Empresa de Correos de Honduras
Gobierno de la República

SECRETARIA DE TRABAJO Y SEGURIDAD SOCIAL
INSPECCION GENERAL DE TRABAJO
RECIBIDO
FECHA: _____ HORA: _____
POR: _____

HONDURAS
GOBIERNO DE LA REPÚBLICA

CC: COPIA DE MEMORANDUM DG-117-2022

MANUAL DE PROCESOS Y PROCEDIMIENTOS DE INFORMATICA Y TECNOLOGIA DE LA EMPRESA DE CORREOS DE HONDURAS (HONDUCOR)

ORGANISMO	ACUSE DE RECIBO
Secretaria de Estado en los Despachos de Trabajo y Seguridad Social / Dirección General de Inspección de Trabajo (DGIT)	SECRETARIA DE TRABAJO Y SEGURIDAD SOCIAL INSPECCION GENERAL DE TRABAJO RECIBIDO FECHA: 18/11/2022 POR: Luis HORA: 2:30 pm
Tribunal Superior de Cuentas (TSC)	TRIBUNAL SUPERIOR DE CUENTAS SECRETARIA GENERAL 18 NOV 2022 NOMBRE: Josy Aguilar HORA: 11:48 am
Oficina Nacional de Desarrollo Integral del Control Interno (ONADICI)	SECRETARÍA DE TRANSPARENCIA ONADICI RECIBE Angelica Martinez FECHA 18/11/2022 HORA 11:56 a.m RECIBIDO
Portal de Transparencia de HONDUCOR / Supervisado por el IAIP	Subido Portal de Transparencia HONDUCOR 18/11/22
SITRAHONDUCOR	Francisco Munguia Pag 2 18/11/2022 COMITE EJECUTIVO PRESIDENTE HONDURAS

EMPRESA DE CORREOS DE HONDURAS

Empresa de Correos de Honduras
Gobierno de la República

HONDURAS
GOBIERNO DE LA REPÚBLICA

MEMORANDUM DG-117-2022

DIRECCIÓN GENERAL DE LA EMPRESA DE CORREOS DE HONDURAS (HONDUCOR)

PARA: ***EMPLEADOS DE LA EMPRESA DE CORREOS DE HONDURAS***

PROCEDENCIA: **COMITÉ DE CONTROL INTERNO DE HONDUCOR**

DOCUMENTO: **MANUAL DE PROCESOS Y PROCEDIMIENTOS DE INFORMATICA Y TECNOLOGIA DE LA EMPRESA DE CORREOS DE HONDURAS (HONDUCOR)**

FECHA: 17 DE NOVIEMBRE 2022

Por este medio me dirijo al equipo de trabajo de la Empresa de Correos de Honduras (HONDUCOR), con el propósito de remitir el MANUAL DE PROCESOS Y PROCEDIMIENTOS DE INFORMATICA Y TECNOLOGIA, y con el propósito de hacer de su conocimiento que se esta realizando la labor de ***redacción, conformación, revisión, sociabilización, aprobación y divulgación*** de los diferentes manuales básicos de cada área de nuestra empresa, mediante un *proceso abierto y transparente que inicia con el borrador básico generado por cada área específica, que posteriormente es sometido a revisión y oportunidades de mejora del resto de áreas pertinentes*, siendo finalmente aprobado por el Comité de Control Interno de la Empresa de Correos de Honduras (HONDUCOR), el cual es conformado por los titulares o representantes de las diferentes áreas que abonan al crecimiento y recuperacion de esta empresa del Estado de Honduras.

Para tal efecto, es obligación de cada jefe o encargado de área poner a la disposición cada manual o reglamento que sea generado, ya que forma parte de la normativa interna y constituye una responsabilidad su obligatorio cumplimiento, conforme al numeral 2) del articulo 36 del Reglamento Interno de Trabajo de la Empresa de Correos de Honduras (HONDUCOR), el cual literalmente establece lo siguiente: *"Realizar personalmente la labor con eficiencia, cuidado y esmero apropiado, en los términos estipulados, en los Manuales de Procedimientos de la Empresa, observar los preceptos de este Reglamento, acatar y cumplir las instrucciones del patrono o su representante dentro de la Empresa, según el orden jerárquico".*

Empresa de Correos
de Honduras
Gobierno de la República

HONDURAS
GOBIERNO DE LA REPÚBLICA

MANUAL DE PROCESOS Y PROCEDIMIENTOS DE INFORMATICA Y TECNOLOGIA HONDUCOR

ENTREGA DE CODIGOS DE SERVICIO

FECHA: ____/ ____/ ____

Oficina o Depto. Receptor: _____

Numeración Inicial	Numeración Final

OBSERVACIONES: _____

_____

_____ _____ _____

Trabajo Realizado por Nombre Firma y Sello

ENTREGA DE CODIGOS DE SERVICIO

FECHA: ____/ ____/ ____

Oficina o Depto. Receptor: _____

Numeracion Inicial	Numeración Final

OBSERVACIONES: _____

_____

_____ _____ _____

Trabajo Realizado por Nombre Firma y Sello

C.c./Archivo

Aeropuerto Toncontín Edificio de Centro de Clasificación Postal, Frente a City Mall
Tegucigalpa MDC, Honduras, C.A.
Teléfonos: (504) 2233-0585, (504) 2237-6353
Sitio Web:

INDICE

1. GENERALIDADES

1.1 INTRODUCCIÓN

El Manual de Políticas de Tecnología de la Información del Correo Nacional de Honduras, representa una importante herramienta que servirá para garantizar el buen funcionamiento de los procesos, para contribuir con su eficiencia, para optimizar los sistemas internos y garantizar la calidad en la gestión, con el objetivo de asegurar la seguridad de las informaciones.

Tiene como finalidad dar a conocer los estándares, normas y políticas de seguridad informática que deberán observar los servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de Honducor.

Se define Tecnología de la Información (TI), a las herramientas y métodos utilizados para recabar, retener, manipular o distribuir información, la cual se encuentra por lo general relacionada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones. En los sistemas de información la ética debe estar presente, por lo que la el Correo Nacional como institución promotora de la ética y la transparencia, espera que el establecimiento de este manual de políticas pueda transparentar y dar idoneidad a los métodos que son utilizados para manejar el uso de la tecnología de la información que dispone la institución.

Con este manual, se pretende trazar los lineamientos bajo la responsabilidad de los usuarios del uso de la misma, a fin de que toda administración en este contexto se realice de una manera clara, precisa, transparente y lo más real posible, donde se respeten los principios éticos que, dentro del marco normativo aceptado por la sociedad, produciendo así una escala de valores de hechos y formas de comunicación dentro de la institución.

