DIRECTIVA PARA EL CORRECTO USO DEL CORREO ELECTRÓNICO

RED DE SALUD TRUJILLO

1. **Finalidad**
   Fomentar el uso correcto del servicio de correo electrónico institucional.

2. **Objetivo**
   Establecer los lineamientos para el uso correcto del servicio de correo electrónico institucional.

3. **Ámbito de Aplicación**
   La presente Directiva Administrativa es de aplicación en las Oficinas, Unidades Funcionales, Micro Redes y Establecimientos de Salud, que utilicen el correo electrónico institucional de la Red de Salud Trujillo.

4. **Base Legal**
   - Ley Nº 27269 - Ley de Firmas y Certificados Digitales.
   - Ley Nº 27444 - Ley del Procedimiento Administrativo General.
   - Ley Nº 27657 - Ley del Ministerio de Salud.
   - Ley Nº 28493 - Ley que Regula el Uso de Correo Electrónico Comercial No Solicitado.
   - Decreto Supremo Nº 019-2002-JUS, que aprobó el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales.
   - Decreto Supremo Nº 031-2005-MTC, que aprobó el Reglamento de la Ley Nº 28493 - Ley que Regula el envío del correo electrónico comercial no solicitado.
   - Resolución de Contraloría Nº 072-98-CG, que aprobó las Normas de Control Interno para Sistemas Computarizados.
   - Resolución Ministerial Nº 1942-2002-SA/DM, que aprobó la Directiva Nº 001-2002-0GEI: "Normas Generales sobre Acciones de Sistemas de Información, Estadística e Informática en el Ministerio de Salud".
   - Resolución Ministerial Nº 224-2004-PCM, que aprobó el Uso Obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 1° Edición", en todas las Entidades integrantes del Sistema Nacional de Informática.
   - Resolución de la Comisión de Reglamentos Técnicos y Comerciales Nº 0103-2003- CRT-INDECOPI, que aprobó las Disposiciones Complementarias del Reglamento de la Ley de Firmas y Certificados Digitales.
   - Resolución Jefatural N° 207-2002-INEI, que aprobó la Directiva Nº 010-2002-INEI/DTNP: "Normas Técnicas para la asignación de Nombres de Dominio de las entidades de la Administración Pública".
   - Resolución Jefatural Nº 088-2003-INEI, que aprobó la Directiva Nº 005-2003- INEílDTNP sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública".

5. Disposiciones Generales

5.1. El correo electrónico institucional es una herramienta de comunicación e intercambio de información institucional entre personas; no es una herramienta de difusión indiscriminada de información, con la excepción de los grupos de correo establecidos por la institución.

5.2. La asignación de cuentas de correo electrónico institucional se solicitará utilizando el formato de Solicitud de Cuentas de Usuario (Anexo 1). Esta asignación se encuentra supeditada a la aprobación del director de la Oficina de Administración y con el visto del jefe inmediato del área. En esta aprobación, se especifica:

a. Tipo de solicitud
b. Datos del solicitante
c. Firma y V°B° de quienes autorizan.
d. Fecha de la solicitud.

5.3. La cuenta de correo electrónico es personal, individual e intransferible y el contenido de los mismos es secreto. Sólo el usuario autorizado puede acceder a su cuenta de correo. La Red de Salud Trujillo, a través de la Oficina de Informática y Estadística, puede auditar los correos electrónicos ante la presunción de infracciones a la presente directiva. Esta intervención debe ser autorizada por el titular de la entidad o quien asuma sus funciones durante su ausencia.

REGIÓN LA LIBERTAD V°B° GESTIÓN DE LA INFORMACIÓN UTES N° 06 TRUJILLO ESTE

5.4. Las cuentas de correo electrónico son utilizadas para actividades que estén relacionadas de manera directa con el cumplimiento de su función en la institución.

