GOBIERNO REGIONAL LA LIBERTAD

GERENCIA REGIONAL DE SALUD

HOSPITAL REGIONAL DOCENTE DE TRUJILLO

OFICINA DE ESTADÍSTICA E INFORMÁTICA – ÁREA DE INFORMÁTICA

"DIRECTIVA PARA NORMAR EL USO DEL SERVICIO DE CORREO ELECTRÓNICO INSTITUCIONAL EN EL HOSPITAL REGIONAL DOCENTE DE TRUJILLO"

DIRECTIVA Nº:		**Versión:** **1.0**	**Página:** **09**
ELABORADO POR:	**Ing. José Martín Andonaire Flores** Jefe del Área de Informática **Equipo de Trabajo** Área de Informática	**FIRMA**	**FECHA** **26/04/2019**
REVISADO POR:			
APROBADO POR:			

Trujillo, abril 2019

CONTENIDO

1. OBJETIVO

1.1. Delinear el procedimiento correcto para el uso del servicio de correo electrónico institucional en las diferentes Unidades Orgánicas que conforman el Hospital Regional Docente de Trujillo (HRDT).

2. FINALIDAD

2.1. Normar los procedimientos para el uso del correo electrónico institucional a nivel de las diferentes Unidades Orgánicas que conforman el Hospital Regional Docente de Trujillo, para permitir que la comunicación e intercambio de información entre personas y entidades de la administración pública sea ágil y fluida.

3. BASE LEGAL

3.1. Resolución Ministerial **N°246-2007-PCM**, que aprueba el curso obligatorio de la Norma Técnica Peruana **"NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de seguridad de la información. 2ª Edición"**, en todas las entidades integrantes del Sistema Nacional de Informática.
3.2. Resolución Ministerial **N°004-2016-PCM**, que aprueba el uso obligatorio de la Norma Técnica Peruana **"NTP-ISO/IEC 27001:2014 EDI. 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.
3.3. LEY N° 27658, Ley Marco de Modernización de la Gestión del Estado.
3.4. LEY N° 27815, Ley del Código de Ética de la Función Pública.
3.5. LEY N° 29733, Ley de Protección de Datos Personales.
3.6. Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales aprobado por decreto supremo 003-2013-JUS.
3.7. Directiva N° 005-2003-INEI/DTNP "Normas para el uso del servicio del correo electrónico en las entidades de Administración Pública", aprobada por resolución Jefatural N° 088-2003-INEI.

4. ALCANCE

4.1. La presente Directica es de **cumplimiento obligatorio por todo el personal que labora en todos las Unidades Orgánicas que conforman el Hospital Regional Docente de Trujillo**, y dicho servicio es administrado por la Oficina de Estadística e Informática, a través del Área Informática.

5. GLOSARIO DE TÉRMINOS

5.1. Buzón: Es la bandeja de entrada, en la cual se almacenan los correos electrónicos.
5.2. Intranet: Es una red privada cuyo propósito es compartir la información del HRDT.
5.3. Listas de Distribución: Son listas de direcciones de correo electrónico, que pueden ser divididas por oficina, direcciones a nivel institucional.
5.4. Software: Equipamiento o soporte Lógico de una computadora que hacen posible la realización de tareas específicas.

5.5. Spam: Son los mensajes no solicitados, no deseados o de remitentes no conocidos, habitualmente de tipo publicitario, enviados en grandes cantidades (inclusive masivo) que perjudican de alguna o varias maneras al receptor.

5.6. Sistema Operativo: Es el programa o conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático, y que permite la normal ejecución del resto de las operaciones (ejemplo el sistema operativo Windows).

5.7. Usuario: Persona que emplea los recursos informáticos (hardware y software) disponibles en el HRDT.

6. DISPOSICIONES GENERALES

6.1. El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información, con la excepción de las listas de interés establecidas por el HRDT para fines institucionales.