Para definir las políticas de TI, fue necesario asegurar una planeación estratégica tomando en cuenta las necesidades presentes y futuras de la institución, considerando como factor principal al capital humano con que cuenta la organización. De esta manera se busca que sus funcionarios y empleados se identifiquen con las políticas establecidas, encauzando sus esfuerzos en el fomento del trabajo en equipo, en la integración y en la coordinación de todas las áreas en una misma dirección.

Conscientes de que el uso de la tecnología electrónica ha transformado a toda la humanidad, pretendemos encauzar la administración de la tecnología de la información de nuestra organización, estableciendo políticas enfocadas a los procesos de la institución y orientadas al logro de los planes, metas y objetivos de la misma, por lo que esperamos que nuestros mayores esfuerzos estén centrados en nuestra Misión y Visión, razón demuestra esencia como Institución y en reforzar nuestros valores éticos y morales para que inspiren nuestros actos.

El Manual de Políticas de Tecnología de la Información del Correo Nacional, ha sido un producto de la participación activa de los funcionarios y empleados de dicha Jefatura de Informática y Tecnología, quienes formularon propuestas de políticas a definir, a fin de hacer

más eficaz su funcionamiento. En lo adelante nos referiremos a los términos de Informática y Tecnología de la Información con las siglas TI.

1.2 POLÍTICAS Y LINEAMIENTOS GENERALES

a) El director(a) General a través de su asesor de sistemas es el encargado de establecer las políticas y lineamientos en materia de informática y tecnología de Honducor.

b) El director(a) General, autorizará la solicitud de compra de dispositivos para los equipos de cómputo.

c) Los privilegios de internet los autoriza el director general, previa nota de solicitud emitida por las jefaturas detallando su uso.

d) El jefe(a) de Bienes Nacionales autorizará la salida de equipos de cómputo de la institución.

e) El jefe(a) de Informática y Tecnología, sólo firmará los diagnósticos, requerimientos, dictámenes técnicos, verificaciones e informes en materia de sistemas de información e informática de la entidad.

f) El jefe(a) de la oficina de prensa, es el responsable de la información que se publique en el portal web institucional www.honducor.gob.hn

g) El manejo de las redes sociales de la entidad será del jefe(a) de prensa.

1.3 OBJETIVOS DEL MANUAL

Los objetivos del Manual de Políticas de Tecnología de la Información para el Correo Nacional, son los siguientes:

a) Crear y definir las políticas generales y específicas que faciliten la ejecución de las actividades de tecnología de la información en las diferentes áreas de la Institución.

b) Promover el uso adecuado de los recursos humanos, materiales y activos tecnológicos adecuados.

c) Normar los procesos de información con la finalidad de mejorar el rendimiento de las áreas de desempeño y de procesos.

d) Establecer las políticas para resguardo y garantía de acceso apropiado de la información de los activos tecnológicos de la institución.

1.4 ALCANCE

El presente Manual abarca las políticas que serán aplicadas en la Institución, a través de la Jefatura de Informática y Tecnología.

1.5 PROPÓSITO

Dejar establecidas las políticas de TI que regirán el uso y mantenimiento de la plataforma tecnológica tanto física como lógica de la institución, para asegurar su operatividad, de manera que los responsables del uso de las tecnologías disponibles, aseguren el cumplimiento de las mismas, con miras al desarrollo de un trabajo óptimo y de calidad.

1.6 AUTORIZACIÓN

El Manual de Políticas de Tecnología de la Información del Correo Nacional de Honduras, es aprobado, previa revisión y verificación del director general del Correo Nacional.

1.7 EDICIÓN Y DISTRIBUCIÓN

La edición se realizará en formato digital, colocándolo en los correos electrónicos institucionales de todas las áreas involucradas para dar fiel cumplimiento al mismo. La versión en físico será encuadernada, a fin de que permita realizar la sustitución de las páginas cuando ocurran revisiones y modificaciones.

Recibirán un ejemplar completo del Manual:
- El director ejecutivo.
- La Jefatura de Informática y Tecnología.
- Departamento de planificación.
- Recursos Humanos.
- Área Legal.
- Auditoría Interna.

1.8 REVISIONES Y MODIFICACIONES

Cualquier cambio, corrección o recomendación se comunicará al Departamento de Planificación, Legal y Recursos Humanos responsables de llevar a cabo revisiones periódicas al documento.

2. POLÍTICAS DE USO ACEPTABLE CORREO ELECTRÓNICO

1. La institución proporcionará el sistema de correo electrónico para ayudar a los empleados en la ejecución de sus trabajos y su uso estará limitado al giro de la institución y bajo sus normas y políticas.

2. No obstante, el uso personal incidental u ocasional del correo electrónico, es autorizado por la institución, en el entendido que los mensajes personales serán tratados igual que los mensajes de la institución.

3. El uso personal del sistema de correo electrónico no deberá afectar el flujo normal de tráfico de correo electrónico relacionado con las labores de la institución. La institución se reserva el derecho a depurar correo electrónico personal para preservar la integridad de los mismos.

4. Ningún empleado, consultor o contratista debe usar el sistema de correo electrónico de la institución en ninguna forma que pueda ser interpretada como insultante, perturbadora, u ofensiva para cualquier otra persona, o institución, o que pueda ser perjudicial para la Institución.

5. Los ejemplos de material prohibido incluyen:

- Mensajes Sexualmente explícitos, imágenes, dibujos o chistes;
- Propuestas desagradables, peticiones de fechas o cartas de amor.
- Blasfemia, obscenidad, calumnias o libelo.
- Difamación étnica, religiosa o racial.
- Opiniones políticas o críticas.

Cualquier otro mensaje que pueda ser interpretado como hostigamiento o menosprecio de otros basados en sexo, raza, orientación sexual, edad, origen, discapacidad o creencias religiosas o políticas.

6. Todo correo electrónico enviado o recibido será, cuando la institución lo considere apropiado, abierto y leído por un funcionario debidamente autorizado de la institución a fin de verificar el uso no apropiado del sistema.

7. No se permite el envío y/o recepción de correos electrónicos relacionados a actividades ilegales.

8. El sistema no debe ser usado para beneficios financieros personales.

9. Los compromisos contractuales no deben ser hechos vía correo electrónico salvo como precursores a una carta formal o Fax.

10. Está estrictamente prohibido el despacho de cartas cadenas. Esto incluye aquellas con propósitos de caridad u otras buenas causas, así como también aquellas que prometen riqueza u otro beneficio personal. Las advertencias de virus están bajo la misma exclusión, la mayoría son falsas, si usted desea verificar la veracidad de estos mensajes, hable con la

Dirección de Sistemas, pero bajo ninguna circunstancia envíe estos mensajes a nadie dentro o fuera de la institución.

11. Ningún mensaje debe ser enviado a más de 20 destinatarios externos. Esto puede ser considerado como "spamming" lo que es una actividad ilegal en muchos países.