5.5. El usuario que posee una cuenta de correo electrónico institucional está comprometido y obligado a aceptar las normas establecidas por la institución y se somete a ellas.

5.6. El usuario es responsable de respetar la ley del derecho de autor, no utilizando este medio para distribuir o reproducir información protegida por esta ley.

5.7. El usuario sólo podrá acceder al correo electrónico institucional mientras esté vinculado con la institución.

5.8. La Oficina Estadística e Informática es responsable de:

a. Capacitar al personal en el uso del correo electrónico institucional
b. Capacitar al personal en la selección de contraseñas seguras.
c. Disponer las medidas de seguridad necesarias para garantizar la integridad, confidencialidad y disponibilidad del servicio de correo electrónico.

5.9. Se crearán cuentas con los nombres de las Oficinas, Unidades Funcionales, Micro Redes y Establecimientos de Salud de la institución; de existir de cuentas a nombre personal, estas deben estar formado por la letra inicial del nombre de pila del usuario, seguido del apellido paterno, ligado con el símbolo @ al nombre de dominio de la institución. Por ejemplo:

a. Nombre del Usuario: Juan Pérez
b. Nombre de la cuenta: jperez@ristrujillo.gob.pe

En caso de existir dos formaciones de cuenta de correo similares, la Oficina de Estadística e Informática procederá a incluir tantas letras del segundo apellido como sean necesarias en la cuenta de la persona recientemente incorporada. Por ejemplo:

Nombre de Usuario	Nombre de la Cuenta
Juan Pérez Villacorta	jperez@ristrujillo.gob.pe
José Pérez Villavicencio	jperezv@ristrujillo.gob.pe
Jeisson Pérez Villarán	jperezvi@ristrujillo.gob.pe

5.10. Los usuarios de cuentas de correo electrónico son responsables de:

a. El correcto uso sus cuentas de correo electrónico.
b. Depurar constantemente los mensajes del correo electrónico.
c. Cumplir con las normas establecidas por la Red de Salud Trujillo
d. Los mensajes emitidos con su usuario de correo electrónico.
e. No compartir la cuenta de correo electrónico asignada a su cargo.

5.11. La Oficina de Estadística e Informática reportará las faltas cometidas con el correo electrónico a la Dirección Ejecutiva para que ésta tome las medidas necesarias.

5.12. La Oficina de Estadística e Informática debe establecer las medidas de seguridad que permitan evitar el mal uso del correo electrónico institucional, sin transgredir las normas legales vigentes.

5.13. El personal de la Oficina de Estadística e Informática no debe acceder al buzón de correos electrónicos de los servidores. Este acceso será autorizado por el titular de la entidad o quien asuma sus funciones durante su ausencia ante la presunción de falta o trasgresión a la presente directiva.

REGION LA LIBERTAD V°B° OFICINA DE GESTIÓN DE LA INFORMACIÓN UTES N° 06 TRUJILLO ESTE

5.14. Los responsables de Oficinas, Unidades Funcionales, Micro Redes y Establecimientos de Salud, que tienen asignados cuentas de oficina o Micro Red/EESS, al dejar esta responsabilidad, en su entrega de cargo deberán consignar la cuenta y contraseña del correo institucional.

5.15. El personal que asumen la responsabilidad de Oficinas, Unidades Funcionales, Micro Redes y Establecimientos de Salud, al recibir en la entrega de cargo la cuenta y contraseña del correo institucional, inmediatamente deberá de cambiar la contraseña por una de uso a exclusivo.

6. Disposiciones Específicas

Del buen uso del correo electrónico

Uso de contraseñas

6.1. El usuario debe establecer una contraseña para poder utilizar su cuenta de correo. Ésta contraseña es personal e intransferible, no debiendo ser utilizada por otra persona.

6.2. El usuario es responsable de cambiar su contraseña de correo electrónico luego de la notificación de la creación de su cuenta. La elección de la nueva contraseña deberá seguir las recomendaciones propuestas en el anexo 2.

