Tipo de documento: Reglamento	Última actualización: 09/06/2021
Redacción: Manuel Quiroga	Difusión: Interno
Validación: Camilo Vélez	Estatuto:

POLÍTICA DE USO DE ORDENADORES
HI COLOMBIA PROGRAMA COLOMBIA

Contenido

CAPITULO I DISPOSICIONES GENERALES

1. ALCANCE

El presente documento es aplicable a todos los empleados, contratistas, consultores, colaboradores, practicantes, incluyendo a todo el personal externo que en algún momento cuente con acceso a los recursos informáticos o información de La organización. La elaboración de las políticas de tecnología está fundamentada bajo la metodología ITIL, la norma ISO 27000 y las guías del MINTIC.

Las políticas definidas están en concordancia con los estatutos y reglamentos internos de la organización, asegurando la seguridad y optimización de los sistemas tecnológicos brindándole al usuario garantías básicas.

2. OBJETIVO

Brindar la información necesaria a todos los usuarios de tecnología, (directivos, gerentes, empleados) de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red, así como la información que es procesada y almacenada en estos. Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la organización.

3. TÉRMINOS DE USO

Todos los trabajadores de HI COLOMBIA reconocen y aceptan que el uso de ordenadores está expresamente sujeto a las siguientes condiciones:

ORDENADORES

- Son propiedad exclusiva de HI.
- Se confía un ordenador a los trabajadores de HI para su uso con fines profesionales.

CAPITULO II - ADMINISTRACIÓN, CONTROL Y MANTENIMIENTO DE LOS DISPOSITIVOS

4. ADMINISTRACION Y CONTROL

El Logista Base es el responsable de la implementación y el mantenimiento de esta política en su base. También son responsables de garantizar que los dispositivos necesarios estén disponibles. Los ordenadores son equipos estándar que se deben adquirir ir a través del Contrato Marco establecido a

nivel central y por los modelos estándares de la organización. Los proyectos deben solicitar ordenadores a través del Log Base.

El Adjunto Log Manager para Aprovisionamiento asegura que la elección del dispositivo corresponda con las necesidades de los trabajadores de HI.

El Logista Base está a cargo de administrar el mantenimiento y es responsable de almacenar los ordenadores y de mantener un inventario actualizado de los dispositivos.

El Logista base debe tener la hoja de entrega del equipo (Anexo1) por cada ordenador que esté a su cargo.

5. RESPONSABILIDADES DE LOS USUARIOS

- Todos los ordenadores de HI deben estar protegidos por una contraseña (de al menos 6 caracteres), que contengan mayúsculas, minúsculas, números y caracteres espaciales como ¡#*. Etc.
- No se recomienda usar contraseñas donde todos los dígitos sean idénticos (por ejemplo, 1111, 2222 ...), consecutivos (por ejemplo, 1234, 2345 ...), códigos que comiencen con uno o más ceros o códigos basados en números de seguridad social o fechas de nacimiento, placas de automóviles. No se recomienda usar la misma contraseña de ingreso a sitios web.
- Los trabajadores de HI deben respetar y garantizar la confidencialidad de los datos almacenados, procesados o transmitidos a través de los ordenadores de HI. Se implementan varias aplicaciones profesionales en el ordenador de HI (por ejemplo, paquete de office, adobe Reader, 7zip) para fortalecer la seguridad de los datos y cada trabajador de HI debe utilizarlas para procesar datos confidenciales en su ordenador.
- El ordenador asignado es de uso personal por lo tanto cada usuario es responsable de éste y del buen uso que le dé.
- Los usuarios tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- No realizar cambios en las configuraciones de hardware o software instalado en los equipos de cómputo, ya que éste solo se deberá realizar por el área de tecnología informática.
- A no divulgar la clave de acceso ya que esta es de uso personal e intransferible, como consecuencia se entiende para todos los efectos que solo la conoce el responsable del equipo.
- El usuario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al área TI lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las directivas, el usuario informático deberá notificar al área TI.

- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información debe ser reportado al área TI.
- El usuario tiene la obligación de almacenar la información sincronizándola en la herramienta de OneDrive una vez por semana, se recomienda realizar el ultima día laboral de la semana.
- Los usuarios que manejen información crítica de la organización deben realizar la solicitud a Soporte TI para la instalación de la aplicación (QNAP) y realizar el respaldo en nuestro sistema central de BACKUP
- Es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Los usuarios pueden pedir apoyo al departamento de sistemas para el uso de antivirus.
- Los usuarios que tengan archivos que contengan datos personales (lista de contactos / detalles de contacto de personas), deberán protegerlos con contraseña por medio del software AxCrypt y en caso de compartirlos deberán hacerlo por medio de un enlace de SharePoint o canales privados en teams.
- El usuario deberá configurar en su correo la firma estándar de la organización, incluyendo debajo de la firma el aviso de confidencialidad.

6. RESPONSABILIDADES EQUIPO DE SOPORTE

La organización contratará los servicios profesionales para la mesa de ayuda, cuyos funcionarios tendrán las siguientes atribuciones y/o responsabilidades:

- Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del usuario de la computadora, y con los programas remotos autorizados por el área de TI
- Instalación y formación en las herramientas de Backup de la información y definir periodicidad del mismo.
- Asegurar la formación de los usuarios en todas las aplicaciones y herramientas de la organización
- Deben actualizar la información de los recursos de cómputo de la organización, cada vez que adquiera e instale equipos o software
- Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Respuesta a los requerimientos de los usuarios, según los niveles de servicios establecidos, con numero de Ticket hasta el cierre del caso
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar al área de IT los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

7. EQUIPO DE COMPUTO

- La organización proveerá al empleado de un equipo, según los estándares definidos por la misma, para garantizar el correcto funcionamiento del equipo de cómputo deberá realizarse como mínimo mantenimientos preventivos cada 6 meses, de acuerdo con el plan de mantenimiento preventivo elaborado por el área TI.
- El área de TI será el encargado realizar la configuración inicial antes de ser utilizado por el usuario.
- Deberá determinar la vida útil de los equipos de informática, con la finalidad de optimizar su uso.
- El área de TI instalará todas las aplicaciones de los equipos y programas informáticos utilizados por la organización.
- Los logistas deberán informar al área IT una vez adquieran un ordenador nuevo para crear la hoja de vida del equipo.
- Verificará que los proveedores de programas de computadoras suministren los manuales correspondientes al funcionamiento de los equipos o programas especializados.
- El área de TI llevará inventario de hardware y software (programas) instalados en la organización, el cual será revisado en conjunto con el Oficial Técnico Logística y será incluido en el informe de tabla de seguimiento de equipos (TSE).

CAPITULO III -RESPONSABILIDADES Y PROHIBICIONES

8. PROHIBICIONES:

Los trabajadores de HI no están autorizados a:

- Editar el software estándar y la configuración del sistema del ordenador.
- Añadir opción de recuperación alternativa.
- Descargar o usar aplicaciones de fuentes desconocidas o que no sean de confianza.
- Descargar o usar aplicaciones que no pertenezcan a la organización y no tenga previa autorización por operación y el Área de TI.
- Los usuarios no deben interferir en los procesos computacionales de la organización ni en el buen funcionamiento de los servicios y recursos de la misma mediante acciones deliberadas que disminuyan el desempeño, la capacidad o la seguridad de los equipos instalados.
- Está prohibido instalar retirar sellos de los mismos. Lo anterior es responsabilidad exclusiva del área TI, por lo tanto, en caso de requerir este servicio deberá solicitarlo.
- Instalar cualquier software no autorizado por la organización

9. PROCEDIMIENTO PARA DAR DE BAJA/DESECHAR EQUIPO INFORMATICO.

- Elaboración de un certificado de destrucción por parte de HI según Formato de Destrucción (Pestaña SWORN STATEMENT del TSE)

- Adjuntar Certificado de Destrucción por la entidad que recolecta el equipo informático, la cual debe poseer la debida Licencia Ambiental para realizar dichas labores

10. PROCEDIMIENTO EN CASO DE PÉRDIDA O ROBO DE LOS ORDENADORES

- Si su ordenador se pierde o es robado, los trabajadores de HI deben informar inmediatamente al Encargado de Logística, y de acuerdo al análisis de cada caso se definirá la responsabilidad sobre la reposición de le equipo
- Se debe realizar la respectiva denuncia del robo o pérdida ante las autoridades pertinentes del equipo y entregarlo al Logista de base.
- Se debe llenar el formato de perdida que aparece en la Tabla de Seguimiento de equipos (Anexo 2. TSE Pestaña SWORN STATEMENT).