12. El usuario conectado al computador será considerado como autor de cualquier mensaje enviado desde ese computador. Recuerde desconectar o cerrar su computador si Ud. se ausenta de su escritorio. Bajo ninguna circunstancia envíe un correo electrónico desde otro computador personal que no sea con su usuario.

13. Usted no debe suscribirse a listas de correos electrónicos no aprobadas por la institución. Los volúmenes de mensajes que pueden ser generados son altos y usted no tiene control sobre los contenidos, lo que puede llevarlo a conflicto con las condiciones señaladas anteriormente.

14. El correo electrónico no debe ser usado para enviar archivos adjuntos de gran tamaño (máximo 10 MB), a menos que sea debidamente autorizado. Muchos sistemas de correo electrónico no tienen capacidad para archivos grandes, de los cuales serán devueltos ocasionando sobrecarga en el sistema de correo electrónico de la institución. Siempre que sea posible, deben usarse discos compactos para o DVD para enviar grandes cantidades de información. No obstante, lo anterior, la Institución se reserva el derecho de asignar mayor o menor cantidad de destinatarios según las funciones del personal.

15. No abra archivos adjuntos a mensajes de correo electrónico a menos que los esté esperando y en ese caso, utilice extrema precaución.

16. La facilidad de remitir automáticamente mensajes no debería ser usada para remitir mensajes a cuentas personales de correo electrónico. La institución proporcionará diversas soluciones para acceder al sistema de correo electrónico de la institución cuando se esté fuera de la oficina.

17. La Jefatura de Recursos Humanos o Legal, deberán informar a esta área sobre cualquier bloqueo de cuentas de correo "previo" a cualquier proceso de investigación o despido de cualquier usuario; esto, para asegurar que la información sea resguardada en todo momento, de lo contrario, el departamento de informática y tecnología queda exonerado de cualquier evento al no ser informado.

18. Las licencias antivirus deberán estar activas, vigentes y actualizadas, para dar cumplimiento a la protección de dicha información.

19. El incumplimiento de las políticas mencionadas en los numerales anteriores, conlleva a una penalización con la inactividad de dicho servicio bajo las normas que se establezcan en el área Legal o Recursos Humanos.

3. ACCESO A LA RED DE DATOS

1. La institución proporcionará acceso a Internet a los empleados autorizados para ayudarlos en el desempeño de sus trabajos. Únicamente para fines laborales.

2. El uso del acceso proporcionado se limitará a los asuntos oficiales de la institución. No obstante, se reconoce que puede haber ocasiones cuando los empleados deseen utilizar Internet por motivos personales, esto se permite durante los descansos para almorzar y antes o después de las horas de trabajo normales, las cuales no interrumpan el proceso normal en el desempeño operativo de los sistemas.

3. No se debe despachar mediante Internet u otro servicio de Red similar ningún mensaje que pueda ocasionar desprestigio de la institución o que pueda hacer que una persona razonable lo considere ofensivo o abusivo. La lista del material prohibido es la misma que para el correo electrónico.

4. Aun cuando usted no deje su nombre, existen otros métodos de identificación, incluyendo la dirección del computador, teléfono, tableta o dispositivo inteligente que esté usando, lo que puede permitir a otros ubicar la institución para la cual usted trabaja, y el computador o dispositivo particular que fue usado para enviar el mensaje. Como parte de las medidas rutinarias de seguridad, todos los sitios visitados están conectados centralmente.

5. Queda terminantemente prohibido acceder a sitios para descarga de programas, música y videos, así como la instalación y uso de programas que faciliten estas descargas. También, queda prohibido el uso de programas que faciliten este tipo de estos procesos, entre otros.

6. El servicio de Internet no podrá ser utilizado para ver videos, escuchar música o conectarse a emisoras de radio publicadas en Internet. en caso de identificar equipos se procederá al bloqueo del mismo e informar a la dirección general y recursos humanos.

7. No se permitirá el uso de mensajería instantánea externa sin autorización o nota emitida y aprobada por la Dirección General por escrito.

8. Usted no debería de comprometerse en ninguna actividad ilegal al usar Internet.

9. El sistema no debe ser usado para beneficios financieros personales, ni para proporcionar un sitio WEB en ningún equipo de la institución sin autorización expresa.

10. El uso del sistema no debe tener un efecto evidente sobre la disponibilidad del sistema para los otros usuarios. Por lo tanto, usted no debería participar en juegos en línea o tener activos cualquier canal de red que difunda frecuentes actualizaciones para su computadora.

11. Usted no debe visitar los sitios Web que desplieguen material de naturaleza pornográfica o que contengan material que pueda ser considerado ofensivo o que pueda infectar de virus y otros programas maliciosos en los equipos, de causar una falla en los equipos de la red por lo antes expuesto, el usuario que se le identifique de tal ilegalidad será sancionado por las normas o procedimientos regidos por el área Legal o Recursos Humanos.

12. Usted no debería bajar ningún archivo de Internet o tomar ninguna imagen desplegada de procedencia dudosa.

13. Usted no debe ingresar innecesariamente a su dirección de correo electrónico en sitio Web de dudosa procedencia. Si usted proporciona su dirección al llenar encuestas u otros cuestionarios, se arriesgará a recibir correos basura no deseados.

14. La persona conectada a un computador será considerada como la persona que navegará por Internet. Usted debe desconectar o cerrar su computador si se aleja de su escritorio.

15. La institución monitorea o registra todos los accesos a Internet y se reserva el derecho de acceso y reporte de esa información.

16. El incumplimiento de las políticas mencionadas en los numerales anteriores, conlleva a una penalización con la inactividad de dicho servicio por medio de la parte Legal y Recursos Humanos.

17. Los Sistemas tanto internacionales como domésticos, tienen sus usuarios y claves de seguridad las cuales, el usuario a quien ha sido entregada será totalmente responsable por el uso del mismo.

18. El acceso a internet por medio de los dispositivos móviles, será de uso exclusivo para acciones o tareas de trabajo en ningún momento personal.

19. Queda terminantemente prohibido realizar llamadas vía WhatsApp, Telegram, Skype u otra plataforma de videollamadas para beneficio personal.

20. Los accesos a internet serán proporcionados únicamente por el personal de informática, queda terminantemente prohibido compartir los accesos por otros medios.

21. El personal de informática se limita a quitar cualquier acceso a internet a todo aquel usuario que se le compruebe que navega de forma fraudulenta a internet en sitios que no son oficiales para la institución, informando a las áreas Legales y de Recursos Humanos sobre lo acontecido.

22. Los accesos a la red cableada o wifi serán autorizados únicamente por medio de nota debidamente autorizada por la Dirección General, Recursos Humanos y Legal, justificando por qué debería proporcionarle el servicio.