6.3. El usuario que deja desatendido su equipo tomará las medidas necesarias para evitar que otra persona utilice su cuenta de correo electrónico.

Lectura de Correo Electrónico

6.4. El usuario debe leer, de manera obligatoria, su correo electrónico durante su permanencia en la institución. Por este motivo, deben mantener en línea el cliente de correo electrónico que utilicen.

6.5. El usuario debe eliminar los mensajes innecesarios para el normal desarrollo de sus responsabilidades laborales.

6.6. El usuario debe comunicar la recepción de mensajes ofensivos a la Oficina de Estadística e Informática a fin de tomar las acciones respectivas.

6.7. La lectura del correo electrónico es de carácter personal. No se permite la lectura de mensajes por personas distintas al destinatario final. En caso de comprobar

que un usuario de la institución lee o accede al correo electrónico de otro se considerará como falta y será comunicada a la Oficina de Administración para la sanción respectiva.

Envío de Correo

6.8. El usuario debe utilizar el campo "asunto" para resumir el tema del mensaje

6.9. Los mensajes de correo electrónico deberán expresar las ideas completas y de claro entendimiento.

6.10. Enviar mensajes de correo electrónico evitando:

a. El uso indiscriminado de letras mayúsculas
b. El uso de tabuladores
c. El uso indiscriminado de las opciones de confirmación de entrega y lectura, en especial cuando se envíe la información a un grupo de personas.
d. Enviar el mensaje a personas que no conoce.
e. Enviar el mensaje a listas globales, salvo asuntos oficiales.

6.11. El envío de: mensajes globales sólo está permitido a las personas o áreas de la institución que lo requieran como parte de sus funciones laborales.

6.12. Los usuarios no deben iniciar, enviar o responder mensajes de tipo cadena en el correo electrónico institucional.

Reenvío de Mensajes

6.13. El usuario debe incluir el mensaje original cuando reenvíe mensajes de correo electrónico, para que el destinatario conozca el contexto en que se está dando el mensaje que recibe.

6.14. El usuario sólo incluirá mensajes adjuntos en el reenvío de correo electrónico cuando se hayan realizado modificaciones a los archivos.

Autofirmas

6.15. La firma debe ser breve e informativa. no debiendo ocupar más de tres líneas. La firma debe contener la siguiente información:

a. Nombre
b. Cargo
c. Unidad Orgánica o Funcional / Establecimiento de Salud.

6.16. Todo mensaje enviado desde la cuenta de correo electrónico institucional debe incluir la autofirma correspondiente. Esto incluye a mensajes nuevos; respuestas y reenvíos.

Del mal uso del correo electrónico

6.17. Se considera falta facilitar u ofrecer la cuenta y/o buzón de correo electrónico institucional a terceras personas, así como al mal uso del mismo.

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

a. Utilizar el correo electrónico institucional para cualquier propósito ajeno a la institución.
b. Participar en la propagación de mensajes encadenados.
c. Distribuir mensajes con contenidos impropios y/o lesivos a la moral
d. Falsificar las cuentas de correo electrónico
e. Difusión de contenidos inadecuados, como:

- Complicidad con hechos delictivos.
- Difusión de pornografía.
- Emisión de amenazas.
- Planificación o ejecución de estafas (Phising) (Anexo 3).
- Distribución de Malware (Anexo 3).

f. El uso del correo electrónico institucional como reenvío (Relay) de correo para envío de correo personales.
g. Envió de Spam (Anexo 3).
h. Utilizar los recursos de la institución para realizar ataques a cuentas de terceros.

De la seguridad del Correo Electrónico

6.19. El proveedor del servicio de correo electrónico institucional es responsable de:

a. Realizar las copias de respaldo al servidor de Correo Electrónico mediante el procedimiento definido para estos fines.
b. Implementar los medios técnicos necesarios para reducir los riesgos de recepción y envío de Malware, Spam y Phising.
c. Mantener actualizado el antivirus del servidor de correo electrónico.
d. Diseñar los procedimientos de auditoría de correo electrónico institucional.