11. BUENAS PRÁCTICAS

SINCRONIZACION DE INFORMACION

- El respaldo de la Información además de ser una buena práctica es una obligación como lo mencionamos en Capitulo 5. Ubique sus archivos en las carpetas en OneDrive, así podrá guardar su información para que de forma automática sea sincronizada en la nube, en dado caso de necesitar ayuda puede solicitar apoyo al departamento IT

ADMINISTRACIÓN DE LA BATERÍA

- Desconecte el cargador una vez la batería esté cargada al 100%.
- Ponga a cargar el computador cuando el indicador encuentre al 15% o menos.
- Apagar WIFI y Bluetooth de no estarlos utilizando.
- No permita que su ordenador se caliente demasiado (no lo deje directamente al sol u obstruya las rejillas de ventilación, no lo ponga sobre sábanas, mantos, cobijas, etc. Que ayuden al recalentamiento del mismo.

12. DERECHOS DE AUTOR

- Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la organización bajo ninguna circunstancia sin la autorización escrita del área de TI.
- Está prohibido cargue o descargue programas informáticos no autorizados de Internet, (Ej. Kazaa,) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor. (debe ir en prohibiciones)
- Está prohibido realizar intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo. (debe ir en prohibiciones)

- Si un usuario desea utilizar programas informáticos autorizados por la organización en su hogar, debe consultar con el área de TI para asegurarse de que ese uso esté permitido por la licencia del editor.
- Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.
- Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.

13. SEGURIDAD

13.1 **Seguridad del recurso humano**

- Todo el personal nuevo de la organización, deberá ser notificado al área TI por la Gerencia RRHH++, de tal forma que se asigne los recursos correspondientes (Equipo de cómputo, creación de usuario para la red, perfil de usuario en el directorio activo) o en caso de retiro, anular y cancelar los derechos otorgados como usuario informático
- El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.
- Todos los usuarios empleados, contratistas y terceras personas deberán devolver todos los activos tecnológicos de la organización que tengan a su cargo a la terminación de su empleo, contrato o acuerdo.

13.2 **Acuerdo de confidencialidad**

Los acuerdos de confidencialidad o no divulgación deben tener en cuenta el requerimiento de proteger la información confidencial, para identificar los requerimientos de los acuerdos de confidencialidad o no divulgación, se debe considerar los siguientes elementos:

- Una definición de la información a protegerse (por ejemplo, información confidencial)
- Responsabilidades y acciones de los de los firmantes para evitar la divulgación de información no autorizada (tal como “sólo lo que necesita saber” para el cumplimiento de su trabajo).
- Propiedad de la información, secretos comerciales know how y propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial.
- Uso permitido de la información confidencial y los derechos del firmante para utilizar la información.
- Las contraseñas de los programas y accesos, son exclusivamente de uso y conocimiento del usuario, por tal motivo, el área de TI las desconoce y cualquier mal uso de los activos de la organización (mal uso en uso de información, por ejemplo), será únicamente responsabilidad del

usuario y podrá ser verificada al ser manipulada por un nombre de usuario. El área de TI, tendrá acceso a la restauración de las claves de acceso si así fuera necesario.

13.3 **Centro de datos**

- El acceso al centro de datos es restringido y solo personal autorizado por el área de TI puede tener acceso a él.
- El acceso a los servidores de la organización ya sea usando la consola de administración local o una consola de administración remota es restringido al personal autorizado por el área de TI
- Asear al menos una vez cada 3 meses, para permitir mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- El Centro de datos debe mantener la temperatura del aire acondicionado entre 18 a 21 grados centígrados para evitar daños en los equipos o en perores casos incidentes relacionados con fuego.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Contar con algún esquema que asegure la continuidad del servicio.
- Contar por lo menos un extintor de incendio adecuado y cercano al centro de datos.
- El centro de datos debe estar libre de líquidos, por derrame o por situaciones ambientales.