4. SOBRE EL USO DEL EQUIPO INFORMÁTICO

4.1 Control de acceso a Sistemas Internacionales y Nacionales

1. Cada equipo de cómputo, deberá tener una cuenta de usuario y contraseña de administrador local y usuario de uso para el acceso al mismo, la cual únicamente será de conocimiento de la persona asignada y ésta no se deberá compartir con ninguna persona.

2. La estructura de una contraseña debe incluir la combinación de caracteres alfabéticos (mayúsculas y minúsculas) y caracteres numéricos.

3. Los accesos a los sistemas deberán ser solicitados y justificados el uso mediante nota escrita por parte de la jefatura que la necesite.

5. RESPONSABILIDADES Y/O PROHIBICIONES DE LOS USUARIOS

El software existente en los equipos asignados a los usuarios y uso de los mismos, estará regido por los siguientes lineamientos:

a) Está prohibido instalar y/o descargar juegos, videos, música ni aplicaciones de ningún tipo de las páginas del Internet, que no guarden relación con la/los procesos operativos de la institución.

b) Está prohibido tener en los equipos archivos que no tengan o guarden relación con el Correo Nacional. Tales como:

- MP3 (u otro formato de música)
- EXE (archivos ejecutables)
- MSI (archivos de instalación)
- JPG; JPEG, GIF, BMP, PNG, ETC (imágenes)
- INI (Archivos de configuración de instalación)
- INF (Archivos de configuración de instalación)
- DLL (librerías de archivos)
- ZIP (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
- RAR (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
- Entre otros

c) Está prohibido tener en los equipos, archivos que no tengan o guarden relación con el Correo Nacional.

d) Está prohibido desinstalar el Antivirus y otras aplicaciones que sean instaladas por el departamento de informática en su equipo, ya que es de alto riesgo para la seguridad ante el peligro de los virus y funcionamiento del mismo.

e) Deberá informar a TI, en caso de presentarse cualquier problema de virus o falla en su equipo informático, por medio de nota o correo electrónico (Medios únicamente oficiales).

g) Los encargados deberán informar a TI cuáles empleados de su área están autorizados para laborar fuera de horario de trabajo.

h) No se podrá instalar o usar equipos tecnológicos que necesiten acceso a la red de datos del Correo Nacional sin previo conocimiento o autorización de la Jefatura de Informática, de no darnos por enterado, esta Jefatura queda exonerada de cualquier inconveniente creado por dicha falta o acontecimiento y dará a conocer a las autoridades competentes dicha falta.

i) A los usuarios que sean entregados equipos tecnológicos, serán responsables del cuidado respectivo de los mismos según normas legales del resguardo de los bienes nacionales.

j) Queda terminantemente prohibido tener cerca de los equipos informáticos líquidos, comidas o cualquier otro producto o material que pueda ser derramado y pueda ocasionar fallas en los mismos, siendo responsable el usuario a quien este cargado dicho bien nacional.

Al ser asignado un activo a un usuario todo lo concerniente al mismo será de su responsabilidad por lo cual:

a) Será responsable de la custodia de los equipos informáticos asignados (PC´s, monitores, teclados, impresoras, USB, etc.)

b) Notificará, vía electrónica o cualquier otra vía los inconvenientes o anomalías presentadas con los equipos, accesorios, impresoras, sistemas, entre otros.

La responsabilidad de los usuarios ante la solicitud de asistencia del área de informática es la siguiente:

a) Solicitará, vía correo electrónico a TI, las solicitudes de modificaciones o servicio técnico, así como cualquier anormalidad en su equipo, con copia a su superior inmediato.

b) Solicitará todos los servicios de soporte tecnológicos, a través de correo electrónico con copia a su superior inmediato. En caso que el equipo no responda, será efectuada, vía nota a la Jefatura de TI.

6. PROCEDIMIENTOS DE INFORMÁTICA Y TECNOLOGÍA.

6.1 PROCEDIMIENTO DE ADMINISTRACIÓN DE CENTRO DE DATOS Y SEGURIDAD INFORMÁTICA:

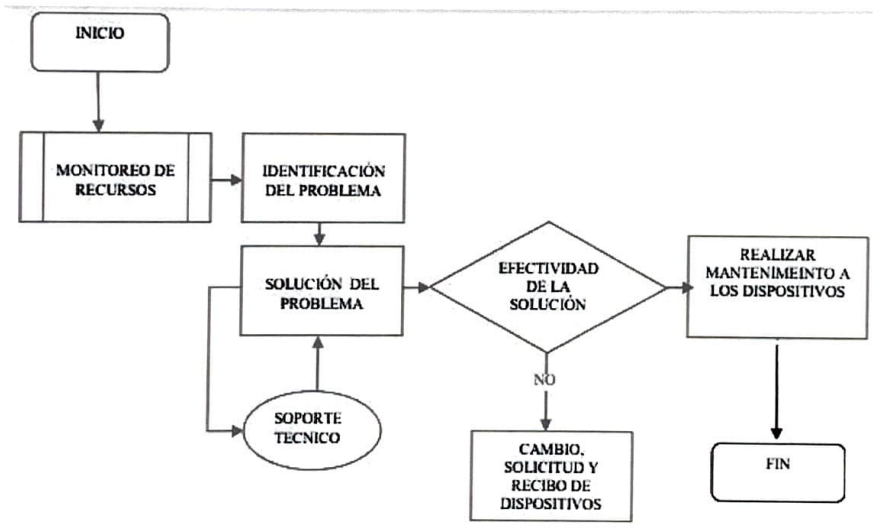
6.1.1 CENTRO DE DATOS Y SEGURIDAD INFORMÁTICA:

