecer el procedimiento para el acceso, asignación de privilegios, uso adecuado de los sistemas de información y demás recursos informáticos del Hospital de Emergencias José Casimiro Ulloa

Que, con Informe N° 027-2021-OEPP-HEJCU, de fecha 22 de febrero de 2021, el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento y Presupuesto remite el Informe N° 013-2021-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° 002-2021-OEI-HEJCU: Directiva administrativa que establece el procedimiento para el acceso, asignación de privilegios, uso adecuado de los sistemas de información y demás recursos informáticos del Hejcu.

Que, conforme a lo señalado en los párrafos precedentes y de la revisión de la Directiva Administrativa N° 002-2021-OEI-HEJCU: Directiva administrativa que establece el procedimiento para el acceso, asignación de privilegios, uso adecuado de los sistemas de información y demás recursos informáticos del Hospital de Emergencias José Casimiro Ulloa, se verificó que la misma cumple con la normatividad vigente, por lo tanto, resulta necesario su aprobación mediante el presente acto resolutivo.

Que, estando a lo señalado en los párrafos precedentes y contando con el visado de la Jefa de la Oficina de Estadística e Informática, de la Directora Ejecutiva 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° 002-2021-OEI-HEJCU: Directiva administrativa que establece el procedimiento para el acceso, asignación de privilegios, uso adecuado de los sistemas de información y demás recursos informáticos del Hospital de Emergencias José Casimiro Ulloa, la misma que, como anexo, forma parte integrante de la presente resolución.

ARTÍCULO 2.- DEJAR SIN EFECTO toda disposición que se oponga a la presente resolución.

ARTÍCULO 3.- ENCARGAR a la Oficina de Estadística e Informática la ejecución de las acciones correspondientes para la difusión, implementación, aplicación y supervisión de la directiva aprobada.

ARTÍCULO 4.- 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

MINISTERIO DE SALUD
Hospital de Emergencias "José Casimiro Ulloa"
Dr. LUIS JULIO PANCORVO ESCALA
Director General (e)
CMP 9633 RNE 2547

LJPE/VDP/MRIA/LCD/jp
Distribución:
- Dirección General
- Dirección Medica
- Of. Administración
- Of. Estadística e Informática
- Of. Planeamiento y Presupuesto
- Of. de Asesoría Jurídica
- Of. de Comunicaciones
- Archivo

HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA

DIRECTIVA ADMINISTRATIVA Nº 002-2021-OEI-HEJCU

DIRECTIVA ADMINISTRATIVA QUE ESTABLECE EL PROCEDIMIENTO PARA EL ACCESO, ASIGNACIÓN DE PRIVILEGIOS, USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN Y DEMÁS RECURSOS INFORMÁTICOS DEL HOSPITAL DE EMERGENCIAS JOSÉ CASIMIRO ULLOA

OFICINA DE ESTADISTICA E INFORMATICA

AREA DE INFORMATICA

2021

DIRECTIVA ADMINISTRATIVA N° 002-2021-0EI-HEJCU

DIRECTIVA ADMINISTRATIVA QUE ESTABLECE EL PROCEDIMIENTO PARA EL ACCESO, ASIGNACIÓN DE PRIVILEGIOS, USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN Y DEMÁS RECURSOS INFORMÁTICOS DEL HOSPITAL DE EMERGENCIAS JOSÉ CASIMIRO ULLOA

I. FINALIDAD:

Contribuir con la adecuada automatización y preservación de la información que se genera en el Hospital de Emergencia José Casimiro Ulloa

II. OBJETIVO:

Establecer el procedimiento del acceso, asignación de privilegios y uso adecuado de los sistemas de información, así como los demás recursos informáticos del Hospital de Emergencia José Casimiro Ulloa

III. AMBITO DE APLICACIÓN:

La presente Directiva Administrativa es de aplicación obligatoria a todas las dependencias del Hospital de Emergencia José Casimiro Ulloa

IV. BASE LEGAL:

- Ley N° 26842, Ley General de Salud.
- Ley N° 27815, Ley del Código de Ética de la Función Pública.
- Ley N° 30096, Ley de Delitos Informáticos, y sus modificatorias.
- Ley N° 29733, Ley de Protección de Datos Personales y su modificatoria.
- Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, y modificatoria.
- Decreto Supremo N° 008-2017-SA, que aprobó el Reglamento de Organización y Funciones del Ministerio de Salud.