13.4 **Seguridad perimetral o red**

- Los equipos electrónicos de gestión e infraestructura de la red de La organización serán instalados, configurados y mantenidos exclusivamente por el área de tecnología informática.
- No es permitido a ningún funcionario, excepto el área de tecnología informática, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).
- El área de TI es la responsable de proporcionar a los usuarios el acceso a los recursos de conectividad.
- El área de TI deberá garantizar la configuración de Firewall perimetral de la red local de la organización, de ser posible, aplicar lo mismo para cada una de las sedes.

12.5 Seguridad de la información

- Uso del Software AxCrypt para la encriptación de archivos y en caso de compartirlos deberán hacerlo por medio de un enlace de SharePoint o canales privados en teams.
- Los usuarios deben guardar la información en las carpetas asignadas y de acuerdo a las tablas de retención documental, en el proceso que corresponda y de acuerdo a la política de archivo, para garantizar que dicha información sea respaldada.
- Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso de los programas y sesiones de Windows.

- No es responsabilidad del área de TI la perdida de información personal que se encuentre en cada equipo, la información debe ser sincronizada en el servidor y/o la nube. (OneDrive).
- Todo acceso a la información de la organización deberá tener las respectivas autorizaciones y accesos, que garanticen su respectiva seguridad, integridad y confidencialidad de la información almacenada.
- Los funcionarios deben realizar revisiones periódicas de su información almacenada con el fin de no mantener información innecesaria.
- Las copias de seguridad o respaldos se deben realizar de acuerdo al plan definido.

14. USO DE INTERNET

En caso de que se identifique que algún acceso que se solicite, amenace la seguridad de la información de la organización, no se concederán los permisos, tales como accesos remotos, VPN externas, carpetas públicas, etc.

14.1 Prohibiciones de internet.

- Páginas con contenido pornográfico.
- Descargue de ninguna aplicación sin autorización del área de tecnología.

15. CORREO ELECTRÓNICO

Teniendo en cuenta que el correo electrónico es una herramienta que provee la organización para el cumplimiento de las funciones, toda la información manejada y almacenada es propiedad de la organización incluyendo las copias de seguridad del mismo. El departamento de RRHH será el responsable de la apertura y cierre de la cuenta. En caso de tener problemas relacionados con el correo el Área de TI será la encargada de dar respuesta al evento.

16. RENOVACIÓN DE EQUIPOS

Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por (5 años) sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de tecnología a fin de que se seleccione el equipo adecuado. Sin el visto bueno de tecnología no podrá liberarse una orden de compra.

Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación

CAPITULO IV - LAS SANCIONES

- La violación a esta política con lleva a una sanción disciplinaria que esta consignada en el Reglamento interno de la Organización.
- El empleado de **HI COLOMBIA** será obligado a aportar o cubrir los daños causados por su propia responsabilidad (negligencia) al utilizar el ordenador, previa investigación debidamente comprobada.

- Pagar los valores adicionales o servicios utilizados no contemplados en el PLAN INSTITUCIONAL.

CAPITULO V - MODIFICACIONES, ENMIENDAS Y LA VIGENCIA

Las modificaciones o enmiendas a esta política, solo se podrán hacer con la autorización de La Dirección de Programa Colombia.

Esta Política entra en vigor a partir de la comunicación de este a todo el personal de HI COLOMBIA, oficina de programa Colombia.

CAPITULO VI -ANEXOS

1. Formato entrega equipamiento (Pestaña Equipment Card del TSE)
2. Formato de Perdida (Pestaña SWORN STATEMENT del TSE)

BIBLIOGRAFIA

• ICONTEC, ISO 27000:2013/ Sistema de seguridad de la información.
• MIN TIC/ Guía No. 3 Procedimiento de seguridad de la información. 25 de abril de 2016.
• ITL, Versión 3