6.1.1.1 DESARROLLO DE LAS ACTIVIDADES:

No	RESPONSABLE	DESCRIPCIÓN DE LAS ACTIVIDADES
1	**Informática y Tecnología / Bienes Nacionales**	**MONITOREO DE ACTIVOS TECNOLÓGICOS:** -Se realiza un monitoreo del desempeño de los discos duros en cada uno de los equipos, verificando la velocidad de lectura y escritura y capacidad usada. -Se realiza un monitoreo del desempeño del CPU, verificando el porcentaje de consumo del sistema y las aplicaciones. -Se realiza un monitoreo de los tiempos de respuesta del enlace de internet, también se verifica el ancho de banda consumido por el mismo. -Se realiza una revisión de los diferentes archivos de logs de los equipos para determinar si en el hardware o software se presentan anomalías. -Se realiza una revisión de los enlaces de datos (Internet e Intranet) y los equipos de red (swiches y enrutadores) para detectar posibles fallas o la no disponibilidad operativa de los mismos. -Si los problemas en los discos, la CPU, interfaces de red, equipos de red, y los logs persisten se pasa a la siguiente actividad para su identificación.
		IDENTIFICACIÓN DEL PROBLEMA: **Para los discos duros:** Se verifica que la aplicación no esté generando problema sobre la lectura o escritura del disco. Se verifica que el disco o partición no esté presentado fallos físicos. Se verifica que el disco no esté ocupado al 100% de su capacidad. **Para la CPU:** Se identifica el proceso o procesos que estén generando los mayores consumos de CPU Nota: el valor de uso de CPU varía de acuerdo con el tipo de aplicación. **Para interfaces de red:** Se verifica el consumo de ancho de banda, Dependiendo de este tipo de tráfico se verifica si hay algún problema en los dispositivos de red o si algún equipo o está haciendo uso indebido del ancho de banda. Para equipos de red: Se localiza el equipo de red afectado Se detecta la falla en el equipo o puerto. Para logs: Se identifica el tipo de mensaje reportado, el cual permite establecer sobre qué dispositivo o aplicación se está presentando la anomalía.
3		**SOLUCIÓN DEL PROBLEMA:** Se realizan las correcciones necesarias para el correcto funcionamiento de los dispositivos: discos, CPU, equipos de red, cables y logs. Nota: En algunas ocasiones los problemas presentados en las interfaces de red se deben a clientes de la intranet; para su solución se notifica al auxiliar de Computo para que programen el servicio, revise y corrija el problema presentado por el usuario.
4		**CAMBIO, SOLICITUD Y RECIBO DE DISPOSITIVOS:** En caso de falla de algún dispositivo se verifica: -Si el dispositivo tiene garantía, se verifica el proceso a seguir con el proveedor. -Si la garantía está vigente se contacta telefónicamente al proveedor del

		dispositivo para que diagnostique y sustituya el dispositivo. -Cuando el dispositivo (servidor, equipo de red o componente) no tiene garantía vigente se hace un informe técnico que diagnostique el problema y la solución, se envía a Dirección General para la solicitud de orden de compra, esto se hace a través del formato de requerimientos de dispositivos, se recibe el dispositivo y la salida de almacén, por parte de la Oficina de Almacén. -En el momento en que se realiza la instalación por parte del Auxiliar de Computo, se hace un seguimiento a la instalación y posteriormente se verifica el correcto funcionamiento del mismo. -Se envía un oficio a Bienes Nacionales verificando la entrega a satisfacción del dispositivo.
5		**REALIZAR MANTENIMIENTO A LOS DISPOSITIVOS:** Se hace limpieza y se corren diagnósticos a los dispositivos. (dispositivos y servidores) Se realiza la afinación del servidor, configurando los parámetros óptimos para tener el mejor desempeño del servidor.

6.1.2 FLUJOGRAMA PROCEDIMIENTO DE ADMINISTRACIÓN DE CENTRO DE DATOS Y SEGURIDAD INFORMÁTICA:

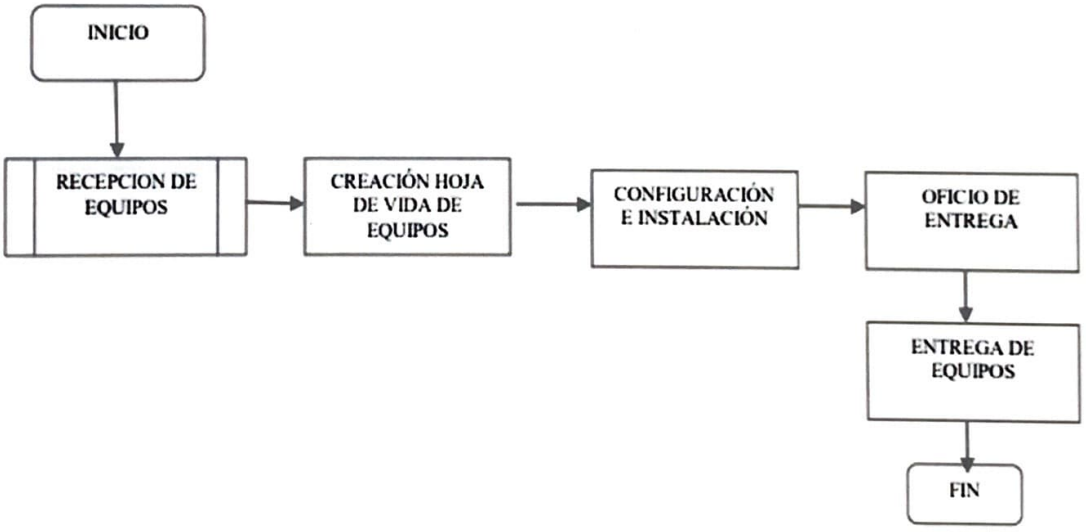


7. PROCEDIMIENTO DE SOPORTE TÉCNICO:

7.1. RECEPCIÓN Y ASIGNACIÓN DE EQUIPOS:

7.1.1. DESARROLLO DE ACTIVIDADES:

No	RESPONSABLE	DESCRIPCIÓN DE LAS ACTIVIDADES
	Auxiliar de Computo	**RECEPCIÓN DE EQUIPOS:** Recibe los equipos solicitados y se verifica que correspondan al pedido aprobado en el plan de compras o por requerimiento técnico de los usuarios.
		CREACIÓN DE HOJA DE VIDA DEL EQUIPO: se crea la hoja de vida respectiva para el control de inventario tecnológico.
		CONFIGURACIÓN E INSTALACIÓN: Configuración e instalación de equipos y entrega a usuarios a satisfacción.
		OFICIO DE ENTREGA: El equipo será recibido para reparaciones técnicas por medio de nota previa, para que una vez reparado o de no tener reparación se realizará oficio de respuesta al usuario.
		ENTREGA DE EQUIPOS: Se entrega el equipo a usuario final a satisfacción en formato de entrega de equipos