- Decreto Supremo N° 050-2018-PCM, Decreto Supremo que establece la definición de la seguridad digital de ámbito nacional, en cumplimiento con la segunda disposición complementaria final de la Ley N° 30618, Ley que modifica el Decreto Legislativo N° 1141.
- Decreto Supremo N° 051-2018-PCM, Decreto Supremo que crea el Portal de Software Público Peruano y establece disposiciones adicionales sobre el Software Público Peruano.
- Resolución Ministerial N° 381-2008-PCM, Lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado.
- Resolución Ministerial N° 129-2014-PCM, que aprueba el uso obligatorio de la 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 2da Edición en todas las entidades integrantes del sistema nacional de informática.
- Resolución Ministerial N° 431-2015/MINSA, que aprueba el Documento Técnico "Política de Seguridad de la Información del Ministerio de Salud - MINSA".
- Resolución Ministerial N° 004-2016-PCM, 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".
- Resolución Ministerial N° 074-2017/MINSA, que aprueba la Directiva Administrativa N° 227-MINSA/2017/OGTI, Directiva Administrativa de Organización del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud.
- Resolución Ministerial N° 119-2017/MINSA, Directiva Administrativa N° 229 - MINSA/2017/OGTI "Directiva Administrativa para el Uso de Servicios Informáticos del MINSA de Salud".
- Resolución Ministerial N° 120-2017/MINSA, Directiva Administrativa N° 230-MINSA/2017/OGTI "Directiva Administrativa que establece los estándares y criterios técnicos para el desarrollo de los sistemas de información en salud".
- Resolución Directoral N° 019-2013-JUS/DGPDP que aprueba la Directiva de Seguridad de la Información Administrada por los bancos de datos personales por la Autoridad Nacional de Protección de Datos Personales del MINSA de Justicia y Derechos Humanos.

V. DISPOSICIONES GENERALES

5.1 DEFINICIONES OPERATIVAS

5.1.1 **Activo de Información:** Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución, en la que se distinguen tres niveles:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
- Los Equipos/Sistemas/infraestructura que soportan esta información.
- Las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

5.1.2 **Alta de usuario:** Consiste en la creación de una cuenta para un usuario, que le permitirá tener acceso a la computadora designada, aplicaciones, sistemas informáticos y servicios de red.

5.1.3 **Amenaza:** Es cualquier situación o bien tangible (por ejemplo, un objeto, una sustancia, un ser humano) que es capaz de actuar contra un activo de una manera que pueda dañarlo. Una causa potencial de un incidente no deseado.

5.1.4 **Arquitectura Digital:** Es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.

5.1.5 **Baja de usuario:** Consiste en la eliminación definitiva de la cuenta de usuario y los servicios de red de la Institución, teniendo el debido cuidado con la información generada.

5.1.6 **Banco de datos personales:** Es el conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

5.1.7 **Base de datos:** Es una serie de datos organizados, agrupados, estructurados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una entidad.

5.1.8 **Compromiso de Confidencialidad:** Es el documento suscrito con los Funcionarios MINSA y Servidores Públicos que manejan Información del Ministerio de Salud, precisando obligaciones de no difundir la información ante terceros y el uso indebido de la misma.

5.1.9 **Confidencialidad de la Información:** Es la condición que mitiga o evita el Impacto negativo al MINSA que se generaría por el acceso a la Información por visitas, Funcionarios MINSA, Servidores Públicos aplicaciones informáticas o cualquier mecanismo no autorizado dentro de un plazo determinado por el Impacto de la difusión de la Información.

5.1.10 **Controles Criptográficos:** Es el conjunto de técnicas que hacen posible el intercambio de mensajes por la red de manera segura, que garantiza que los mensajes sólo puedan ser leídos por las personas a quienes van dirigidos.

5.1.11 **Correo electrónico:** Servicio de internet que permite el intercambio rápido de mensajes entre personas remotas que no necesariamente han de estar conectadas a la vez. Para poder hacer uso, ambas personas deben disponer de una cuenta, ofrecida por un proveedor de estos servicios.