6.2. El Área de Informática (A.I.) tiene la responsabilidad de capacitar al personal en el uso del correo electrónico institucional, salvaguardar la información almacenada y brindar información sobre las diferencias, así como de las limitaciones entre el correo electrónico institucional y el correo electrónico privado.

6.3. El tener una cuenta de correo institucional compromete y obliga a cada usuario aceptar las normas establecidas por el HRDT y a someterse a ellas.

6.4. Los usuarios de las cuentas de correo electrónico son responsables de todas las acciones que realizan con las mismas. Cualquier usuario que deje su cuenta de correo abierta en un lugar publico es responsable de todo aquello que se realice desde dicha cuenta.

6.5. Las cuentas de correo electrónico institucional deben ser utilizadas por los usuarios en actividades que estén relacionadas con el cumplimiento de su función en el HRDT.

6.6. La Institución debe garantizar la privacidad de las cuentas de correo electrónico institucional de todos los usuarios.

6.7. El Área de Informática (A.I.) esta autorizada a otorgar cuentas de correo para los proyectos a solicitud de la autoridad competente.

6.8. Las cuentas de correo electrónicos son asignadas únicamente al personal Nombrado, Contratado y/o C.A.S del HRDT.

7. DISPOSICIONES ESPECIFICAS

7.1. DEL BUEN USO DEL CORREO ELECTRONICO.

7.1.1. Nombre de la cuenta de Correo.

- ✓ El nombre de la cuenta de correo electrónico institucional para cada usuario será otorgado por el Área de Informática, generado por el Administrador de Correo Electrónico y tendrá la siguiente estructura: **primera letra del nombre + apellido paterno@hrdt.gob.pe**

Ejemplo:

Usuario: Juan Pérez Pérez
Cuenta correo: jperez@hrdt.gob.pe

- ✓ En caso de existir dos usuarios similares el Administrador de Correo Electrónico, adicionara la letra inicial del apellido materno para la nueva cuenta, diferenciándola, de este modo, de la cuenta homónima. Asimismo, será factible el otorgamiento de alias (ejm.: juan.perez@hrdt.gob.pe) previa coordinación con el Área de Informática bajo el visto bueno de la Oficina de Estadística e Informática.

7.1.2. Uso de Contraseñas.

- ✓ Los usuarios que tienen asignada una cuenta de correo electrónico institucional utilizarán como la contraseña predefinida por el A.I., la misma que deberán cambiarla al primer inicio de sesión y mantener en secreto para que sus cuentas de correo no puedan ser utilizadas por otra persona.
- ✓ Cuando el usuario interrumpa el uso de su estación de trabajo deberá cerrar el software de correo electrónico y activar su protector de pantalla, para evitar que otra persona utilice su cuenta de correo.

7.1.3. Lectura de Correo.

- ✓ Los usuarios que tienen asignada una cuenta de correo electrónico institucional deben mantener en línea el software de correo electrónico (si lo tienen disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.

7.1.4. Mantenimiento de Mensajes de Correo.

- ✓ Todos los correos que se reciban deberán será almacenados en su Carpeta Personal, ubicada en el Disco Duro de su estación de trabajo (D:\Correo), salvo que por necesidades de la función sea necesario almacenar los correos en el Servidor. Caso que debe contar con la respectiva autorización del Área de Informática.
- ✓ Se debe eliminar permanentemente los mensajes innecesarios.
- ✓ Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
- ✓ Al recibir un mensaje que se considere ofensivo, debe ser reenviado hacia el Administrador de Correo Electrónico del HRDT, a fin de que se tomen las acciones pertinentes.
- ✓ La política de respaldo respecto al correo electrónico, es de responsabilidad de las diferencias Unidades Orgánicas del HRDT, la que debe ser coordinada con el Área de Informática para su ejecución.

Envió de Correo.

- ✓ Revisar el texto y la lista de destinatarios antes de enviar un mensaje, para corregir posibles errores de ortografía, forma y fondo.
- ✓ Utilizar siempre el campo **“asunto”** a fin de resumir el tema del mensaje.
- ✓ Expresar las ideas completas con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
- ✓ Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.