7.2 MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE:

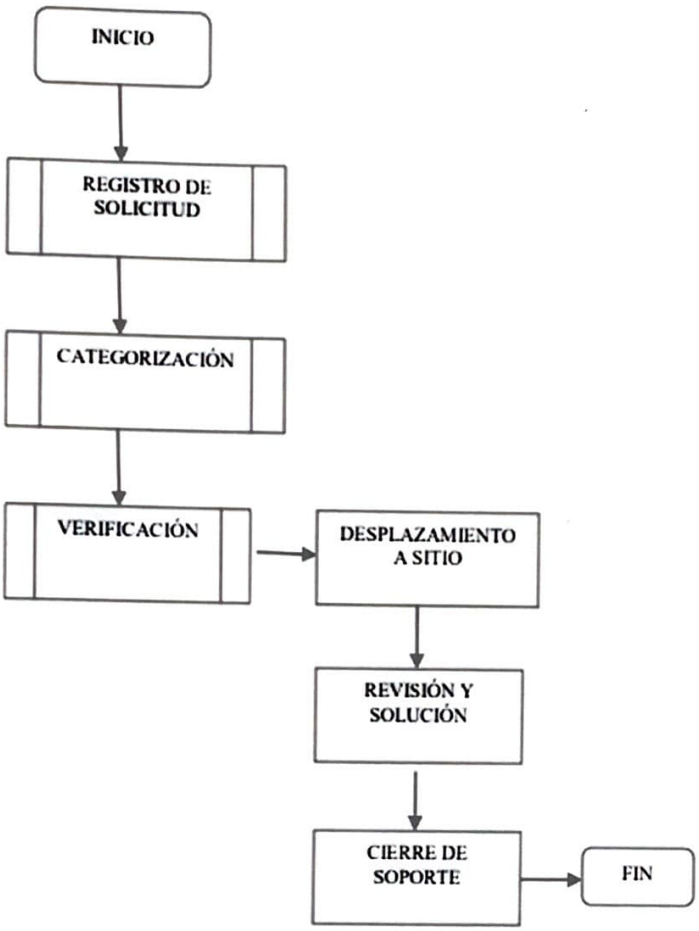
Esta actividad se desarrolla de acuerdo con la elaboración previa de un cronograma elaborado por el asesor de sistemas y aprobado por el director general, el cual se socializa a través de circulares a todos los usuarios. Las evidencias quedan registradas en los formatos de Mantenimiento de software y Hardware.

7.2.1 PROCEDIMIENTO SERVICIO SOPORTE TÉCNICO.

7.2.2 DESARROLLO DE ACTIVIDADES.

No	RESPONSABLE	DESCRIPCIÓN DE LAS ACTIVIDADES
	Usuario	**REGISTRO DE LA SOLICITUD DEL SOPORTE:** Realiza el reporte del incidente o problema, en el formato de solicitud de soporte técnico, La solicitud también puede hacerse por correo electrónico y en el lugar de trabajo se entrega la solicitud de requerimiento.
		CATEGORIZACIÓN Se categoriza la incidencia. Los incidentes pueden ser de soporte técnico a los equipos, conectividad o redes y de Administración del portal web.
		VERIFICACIÓN Los incidentes o problemas serán atendidos por orden de llegada.
		DESPLAZAMIENTO A SITIO: Se desplaza al sitio y evalúa el incidente o problema.
		REVISIÓN Y SOLUCIÓN: Ejecuta las acciones técnicas pertinentes para dar solución al incidente o problema. (Manteniendo correctivo, traslado de equipos y realización de pruebas de funcionamiento.)

7.2.3.2 PR0CESO MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE:



Computadoras: toda computadora propiedad de Honducor la jefatura informática está en la obligación de ser el único el cual puede disponer del Equipo de cómputo en cualquier momento que se requiera, para ello al momento de configurar el equipo tecnológico se crea dos usuarios, el primero es el administrador cuya clave es exclusiva para la jefatura informática, la misma, no se brinda al usuario ya que esta tiene seguridad de que el equipo no sea manipulado por personal externo, también se evita la instalación de software de terceros que podría representar un riesgo de seguridad para la documentación del equipo, así como posibles divulgaciones de virus.

Impresoras: toda impresora propiedad de Honducor la jefatura de informática será garante de su correcto funcionamiento, siempre y cuando no se altere la naturaleza de su trabajo y se intente mejorar o afectar el rendimiento de este.

Impresoras Rentadas: dicho equipo tiene las características de ser un equipo robusto capaz de brindar respuesta a las necesidades de cada jefatura para dichas acciones es necesario la apertura de Tickets en los cuales el arrendador en compañía de la jefatura de IT se apersonará a brindar las soluciones en cuanto a funcionamiento se trata.

Flujo de trabajo

Toda jefatura y/o unidad la cual tenga equipo tecnológico asignado, está en la obligación de notificar mediante correo electrónico o nota por escrito cualquier falla que se presente en el bien tecnológico asignado inmediatamente.

Procedimiento: El no informar/notificar, podría incidir en el daño total del equipo lo que se cataloga como negligencia.

Para un control de seguimiento, la jefatura de informática implementará una hoja de trabajo para llevar un control del equipo, darles seguimiento y llevar un historial de sus fallas; por lo cual, cada usuario que solicite el apoyo de esta jefatura está en la obligación de firmar y sellar la hoja de trabajo al culminar cualquier revisión física o lógica del equipo asignado a su persona.

Al ser notificado de fallas o errores en equipos tecnológicos, el personal de Informática inmediatamente inspeccionará "In Situ" las fallas, para ello se requiere que el usuario brinde un testimonio claro y puntual sobre dicho acontecimiento por lo cual, si el problema atendido está relacionado con el Hardware de dicho equipo, será llevado a la oficina de informática.

·Informática tendrá de 1-5 días para brindar un informe técnico detallado de las fallas del equipo, así como su solución y recomendaciones al usuario y jefatura asignada (dicho diagnóstico está sujeto a que a la jefatura de informática se le brinden todas las herramientas necesarias y se adquieran los repuestos necesarios en tiempo y forma).

·Se le brindara el diagnóstico por escrito al usuario que tiene asignado el equipo tecnológico, el mismo deberá informar a su superior y este deberá solicitar al área administrativa la compra de los materiales y repuestos requeridos.

·La unidad de almacén deberá informar a la jefatura de informática en el momento que ingrese materiales y repuestos para el equipo tecnológico.

·El usuario o su superior deberá solicitar el material de trabajo a la unidad de almacén dicho trámite es necesario para que la jefatura de informática repare dicho equipo.

·Al recibir el material o repuesto la jefatura de informática entregará el equipo tecnológico reparado y en correcto funcionamiento por lo cual el usuario deberá constatar el buen funcionamiento y luego proceder a firmar la hoja de trabajo.

7. INFRACCIONES

Se catalogará como infracciones las siguientes acciones:

1. Quien por medios no autorizados se conecte a la red de Internet de Honducor sin previa autorización por la Jefatura de informática, por lo que:

1. 1 Cualquier persona que requiera acceso para uso exclusivo de asignaciones laborales, deberá solicitar por escrito a esta jefatura el acceso al mismo, informando cuáles serán las funciones por realizar y sitios web que utilizara; dicha autorización deberá venir con el visto bueno de la dirección general de Honducor.

1. 2 Dicho acceso estará sujeto a monitoreo diario de consumo de navegación y ancho de banda utilizada, el cual se bloqueará si su consumo es alto o fuera de lo normal.

2. Cualquier equipo de cómputo que se encuentre compartiendo Internet sin autorización será reportado a la Jefatura de Recursos Humanos y asesoría Legal mismos que implementarán las sanciones correspondientes. Así mismo el usuario que según la unidad de Bienes nacionales sea el asignado será tomado como el responsable de dicha acción siempre y cuando se acredite que esté en funciones dentro de la empresa.

