|  |  |
| --- | --- |
| TIPO DE DOCUMENTO | POLITICAS |
| NOMBRE DE DOCTO | USO DE EQUIPOS DE COMPUTO |
| CODIGO | CCIMA\_SR\_IT:FOR\_POL\_USO\_EQUIPOS\_V1.0 |

POLÍTICAS DE USO DE EQUIPOS DE COMPUTO

Se proponen dentro de los siguientes marcos:

- \*\*Alta/baja/cambio de equipo a usuario\*\*: Proceso para asignación y retiro de equipos a usuarios.

- \*\*Uso restringido\*\*: Los recursos deben usarse solo para fines profesionales.

- \*\*Protección de datos\*\*: Cada empleado es responsable de proteger su contraseña y los datos a los que tenga acceso.

- \*\*Seguridad informática\*\*: El uso de software y dispositivos no autorizados está prohibido. Los equipos deben estar protegidos con software antivirus actualizado.

- \*\*Consecuencias\*\*: El incumplimiento de estas políticas puede resultar en sanciones disciplinarias.

Estas políticas se describen a continuación.

**Objetivo**

Dar a conocer los lineamientos de uso de los equipos de cómputo entre los colaboradores de GRUPO CCIMA con el fin de crear un entorno de trabajo seguro, productivo y legalmente compatible, protegiendo tanto los recursos tecnológicos de la organización como la información confidencial que manejan.

**Alcance**

Estas políticas aplican a todos los empleados, contratistas, consultores de GRUPO CCIMA y cualquier otra persona que utilice los equipos de cómputo proporcionados por la organización.

1. **Alta, Baja y Cambio de equipo a usuario**

- RRHH debe dar aviso al área de sistemas del ingreso, salida o cambio de personal para asignación, baja y/o cambio de equipo, accesos, correo y todo lo que el personal requiera para desarrollar la(s) actividad(es) para la(s) cual(es) fue contratado, bajo la normativa que se estipula en el (los) documento(s) que se haga referencia, los cuales pueden ser:

a. **“Procedimiento de asignación, baja y cambio de equipo para usuarios”.**

**b. “Procedimiento de asignación, baja y cambio de cuenta de correo”**

**c. “Procedimiento de asignación, baja y/o cambio de accesos a plataformas”**

1. **Acceso a Internet**

- El acceso a internet debe ser controlado y supervisado para evitar que los usuarios accedan a contenido inapropiado o malicioso.

- El uso de sitios web debe ser monitoreado y restringido según las necesidades laborales.

1. **Seguridad y Protección de la Información**

- Los usuarios deben utilizar contraseñas fuertes y cambiarlas regularmente, con apoyo del departamento de TI.

- Es obligatorio que los dispositivos tengan software de seguridad (antivirus, firewall, etc.) actualizado.

- Se prohíbe el uso de dispositivos externos no autorizados (USB, discos duros externos, etc.) sin la supervisión del área de TI. Los puertos serán bloqueado a menos que haya una indicación directa del gerente del área de TI.

- Los equipos de cómputo deben ser protegidos con bloqueo automático después de un periodo de inactividad, sobre todo cuando el usuario no esté en su lugar o no pueda atender el equipo. Cuando termine su día, se debe cerrar sesión y apagar el equipo, esto con el fin de cuidar la vida útil del equipo.

- El acceso a datos confidenciales debe ser restringido y controlado.

1. **Mantenimiento y Actualización**

- Los equipos deben ser mantenidos en buen estado de funcionamiento, incluyendo actualizaciones periódicas de software y hardware.

- Se debe agendar un mantenimiento al menos 1 vez al año con el área de TI, siguiendo los lineamientos que el área designe para esta tarea.

- Se debe realizar un respaldo de datos regularmente para evitar pérdida de información crítica.

1. **Comportamiento en Línea**

- Los empleados deben comportarse de manera profesional en todo momento cuando usen los equipos de cómputo, ya sea en comunicaciones internas o externas.

- No se debe enviar, compartir ni almacenar material inapropiado, como contenido ofensivo, discriminatorio o que vulnere los derechos de autor.

1. **Protección contra Malware y Ciberataques**

- Los usuarios deben ser capacitados en prácticas de seguridad cibernética, como evitar hacer clic en enlaces sospechosos, descargar archivos de fuentes no confiables o abrir correos electrónicos de fuentes desconocidas.

1. **Monitoreo y Auditoría**

- La organización puede monitorear el uso de los equipos de cómputo y el acceso a la red para asegurar que las políticas sean cumplidas.

- Se realizarán auditorías periódicas para detectar y corregir cualquier incumplimiento de la política.

1. **Consecuencias por Incumplimiento**

- Las violaciones a las políticas de uso de los equipos de cómputo pueden dar lugar a sanciones disciplinarias, que van desde advertencias hasta la suspensión o terminación del empleo, dependiendo de la gravedad de la infracción.

1. **Procedimiento en Caso de Pérdida o Robo**

- En caso de pérdida, robo o daño de un equipo de cómputo, el usuario debe reportarlo inmediatamente al área de TI.

- El equipo debe ser desactivado o borrado remotamente si contiene información sensible.

- La reposición del equipo se hará de acuerdo a las políticas dentro del documento “Resguardo de equipo”.

1. **Confidencialidad**

- Los usuarios deben comprometerse a no divulgar información confidencial a través de medios no seguros, como correo electrónico o aplicaciones no autorizadas.

1. **Formación y Capacitación**

- Los empleados deberán recibir formación periódica sobre el uso adecuado de los equipos de cómputo, las amenazas cibernéticas comunes y las buenas prácticas de seguridad por parte de TI.

GRUPO CCIMA proporciona equipos de cómputo y acceso a internet exclusivamente para fines laborales. Se espera que todos los empleados utilicen estos recursos de manera responsable, siguiendo las normas de seguridad y respetando la confidencialidad de la información.

Yo \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ he leído y acepto las políticas descritas en este documento como parte de mis responsabilidades dentro de Grupo CCIMA en el tiempo en el cual yo forme parte de la plantilla de usuarios y empleados de la misma.

Queda asentado el día \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ que firmo de conformidad.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nombre y firma del usuario

Elabora: Mayra Alejandra Sánchez Chávez.

Puesto: Auxiliar de Sistemas.

Fecha: 20/03/2025

FIRMA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Autoriza: Brenda Jimena Alarcón Vargas.

Puesto: Gerente Area TI

Fecha: 20/03/2025

FIRMA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_