5.1.12 **Delito Informático:** Es la conducta ilícita que afecta los sistemas, datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación.

5.1.13 **Disponibilidad de la información:** Es la característica de ser accesible y utilizable a pedido de alguna persona natural o jurídica.

5.1.14 **Equipos informáticos:** Es el conjunto de componentes que están destinados a realizar una función específica. Están considerados los servidores de red, computadoras personales, laptops, tablets, impresoras, escáneres, entre otros.

5.1.15 **Equipo de telecomunicaciones:** Es el hardware utilizado para los fines de telecomunicaciones. Están considerados los proyectores, teléfonos celulares, switches, hubs, routers, equipos de radiocomunicación, wi fi, radios, entre otros.

5.1.16 **Hardware:** Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar)

5.1.17 **Información:** Es el conjunto de datos significativos organizados e cualquier forma de ingreso electrónico óptico, magnético, físico o en otros medios, susceptible de ser procesada, distribuida y almacenada, que permita y ayude a la toma de decisiones, cuyo uso no autorizado puede poner en riesgo los intereses del Ministerio de Salud.

5.1.18 **Integridad de la información:** Es la propiedad de salvaguardar la exactitud y el estado completo de los activos.

5.1.19 **Lineamientos:** Es el conjunto de acciones, controles, pautas y requisitos que se deben desarrollar y cumplir prioritariamente para llevar a cabo la implementación de la Política de Seguridad de Información.

5.1.20 **Logs de auditoría:** Es el registro secuencial en un archivo o en una base de datos de todos los acontecimientos, eventos o acciones que afectan a un proceso particular, una aplicación o actividad de una red informática, entre otros. De esta forma constituye una evidencia del comportamiento del sistema.

5.1.21 **Navegador:** Es un software que permite el acceso a Internet, interpretando la información de archivos y sitios web para que éstos puedan ser leídos.

5.1.22 **Plan de Continuidad de negocios:** Es aquel utilizado por una organización para responder ante la interrupción de los procesos críticos de negocio. Depende del plan de contingencia para la restauración de los sistemas críticos.

5.1.23 **Política:** Son las declaraciones de alto nivel sobre la intención y la dirección de la gerencia.

5.1.24 **Procedimiento de anonimización:** Es el tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

5.1.25 **Procedimiento de disociación:** Es el tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.

5.1.26 **Recurso informático y de Comunicaciones:** Son dispositivos tecnológicos de hardware, software o de comunicaciones (también conocidos como Tecnologías de la Información y Comunicación - TIC) destinados a soportar los procesos de los sistemas de información de una entidad. Se incluyen a los equipos informáticos, equipos de telecomunicaciones, internet, intranet entre otros.

5.1.27 **Riesgo:** Es el efecto de la incertidumbre sobre los objetivos.

5.1.28 **Seguridad de la Información:** Es la protección de la información de un amplio rango de amenazas para asegurar la continuidad de las actividades, minimizando los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de la institución.

5.1.29 **Seguridad Digital:** Es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

5.1.30 **Servidor:** Computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes)

5.1.31 **Sistema de información administrativo:** Es aquel que integran todos los datos y la información relevante de los procesos y procedimientos administrativos tales como los de planificación, presupuesto, logística, finanzas, recursos humanos, gestión documentaria, entre otros.

5.1.32 **Sistema de información asistencial:** Es aquel que integran todos los datos y la información relevante de los procesos y procedimientos involucrados en el ámbito de competencia del Ministerio de Salud como ente rector del sector salud.

5.1.33 **Sistema de Información:** Es el conjunto de elementos que interactúan para el tratamiento y administración de datos e información generada que debe cubrir una necesidad o un objetivo, así como estar organizada y disponible para su uso posterior. Para los efectos de la presente Directiva Administrativa se incluye los Sistemas de Información Asistencial y los Sistemas de Información Administrativa.

5.1.34 **Tecnologías Digitales:** Son las Tecnologías de la información y comunicación - TIC como la Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

5.1.35 **Tratamiento de datos personales:** Es cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

5.1.36 **Virus Informático:** Programa informático que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas

5.1.37 **Vulnerabilidad:** Es una deficiencia o debilidad en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.