3. Cualquier equipo de cómputo que se encuentre usando software ilegal o no autorizado que sea un problema para la seguridad del equipo y de la red de internet y que no haya sido instalado por esta jefatura, será reportado a la Jefatura de Recursos Humanos y asesoría Legal mismos que implementarán las sanciones correspondientes.

4.Equipos (Laptop, celulares o módems) que sean conectados en la red de Internet sin autorización de la jefatura de informática serán bloqueados y será reportado a la Jefatura de Recursos Humanos y asesoría Legal mismos que implementarán las sanciones correspondientes.

5. Personal que difunda correos de manera malintencionada mismos que puedan ser de peligro para la infraestructura de Honducor la jefatura de IT bloqueará momentáneamente dicha cuenta de correo y se solicitará una investigación para establecer la responsabilidad.

8. AUTORIZACIONES

Se requerirá solicitud por escrito nota a esta jefatura y con el visto bueno de la dirección general para las siguientes acciones:

· Conexión a la red Wifi de Honducor deberá enviar nota firmada por su superior.

· Conexión a la red de Internet al personal que lo requiera para cumplir con asignaciones.

· Conexión a red de internet para charlas y capacitaciones (se deberá informar con 24 horas de anticipación para adecuar la red y el funcionamiento de esta).

9. PROYECCIONES AÑO 2023

· Reemplazar el cable de Internet (UTP) por cable CAT6 en todo el edificio.

· Implementación del sistema doméstico de facturación.

·Implementación de sistema de posición Global GPS en motocicletas para dar seguimiento a los procesos de entrega.

· Implementar realización de proceso de entrega final en el área de distribución.

· Capacitaciones presenciales para la mejora en la digitación en sistema CDS en conjunto con la Jefatura de operaciones.

· Estructuración, diseño y publicación de la APP móvil Honducor (sujeta a la aprobación del presupuesto requerido).

· Contratación de un enlace alterno de conexión a internet, para no detener las operaciones de los sistemas internacionales al momento de fallar el enlace principal entraría el enlace alterno a funcionar.

10. ANEXOS

EMPRESA DE CORREOS DE HONDURAS

Solicitud de Servicios de Informática y Tecnología
Correo Nacional de Honduras HONDUCOR

DATOS GENERALES DEL SOLICITANTE

Nombre Completo: _____ **Código:** _____

Cuenta de Usuario de Dominio: _____

Departamento: _____

Unidad: _____ **Sección:** _____

Horario de Trabajo: _____ **Numero de IP asignada:** _____

SERVICIOS SOLICITADOS

INTERNET:	☐	Justifique uso: _____
Acceso inalámbrico:	☐	_____
Correo Electrónico:	☐	_____
Mensajería Instantánea:	☐	_____
Wifi Teléfono:	☐	_____

DESCARGA DE DATA

User IPS.POST:	☐	Justifique uso: _____
User CDS.POST:	☐	_____
User Facturación:	☐	_____
User Tracker:	☐	_____

ACCESIBILIDAD A SITIOS WEB

Navegador: _____ **Dirección URL:** _____

Justifique uso: _____

_____

_____

AUTORIZACIÓN POR PARTE DEL JEFE DE DEPARTAMENTO

Por este medio, Yo _____, en mi cargo de: _____ hago constar ante el ***Jefatura de Informática y Tecnología*** que he completado la siguiente ***Solicitud de Servicios de Internet*** y que autorizo al solicitante se le habiliten los incisos arriba seleccionados.

FIRMA AUTORIZADA _____

FECHA DE AUTORIZACIÓN _____

<<Depto. de Informática y Tecnología Honducor>>

REPORTE DE TRABAJO REALIZADO

FECHA: ___/___/____

Oficina o Depto.: _____ Equipo Asignado a: _____

Tipo de Equipo: _____

TRABAJO REALIZADO

	Descripción
1.-	
2.-	
3.-	
4.-	
5.-	
6.-	
7.-	
8.-	
9.-	
10.-	

OBSERVACIONES: _____

_____

_____ _____ _____

Trabajo Realizado por Nombre Solicitante Firma y Sello Solicitante

C.c./Archivo

Aeropuerto Toncontín Edificio de Centro de Clasificación Postal, Frente a City Mall
Tegucigalpa MDC, Honduras, C.A.
Teléfonos: (504) 2233-5585, (504) 2237-8242
Sitio Web:

Empresa de Correos de Honduras

HONDURAS

ASIGNACION DE USUARIO IPS.POST

FECHA: ___/___/___

Oficina o Depto.: _____ **Uso de Cta.:** _____

Usuario	Contraseña
HNA-CEASPIXTA1 PSINF1	

OBSERVACIONES: _____

_____

_____

Trabajo Realizado por	Nombre	Firma y Sello
_____	_____	_____

C.c./Archivo

Aeropuerto Toncontín Edificio de Centro de Clasificación Postal, Frente a City Mall
Tegucigalpa MDC, Honduras, C.A.
Teléfonos: (504) 2233-1555, (504) 2237-8255
Sitio Web: [illegible]

Empresa de Correos de Honduras

HONDURAS

ASIGNACION DE USUARIO MacaTRACKER

FECHA: ___ / ___ / ____

Oficina o Depto.: _____ *Uso de Cta.:* _____

Usuario	Contraseña
Tracklm1021	

OBSERVACIONES: _____

_____

_____

_____	_____	_____
Trabajo Realizado por	Nombre	Firma y Sello

C.c.//Archivo

Aeropuerto Toncontin Edificio de Centro de Clasificación Postal, Frente a City Mall
Tegucigalpa MDC, Honduras, C.A.
Telefonos: (504) 2233-3585, (504) 2237-8353
Sitio Web:

Empresa de Correos de Honduras

HONDURAS

CDS CUSTOMS DECLARATION SYSTEM

ASIGNACION DE USUARIO CDS.POST

FECHA: ___/ ___/ ____

Oficina o Depto.: _____ Uso de Cta.: _____

Usuario	Contraseña
HNA_CDPT008	

OBSERVACIONES: _____

_____

_____

Trabajo Realizado por	Nombre	Firma y Sello

C.c.//Archivo

Aeropuerto Toncontín Edificio de Centro de Clasificación Postal, Frente a City Mall
Tegucigalpa MDC, Honduras, C.A.
Teléfonos: (504) 2233-3585, (504) 2237-8353
Sitio Web:

REPORTE DE CAMBIOS EN SITIO WEB

SEMANA DEL: ___ / ___ / ____ AL: ___ / ___ / ____

TRABAJO REALIZADO

Nº.	Descripción (Título)	Imagen	Fecha
1.-			
2.-			
3.-			
4.-			
5.-			
6.-			
7.-			
8.-			

OBSERVACIONES: _____

_____

Trabajo Realizado por	Nombre RRPP	Firma y Sello RRPP

C.c.//Archivo

Empresa de Correos de Honduras

HONDURAS

ASIGNACION DE CUENTA DE CORREO INSTITUCIONAL

FECHA: ___/___/____

Oficina o Depto.: _____ Uso de Cta.: _____

Trabajo Realizado por	Nombre	Firma y Sello

Nota: Con la firma de recepción de credenciales se aceptan las políticas de uso del correo descritas al reverso de este documento.