7. Responsabilidad

La Oficina de Estadística e Informática, es responsable de hacer cumplir las disposiciones establecidas en la presente Directiva Administrativa.

8. Disposiciones Finales

8.1. Las notificaciones complementarias y comunicados institucionales pueden efectuarse mediante correo electrónico.

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

8.3. La Unidad de Recursos Humanos es responsable de entregar a la Oficina de Estadística e Informática la relación de los trabajadores que hayan ingresado a laborar y los que han dejado de hacerlo de manera temporal y permanente con la finalidad de habilitarles o deshabilitarles la cuenta de correo electrónico.

8.4. La Dirección de Administración es responsable de entregar, en el plazo más breve posible, la relación de personas que brindan servicios no personales a la institución a la Oficina de Estadística e Informática indicando, la fecha de término del servicio. Además, deberá comunicar la prórroga del servicio en caso sea necesario con la finalidad de habilitarles o deshabilitarles la cuenta de correo electrónico.

DIRECTIVA ADMINISTRATIVA Nº -

DIRECTIVA ADMINISTRATIVA PARA EL CORRECTO USO DEL CORREO ELECTRÓNICO EN LA RED DE SALUD TRUJILLO

Anexo 1

SOLICITUD DE CUENTA DE CORREO INSTITUCIONAL

TIPO DE SOLICITUD: **ALTA** ☐ **BAJA** ☐

TIPO DE CUENTA: **PERSONAL** ☐ **DE OFICINA/MR/EESS** ☐

DATOS DEL SOLICITANTE:

- **NOMBRES:** .....
- **APELLIDOS:** .....
- **E-MAIL PERSONAL:** .....
- **N° CELULAR:** .....
- **OFICINA/UNI. FUNCIONAL:** .....
- **CONDICIÓN LABORAL:** .....

REGIÓN LA LIBERTAD V°B° OFICINA DE GESTIÓN DE LA INFORMACIÓN UTES A 06 TRUJILLO ESTE

El solicitante abajo firmante, conoce y acepta las condiciones, recomendaciones y normatividad del correo electrónico para la cuenta solicitada.

---------- ----------

SOLICITANTE **RESP. ADMINISTRACIÓN** **V°B° JEFE ÁREA**

Trujillo, ... de ..... del 20.....

DIRECTIVA ADMINISTRATIVA Nº -

DIRECTIVA ADMINISTRATIVA PARA EL CORRECTO USO DEL CORREO ELECTRÓNICO EN LA RED DE SALUD TRUJILLO

Anexo 2

CARTILLA DE RECOMENDACIONES PARA LA ELECCIÓN DE CONTRASEÑAS

"Un password debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente; y no lo compartas con tus amigos."

Cristian F. Borghello.

Introducción

Actualmente todo acceso electrónico que requiere de un usuario autorizado utiliza un mecanismo de contraseñas. Entre los usos más comunes que se le pueden dar a una contraseña encontramos:

- El acceso a cuentas bancarias
- La contraseña de correo electrónico personal
- El acceso a los sistemas administrativos SIGA y SIAF, entre otros.

Las contraseñas, palabras clave o password son el método más común de autenticación personal. Éste se usa para detener el acceso no autorizado a los servicios o equipos informáticos.

La efectividad de las contraseñas se ha cuestionado muy a menudo, principalmente porque pueden olvidarse. robarse o darse a otra persona. Sin embargo, pueden proporcionar una buena medida si son apropiadamente manejados por personas autorizadas a usarlos y si son apropiadamente guardados y procesados en el sistema de comprobación de password.

¿Qué es un password?

Un buen password es una secuencia de caracteres que puede ser usada para muchos propósitos de autenticación. Los password, a menudo son usados para autenticar la identidad de un usuario de un sistema automatizado de proceso de datos y en algunas instancias para garantizar o denegar el acceso a datos privados o compartidos.