5.2 DE LOS RECURSOS INFORMÁTICOS

5.2.1 Los sistemas de información, recursos y servicios informáticos deberán ser utilizados por los usuarios para las actividades directamente relacionadas con el cumplimento de sus funciones.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 La información contenida en las computadoras no podrá reproducirse o utilizarse para fines ajenos a las funciones del usuario en la institución.

5.2.6 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.

5.2.7 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.

5.2.8 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.

5.2.9 Los servicios de red que se proporcionarán a los usuarios serán 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 ESPECÍFICAS

6.1 GESTIÓN DE ACCESOS Y PRIVILEGIOS A LOS SISTEMAS DE INFORMACIÓN

6.1.1 Proceso de Registro de Usuarios

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)

6.1.2 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 presentará la necesidad de acceso al o los sistemas informáticos que requiera de acuerdo a sus funciones definiendo los niveles de acceso requerido.

- **Definición del proceso**

1. Nombre:

   Proceso de alta de Accesos.

2. 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.

3. 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.

4. Descripción del proceso:

   a. 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.

   b. 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.

   c. 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.

6.1.3 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 Hospital deberán ser dados de baja y se les deberá quitar los accesos proporcionados. Deberán proporcionar los siguientes datos:

- Nombres y apellidos
- N° de Documento Nacional de Identidad o Documento de Identidad (para el caso de extranjeros)
- Área en la que trabajó
- Fecha de baja del trabajador

- **Definición del proceso**

1. Nombre:

   Proceso de baja de accesos.

2. Propósito:

   Proceso soporte que tiene por objetivo el correcto desarrollo de la solicitud de retiro de accesos informáticos para los trabajadores rotados o cesados.

3. 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.

4. Descripción del proceso:

   a. 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.

   b. 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 Departamento Asistencial, lo derivará al Área de Informática para su ejecución.

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

6.1.4 Proceso de modificación de usuarios

Los jefes de Oficinas/Departamentos correspondientes deben comunicar (a través de la Oficina de Estadística e Informática) al Área de Informática cualquier rotación de área dentro de la misma oficina/departamento del personal a su cargo o cambio de funciones para verificar y/o modificar los permisos de acceso a los recursos informáticos asignados.

6.1.5 Autenticación mediante el uso de 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.

6.2 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.

6.2.1 El acceso a los servicios deberá ser solicitado por el jefe del usuario solicitante.

6.2.2 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.

6.2.3 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.

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

6.3 GESTIÓN DE ACCESOS Y PRIVILEGIOS PARA EL USO DEL INTERNET

6.3.1 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.

6.3.2 El usuario solo deberá acceder a los servicios de Internet únicamente a sitios relacionados con sus funciones laborales.

6.3.3 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.

- 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.
- El virus se puede extender por los equipos informáticos y producir cortes o instantes prolongados de inactividad y pérdidas de datos muy graves.

6.3.4 El usuario es responsable por cualquier información obtenida desde Internet.

6.4 GESTIÓN DE ACCESOS PARA EL USO DE CORREO ELECTRÓNICO INSTITUCIONAL

6.4.1 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.

6.4.2 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.

6.4.3 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.

6.4.4 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.

6.4.5 El uso del correo electrónico institucional es oficial y obligatorio, queda delimitado única y exclusivamente para las comunicaciones relacionadas a la función que desempeñan las personas autorizadas, para que a través de este realice bajo su total responsabilidad las operaciones de envío y recepción de correos internamente (hospital) y externamente con otras entidades.

6.4.6 El usuario es el responsable directo del contenido de la información que remite y recepciona a través del correo electrónico asignado.

6.4.7 El usuario deberá revisar periódicamente el correo institucional asignado y responder oportunamente.

6.4.8 El usuario debe abstenerse de abrir correos de dudosa procedencia con la finalidad de evitar posibles infecciones por virus informático.

6.4.9 El usuario es responsable de velar por la seguridad de la información contenida en los correos electrónicos, para ello el usuario deberá coordinar la generación de copias de respaldo de los correos con el apoyo del Área de Informática.

6.4.10 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.

6.5 GESTIÓN DE ACCESOS Y PRIVILEGIOS PARA EL USO DE LECTOR DE DISPOSITIVOS EXTERNOS

6.5.1 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.

6.5.2 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 USD, 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.

6.5.3 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.