- ✓ No utilizar tabuladores, ya que existen softwares administradores de correo que no reconocen este tipo de caracteres, lo que puede introducir caracteres no validos en el mensaje a recibirse.
- ✓ Evitar el uso de la opción de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces provoca demasiado trafico de red.
- ✓ Evitar el envió de mensajes a personas que no se conocen, a menos que sea por un asunto oficial que los involucre.
- ✓ Evitar el envío de mensajes a listas globales, a menos que sea un asunto oficial que involucre al HRDT.

7.1.5. Reenvió de correos.

- ✓ Para el reenvió de un mensaje, incluir el mensaje original, para que el destinatario conozca el contexto en que se esta dando el mensaje que recibe. No incluir ningún archivo adjunto que se pueda haber recibido originalmente, a no ser que se haya realizado modificaciones al(los) archivo(s).

7.1.6. Autofirmas.

- ✓ Todos los correos institucionales deben tener definida la Autofirma del remitente, para efectos de una fácil identificación del usuario dentro de la institución.
- ✓ La Autofirma debe ser breve e informativa, no debiendo ocupar mas de tres líneas.
- ✓ No incluir la dirección de correo en la Autofirma, porque esta ya fue incluida de manera automática en la parte superior del mensaje.

7.1.7. Tamaño de los mensajes.

- ✓ El Área de Informática tiene la responsabilidad de administrar el servicio de correos (en el caso haya un servidor dedicado también es su responsabilidad), en tal sentido, y de acuerdo con la capacidad instalada con la que cuenta, ha determinado un tope de 10Mb para los mensajes salientes; en caso de que la función de algunos usuarios requiera una mayor capacidad, deberá ser coordinado previamente con el jefe del Área de Informática.

7.1.8. Vigencia de los mensajes.

- ✓ Los mensajes en el servidor de correo tendrán una vigencia no mayor de 30 días desde la fecha de entrega o recepción de los mismo. Superado dicho periodo, los mensajes serán eliminados del servidor de correo, salvo que por razones de función amerite su almacenamiento en el servidor, lo cual deberá ser coordinado previamente con el Área de Informática.

7.1.9. Lista de correos.

- ✓ Al enviar un mensaje a una lista o grupo de usuarios, se deberá tener la precaución de revisar que dicha lista este conformada por los usuarios que se desean como destinatarios.

- ✓ Evitar en lo posible el envío de mensajes con archivos adjuntos a grupos de usuarios.
- ✓ Evitar suscribirse por internet a listas ajenas a la función institucional, para no saturar la recepción de mensajes.

7.1.10. Ausencia.

- ✓ En caso de ausencia programada superior a tres (03) días, el titular de la cuenta de correo activa el mensaje de **"Ausencia De Oficina"** para facilitar otra dirección de correo electrónico que garantice la continuidad de la actividad.

7.1.11. Uso del Correo Institucional desde fuera del local de la institución.

- ✓ El Área de Informática, en la solución de correo actual, permite la lectura de los correos electrónicos desde fuera del local institucional a través de un navegador, para lo cual se utiliza el Link denominado "**Correo Institucional**" asociado en la página web del HRDT (www.hrdt.gob.pe), el mismo que está disponible para todos los usuarios de correo.

7.2. DEL MAL USO DEL CORREO ELECTRÓNICO.

7.2.1. Se considera falta grave facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas, los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de servicios de Internet. Asimismo, se considera falta grave el intentar apoderarse o apoderarse de claves de acceso de otros usuarios y acceder y/o modificar mensajes de un usuario que no le corresponde.

7.2.2. Se considera como mal uso del correo electrónico institucional las siguientes actividades:

- ✓ Utilizar el correo electrónico institucional para cualquier propósito comercial o financiero ajeno a la institución.
- ✓ Participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.
- ✓ Distribuir mensajes con contenidos impropios y/o lesivos a la moral.
- ✓ Falsificar las cuentas de correo electrónico.
- ✓ Utilizar el correo electrónico institucional para recoger los mensajes de correo de otro proveedor de Internet.