Un password debe ser conocido solamente por la persona que lo generó, de esta manera, los sistemas pueden autenticar la identidad de esa persona y brindar los niveles de acceso a la información de los usuarios.

¿Qué es un buen password?

Un buen password, contraseña o palabra clave es uno que es muy difícil de adivinar. Éste llega cumplir los siguientes requerimientos:

- Es fácil de digitar por el usuario al momento de ingresar a los sistemas

- Debe contener al menos 8 caracteres y no más de 64. Se recomienda combinar números y letras en mayúscula y minúscula, de preferencia no repetir los mismos caracteres. La contraseña distingue mayúsculas y minúsculas, por ello deberá de recordar las letras que escribe en mayúscula. En caso de incluir caracteres que no sean alfa-numéricos hay que averiguar primero cuáles son los que el sistema permite.
- Es fácil de recordar para la persona que lo generó. Sin embargo, no es una palabra fácil de adivinar como su nombre o el nombre de sus hijos o el año en el que nació o palabras que se encuentra en algún diccionario de cualquier idioma.
- No es la misma para acceder a todos los sistemas. Esto minimiza el riesgo de ataques o perdidas de información en todos los sistemas.
- Su tiempo de vigencia debe ser menor a 3 meses, con lo que se dificulta la posibilidad de adivinar cual es la contraseña.

Lo que no se debe hacer

Para elegir un buen password, tenga en cuenta la siguiente lista de recomendaciones de lo que no debe hacerse:

- Basar un password en información personal como: el nombre, apodos, fechas de cumpleaños, el nombre de esposa/o, el nombre de su hijo/a, el nombre de animal doméstico que los amigos nombran, el apellido de soltera de las madres, el nombre del pueblo, el número de la casa y el nombre de la calle, número de teléfono, el número de afiliado de la obra social, número de registro de automóvil, etc. Tan poco usar sólo una parte de su nombre, o parte de su fecha de cumpleaños.
- Nunca use un password basado en su nombre de usuario, nombre de cuenta, nombre de login, nombre de computadora o dirección de email.
- Nunca deje que otra persona vea cuando digita su password

Anexo 3

GLOSARIO DE TÉRMINOS

1. **Antivirus**: Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos.
2. **Cliente de Correo Electrónico**: Es un programa de computadora (software) usado para leer y enviar mensajes de correo electrónico.
3. **Correo Electrónico**: Servicio informático, similar al correo postal, que permite a los usuarios enviar y recibir información. Permite el envío de archivos adjuntos con los mensajes.
4. **Gusano (Worm)**: Programa informático de tipo malicioso diseñado para copiarse automáticamente a sí mismo de un equipo a otro.
5. **Malware**: La palabra malware proviene de una agrupación de las palabras malicious software. Este programa o archivo, es dañino para la computadora. Esta palabra agrupa a los Virus, Troyanos, Gusanos y Spyware.
6. **Navegador (Browser)**: Programa utilizado para navegar en Internet. Entre los más conocidos tenemos el Internet Explorer, Netscape Navigator, Opera, Mozilla FireFox.
7. **Phishing**: Es una técnica que busca adquirir información confidencial de forma fraudulenta, mediante una aparente comunicación oficial electrónica enviada por correo electrónico.
8. **Spam**: Mensaje de correo electrónico que se recibe sin haberlo solicitado.
9. **Spyware**: Aplicaciones que recopilan información sobre una persona u organización sin su conocimiento.
10. **Troyano o caballo de Troya**: Programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información y/o controlar remotamente la computadora donde ingreso.
11. **Virus**: Es un programa que puede "infectar" o "contaminar" otros programas al modificarlos para incluir una copia de sí mismo. El código viral es típicamente malicioso y perjudicial para la integridad de la información o del sistema.