6.5.4 El Área de Informática, por la naturaleza de sus funciones podrá contar y utilizar dichos dispositivos, los mismos que deben serán monitoreados por el Jefe de dicha Área.

6.6 REVISION DE LOS ACCESOS DE LOS USUARIOS

6.6.1 El Área de Informática realizará una revisión periódica (cada seis meses) de los accesos otorgados a los usuarios, así como después de cualquier cambio como promoción, degradación o término de vínculo laboral.

6.6.2 El Área de Informática realizará una revisión periódica (cada tres meses) las autorizaciones de acceso con privilegios especiales. Los cambios en las cuentas privilegiadas serán registrados para una revisión periódica.

6.6.3 Se definirán los siguientes perfiles de usuario para todos los sistemas de información, recursos informáticos y servicios informáticos: Jefe de Departamento Médico, Jefe de Oficina Administrativa, Jefe de Área Administrativa, Secretaria, Médico Cirujano, Médico Patólogo, Médico Radiólogo, Interno de Medicina, Tecnólogo de Radiología, Tecnólogo de Patología, Admisionista, Técnico de Archivo, Técnico en Estadística, Químico Farmacéutico, Técnico Farmacéutico, Comunicador, Responsable de Página Web, Responsable de Libro de Reclamaciones, Auditor de Control Interno, Técnico Administrativo, Contador, Tesorero, Cajero, Responsable de Docencia.

6.7 PROHIBICIONES PARA EL USUARIO

6.7.1 Almacenar información personal como: música, videos, imágenes, etc.

6.7.2 Iniciar sesión con la cuenta asignada en un equipo de cómputo diferente al que le fue asignado.

6.7.3 Usar los servicios de Internet para actividades lucrativas o comerciales de carácter individual.

6.7.4 Suplantar la cuenta de otro usuario.

6.7.5 Utilizar los recursos informáticos para obtener acceso no autorizado a otros equipos y Servidores.

6.7.6 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.

6.7.7 Guardar información en la red que infrinja los derechos de los demás.

6.7.8 Vulnerar o intentar vulneraciones a los sistemas de seguridad de los equipos de cómputo y sistemas de información a las cuales se tenga acceso.

6.7.9 Modificar el estado de la configuración de Red de las computadoras, cambiando la configuración de red realizada por el Área de Informática.

6.8 DE LAS MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

6.8.1 El Jefe o Director del área, bajo responsabilidad, son responsables de designar a un encargado de archivo que implemente las medidas de seguridad de los DPS, evitando la pérdida o destrucción de estos, tanto de forma manual como a través del uso de las TIC.

6.8.2 La Oficina de Estadística e Informática del Hospital Casimiro Ulloa, debe implementar las siguientes medidas de seguridad de la información:

a. El proceso de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos a acceso a la persona responsable de los datos personales en salud.

b. El proceso de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para los tipos de usuarios a todos los sistemas y servicios brindados, con la debida precisión.

c. La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada, de acuerdo a las responsabilidades asignadas y por un plazo de dos meses solicitando su renovación en caso que amerite.

d. La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.

e. Designar a un personal responsable y competente, con la finalidad de que revise los derechos de acceso de usuarios a intervalos regulares a nivel nacional.

f. El acceso a la información o datos personales en salud y a las funciones del sistema debe ser restringido.

g. Los sistemas y las aplicaciones deben ser controladas por un procedimiento de ingreso seguro.

h. Los sistemas deben ser interactivos y deben asegurar contraseñas de calidad.

i. El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones deben ser restringido y controlarse estrictamente.

j. En el caso de los sistemas de información, el acceso al código fuente de los programas debe ser restringido.

6.9 DE LAS OBLIGACIONES DE LOS DEPARTAMENTOS Y/U OFICINAS DEL HOSPITAL CASIMIRO ULLOA

6.9.1 De los Jefe de Departamentos y/u Oficinas:

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

6.9.2 Del Oficial de Seguridad de la Información:

- 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.
- Aprobar los accesos de asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa.
- Implementar 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.

6.9.3 Del Área de informática:

- 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.
- Realizar la actualización de los equipos de cómputo, a fin de conservar e incrementar la calidad del servicio que prestan.
- Proveer de la infraestructura de seguridad adecuada en atención a los requerimientos específicos de cada área.
- Proporcionar el servicio de acceso remoto a personal autorizado y establecer las medidas pertinentes para salvaguardar la integridad de la información.