En el caso del mal uso del servicio de correo electrónico o la detección de irregularidades contra lo establecido por la institución, el **Área de Informática** tomara las medidas pertinentes, pudiendo suspender o cancelar el servicio, con el respectivo informe a la **Oficina de Administración** del HRDT**.**

7.2.3. Se considera, adicionalmente, malas practicas en el uso de correo electrónico:

7.2.3.1. Difusión de contenido inadecuado.

- ✓ Se considera contenido inadecuado a todo lo que constituye complicidad con hechos delictivos, por ejemplo: apología del

terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general. Asimismo, el contenido fuera de contexto en un foro temático.

7.2.3.2. Difusión masiva no autorizada.

- ✓ Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, "spam".

7.2.3.3. Ataques con objeto de imposibilitar o dificultar el servicio, "mail bombing".

- ✓ Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de las líneas, de la capacidad del servidor de correo, o del espacio en disco del usuario.
- ✓ Suscripción indiscriminada a listas de correo. Es una versión de **"mail bombing"**, en que los ataques no vienen de una sola dirección, sino de varias, lo que es mucho más difícil de controlar.

7.3. DE LA SEGURIDAD DEL CORREO ELECTRÓNICO.

7.3.1. Uso del Antivirus.

- ✓ Los antivirus del HRDT, para servidores y estaciones de trabajo, deben activarse de tal forma que se verifiquen todos los archivos, aun los que se encuentren compactados, y la acción por defecto a seguir será la de eliminar del virus automáticamente.
- ✓ El servicio de correo (así como el servidor de ser el caso) deben contar con antivirus para correo. Si el mensaje que detecta contiene un **virus** o **"Troyano"- "caballo de Troya"** que no puede ser removido, debe eliminarse el mensaje inmediatamente. Asimismo, se deberá informar, al destinatario de correo, el nombre del remitente e indicar que su mensaje fue borrado por contener virus.
- ✓ Las estaciones de trabajo se deben revisar en forma constante para evitar remitir virus al momento de enviar documentos adjuntos. En tal sentido, se responsabilizará a los usuarios por los archivos adjuntos que se envíen.
- ✓ El Área de Informática de la Oficina de Estadística e Informática se encargaría de verificar la presencia de virus en el servidor de correo (o al proveedor del servicio de ser el caso) y en forma inmediata procederá a su eliminación tomando las medidas pertinentes.

7.4. DE LA VALIDEZ OFICIAL DEL CORREO ELECTRÓNICO

7.4.1. El HRDT incorpora dentro de sus documentos oficiales el correo electrónico, en tal sentido tiene validez oficial para las gestiones internas de la Institución.

8. DISPOSICIONES COMPLEMENTARIAS

8.1. Las notificaciones institucionales pueden efectuarse mediante correo electrónico conforme al decreto supremo **N° 006-2017-JUS-**Decreto supremo que aprueba el texto único ordenado de la **Ley N° 27444. Ley Del Procedimiento Administrativo General.**

8.2. Los correos electrónicos que apunten documentos que no son propios del remitente, deberán citar siempre la fuente de origen y/o los actores, a fin de respetar los derechos de propiedad intelectual.

8.3. Si se recibe algo cuestionable o ilegal, comunicar a la unidad de informática para que se tomen las acciones del caso.

8.4. La Oficina de administración a través del Área de Recursos Humanos de la Oficina de Personal deberá de comunicar al Área de informática la relación de trabajadores que hayan ingresado a laborar y de ser factibles las listas a las cuales se deben incorporar (**junto con la copia de documento de identidad de cada persona de la lista enviada**). Asimismo, deberá comunicar la relación de aquellos que han dejado de laborar, para proceder a la activación o desactivación de las cuentas de correo respectivas.

8.5. La Oficina de Estadística e Informática a través del Área de informática es responsable de que el personal de la institución cumpla con los dispuesto en la presente directiva.