C.c.//Archivo

Aeropuerto Toncontín Edificio de Centro de Clasificación Postal, Frente a City Mall
Tegucigalpa MDC, Honduras, C.A.
Teléfonos: (504) 2233-3585, (504) 2237-8353
Sitio Web: http://hondurascorreos.hn

POLITICAS DE USO ACEPTABLE
CORREO ELECTRONICO

1.La institución proporcionará el sistema de correo electrónico para ayudar a los empleados en la ejecución de sus trabajos y su uso estará limitado al giro de la institución y bajo sus normas y políticas.

2.No obstante, el uso personal incidental u ocasional del correo electrónico, es autorizado por la institución, en el entendido que los mensajes personales serán tratados igual que los mensajes de la institución.

3.El uso personal del sistema de correo electrónico no deberá afectar el flujo normal de tráfico de correo electrónico relacionado con las labores de la institución. La institución se reserva el derecho a depurar correo electrónico personal para preservar la integridad de los mismos.

4.Ningún empelado, consultor o contratista debe usar el sistema de correo electrónico de la institución en ninguna forma que pueda ser interpretada como insultante, perturbadora, u ofensiva para cualquier otra persona, o institución, o que pueda ser perjudicial para la Institución.

5.Los ejemplos de materia prohibido incluyen:

•Mensajes Sexualmente explícitos, imágenes, dibujos o chistes;
•Propuestas desagradables, peticiones de fechas o cartas de amor.
•Blasfemia, obscenidad, calumnias o libelo.
•Difamación étnica, religiosa o racial.
•Opiniones políticas o críticas.

Cualquier otro mensaje que pueda ser interpretado como hostigamiento o menosprecio de otros basados en sexo, raza, orientación sexual, edad, origen, discapacidad o creencias religiosas o políticas.

6.Todo correo electrónico enviado o recibido será, cuando la institución lo considere apropiado, abierto y leído por un funcionario debidamente autorizado de la institución a fin de verificar el uso no apropiado del sistema.

7.No se permite el envío y/o recepción de correos electrónicos relacionados a actividades ilegales.

8.El sistema no deber ser usado para beneficios financieros personales.

9.Los compromisos contractuales no deben ser hechos vía correo electrónico salvo como precursores a una carta formal o Fax.

10. Está estrictamente prohibido el despacho de cartas cadenas. Esto incluye aquellas con propósitos de caridad u otras buenas causas, así como también aquellas que prometen riqueza u otro beneficio personal. Las advertencias de virus están bajo la misma exclusión, la mayoría son falsas, si usted desea verificar la veracidad de estos mensajes, hable con la Dirección de Sistemas, pero bajo *ninguna circunstancia* envíe estos mensajes a nadie dentro o fuera de la institución.

11. Ningún mensaje debe ser enviado a más de 20 destinatarios externos. Esto puede ser considerado como "spamming" lo que es una actividad ilegal en muchos países.

12. El usuario conectado al computador será considerado como autor de cualquier mensaje enviado desde ese computador. Recuerde desconectarse o cerrar su computador si Ud. se ausenta de su escritorio. *Bajo ninguna circunstancia* envíe un correo electrónico desde otro computador personal que no sea con su usuario.

13. Usted no debe suscribirse a listas de correos electrónicos no aprobadas por la institución. Los volúmenes de mensajes que pueden ser generados son altos y usted no tiene control sobre los contenidos, lo que puede llevarlo a conflicto con las condiciones señaladas anteriormente.

14. El correo electrónico no debe ser usado para enviar archivos adjuntos de gran tamaño (máximo 10 MB), a menos que sea debidamente autorizado. Muchos sistemas de correo electrónico no tienen capacidad para archivos grandes, de los cuales serán devueltos ocasionando sobrecarga en el sistema de correo electrónico de la institución. Siempre que sea posible, deben usarse discos compactos para o DVD para enviar grandes cantidades de información. No obstante, lo anterior, la institución se reserva el derecho de asignar mayor o menor cantidad de destinatarios según las funciones del personal.

15. No abra archivos adjuntos a mensajes de correo electrónico a menos que los esté esperando y en ese caso, utilice extrema precaución.

16. La facilidad de remitir automáticamente mensajes no debería ser usada para remitir mensajes a cuentas personales de correo electrónico. La institución proporcionara diversas soluciones para acceder al sistema de correo electrónico de la institución cuando se esté fuera de la oficina.

17. La Jefatura de Recursos Humanos o Legal, deberán informar a esta área sobre cualquier bloqueo de cuentas de correo "previo" a cualquier proceso de investigación o despido de cualquier usuario; esto, para asegurar que la información sea resguardada en todo momento, de lo contrario, el departamento de informática y tecnología queda exonerado de cualquier evento al no ser informado.

18. Las licencias antivirus deberán estar activas, vigentes y actualizadas, para dar cumplimiento a la protección de dicha información.

19. El incumplimiento de las políticas mencionadas en los numerales anteriores, conllevará a una penalización con la inactividad de dicho servicio bajo las normas que se establezcan en el área legal o RR HH.

El presente documento ha sido revisado y aprobado por los siguientes miembros juramentados del Comité de Control Interno Honducor 2022.

Jimmy Manuel Hernández Aguilar
Jefe de Transporte

Karol Escoto
Jefe de Operaciones

Jenny Waleska López
Coordinadora comercial

Xiomara Yamileth Ramírez
Jefe Administrativo

Marco Antonio Iagos
Coordinador de Créditos y Cobros

Yosselyn Gabriela Bonilla
Asistente de Cuentas Postales

Edry Rebeca Santizo Ramírez
Jefe UPEG

Nividad Flor Mejía
Jefe de Asuntos y cuentas postales Internacionales

Donatilo Reyes Reyes
Jefe Inspectoría General

Priamo A. Alvarado
Jefe Departamento Legal

Armando Cáceres
Unidad de Distribución

Patricia Barahona
Canon Postal

Glenda Ávila
Bienes Nacionales

Yoanna Chapas
Jefe de Relaciones Públicas

Marco Antonio Moreno Calix
Jefe de Informática y Tecnología.

David Orlando Archaga
Coordinador COCOIN

Ramón David Zelaya Flores
Director General Honducor