- Efectuar el monitoreo constante de los servicios informáticos, así como de los sistemas considerados críticos (relacionados con la atención al paciente).
- Controlar el acceso a la red e Internet, restringiendo el acceso al usuario que contravenga las normas contenidas en la presente Directiva.
- 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.
- Mantener instalado software antivirus licenciado en los equipos de cómputo.
- 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.
- El Área de Informática de la Oficina de Estadística e Informática se encargará de proponer la actualización de la presente Directiva según se requiera.
- 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.
- El Área de Informática se reserva el derecho de evaluar periódicamente su cumplimiento.

6.9.4 De los usuarios

- Los usuarios de los sistemas, recursos y servicios informáticos del Hospital de Emergencias José Casimiro Ulloa, serán responsables de solicitar a través de su jefatura el servicio necesario para la realización de sus funciones ya sea por un incidente o por un requerimiento.

VII. REVISIÓN Y EVALUACIÓN

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).

VIII. RESPONSABILIDADES

8.1 La Oficina de Estadística e Informática en coordinación con el Oficial de Seguridad de la Información del HEJCU son responsables de difundir e implementar la presente Directiva Administrativa a los diferentes actores señalados en el ámbito de aplicación, así como brindar la asistencia técnica que se requiera, y supervisar la implementación de la presente Directiva Administrativa.

8.2 Los Directores y Jefes de Oficinas y Departamentos o quien haga sus veces en los órganos del HEJCU, son responsables de la aplicación de la presente Directiva Administrativa.

IX. DISPOSICIONES FINALES

El incumplimiento de las presentes Políticas, Directivas, Procedimientos, u otros documentos que se deriven de estás, dará lugar a la aplicación de las sanciones correspondientes dispuesto en la Ley N° 27815, Ley del Código de Ética de la Función Pública y lo establecido en el Reglamento de Ley N° 30057, Ley del Servicio Civil, aprobado mediante Decreto Supremo N° 040-2014-PCM, sin prejuicio de las responsabilidades civiles y/o penales que pudieran corresponder.

X. ANEXOS

10.1 Anexo N° 01: Niveles de acceso a los servicios según el cargo y función que realice el usuario.

10.2 Anexo N° 02: Privilegios asignados a los sistemas, recursos y servicios informáticos.

10.3 Anexo N° 03: Formato de solicitud de alta/baja de recursos informáticos.

10.4 Anexo N° 04: Formato de Asignación de cuenta de correo electrónico institucional.

MINISTERIO DE SALUD
Hospital de Emergencias "José Casimiro Ulloa"
Lic. Cristina Dávila Peña
Jefe de la Oficina de Estadística e Informática
COESPE N° 1699

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.
B	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
C	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

ANEXO Nº 02 : PRIVILEGIOS ASIGNADOS A LOS SISTEMAS, RECURSOS Y SERVICIOS INFORMATICOS DEL HEJCU

PERFILES	SISTEMAS DE INFORMACION																													RECURSOS INFORMATICOS									SERVICIOS INFORMATICOS	
	SISTEMA SISGALENPLUS				RIS/PACS		SIGLA			FARMAX				SANPAT					SIGA					SIAF			SISTEMA DE PERSONAL												
	Emergencia	Hospitalizacion	Consulta Externa	Seguimiento	RIS	Visualizador PACs	Definicion del Sistema	Atencion de Pacientes	Visualizacion de Resultados	Tablas	Almacenes	Ventas	Reportes	Donantes	Unidades de Sangre	Control	Reportes	Configuracion	Logistica	Patrimonio	PPR	Utilitarios	Configuracion	Conciliacion de operaciones SIAF	Proceso Presupuestario	Administrativo	Tablas	Programacion	Operaciones	Calculos	Interfase	Reportes	Internet	Correo Electronico	Administracion de Redes Sociales	USB, Lector de Memorias	Carpeta Compartida Postulantes	Carpeta Compartida Libro de	Carpeta Compartida Trabajadores x Terceros	Carpeta Compartida Internos de Medicina	Carpetas Compartidas de archivos de usuarios	Video vigilancia	Administracion de Pagina Web Institucional
Jefe de Departamento Medico				x		x			x																			x				x	x	x						x		
Jefe de Oficina Administrativa																			x						x	x		x				x	x		x					x		
Jefe de Area Administrativa																			x						x	x		x				x		x		x				x		
Secretaria																			x									x				x								x		
Medico			x			x			x																																
Medico Patologo							x	x						x	x	x	x																									
Medico Radiologo					x	x																																			
Interno de Medicina			x		x	x																																			
Tecnologo de Radiologia					x	x																																			
Tecnologo de Patologia							x	x						x	x	x	x																									
Admisionista	x	x	x	x																																					
Tecnico de Archivo				x																												x							x		
Tecnico en Estadistica	x	x		x	x																																		x		
Quimico Farmaceutico										x	x		x																			x	x						x		
Tecnico Farmaceutico											x	x	x																										x		
Comunicador																																x	x	x	x				x	x	
Responsable de Pagina Web																																x	x						x		x
Responsable de Libro de Reclamaciones				x																													x			x					
Auditor de Control Interno																																x	x						x		
Tecnico Administrativo																										x													x		
Contador																								x		x															
Tesorero																										x															
Cajero																																							x		
Responsable de Docencia																																						x			

LEYENDA:

* SISGALENPLUS: Sistema de Gestion Hospitalaria
* RIS/PACS: Sistema de Gestion de Informacion Radiologica
* SIGLA: Sistema de Gestion de Informacion de Laboratorio
* FARMAX: Sistema de Gestion de Farmacia
* SANPAT: Sistema de Banco de Sangre
* SIGA: Sistema Integrado de Gestion Administrativa
* SIAF: Sistema Integrado de Administracion Financiera

HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA – Oficina de Informática

Oficina Ejecutiva de Planeamiento Estratégico, Organización y Modernización – HEJCU – Dpto. Organización

DIRECCIÓN GENERAL – H.E.J.C.U.

ANEXO N° 03

FORMATO DE SOLICITUD DE ALTA/BAJA DE RECURSOS INFORMATICOS

1. Datos del usuario:

Apellidos y Nombre: _____

DNI u Otro Doc. De Identificación: _____

Fecha de Nacimiento: _____

Correo electrónico: _____

Teléfono de contacto: _____

Fecha de solicitud: _____

2. Condición:

( ) Nombrado ( ) CAS

( ) Terceros ( ) Otro: _____

3. Solicitante:

Apellidos y Nombre: _____

DNI u Otro Doc. De Identificación: _____

Teléfono de contacto: _____

Cargo: _____

4. Motivo de la solicitud:

( ) Alta en los Sistemas: _____

( ) Baja en los Sistemas: _____

( ) Alta en recursos informáticos: _____

_____

( ) Baja en recursos informáticos: _____

_____

5. Permisos adicionales requeridos (especificar):

_____

_____

_____

6. Firma

_____ _____

V°B° Jefe Usuario

ANEXO N° 04

FORMATO DE ASIGNACION DE CORREO ELECTRONICO INSTITUCIONAL

Por medio de la presente se hace entrega de la cuenta de correo electrónico institucional del Hospital de Emergencias "José Casimiro Ulloa", para que a través de este realice bajo su total responsabilidad las operaciones de envío y recepción de correos de manera oficial internamente y externamente con otras entidades, siempre y cuando sea en el cumplimiento de sus labores o roles profesionales que desempeñe según el cargo que tiene asignado.

Cuenta: usuario@hejcu.gob.pe

Contraseña: 12345678

No olvide cambiar su contraseña por una nueva que solo sea de su conocimiento para establecer las políticas de privacidad y seguridad de la información que gestionará a través de este medio.

La presente se firma en la sede institucional a los (.....) días del mes de .....del 20....

DIRECCIÓN GENERAL HEJCU

_____

Firma

Oficina Ejecutiva de Planeamiento y Presupuesto, Organización y Modernización HEJCU

Nombre y Apellidos: .....

.....

Cargo: .....

HOSPITAL DE EMERGENCIAS JOSÉ CASIMIRO ULLOA

Oficina / Dpto: .....

Nota: A partir de la fecha usted deberá utilizar el correo institucional asignado (@hejcu.gob.pe) de manera oficial y exclusivo.