



COMITE
OLIMPICO
GUATEMALTECO

GUÍA
INFORMÁTICA
INF-GUÍA-01
VERSIÓN: 01

ELABORADO POR:

Nombre / Puesto	Fecha	Firma
Msc. Sergio Eduardo Golón Díaz / Director de Informática	28/04/2025	

APROBADO POR:

Nombre / Puesto	Fecha	Firma
Luis Enrique Monterroso Batres / Subgerente de Desarrollo Institucional	30/04/2025	





PROPÓSITO Y ALCANCE DE LA GUÍA

La presente guía tiene como objetivo unificar y organizar los procedimientos relacionados con la gestión de los recursos tecnológicos, seguridad informática y uso de sistemas en el Comité Olímpico Guatemalteco (COG). Esta guía está diseñada para ser utilizada por gerentes, personal técnico y usuarios que necesiten implementar, supervisar y garantizar el correcto uso de las tecnologías de la información en la institución.

PROCEDIMIENTOS RELACIONADOS CON LA MODERNIZACIÓN DE EQUIPOS Y SISTEMAS

Sustitución y Modernización de Equipos

Objetivo: Proveer un procedimiento claro para la sustitución de equipos obsoletos o que no cumplan con los requisitos técnicos.

Responsable: Dirección de Informática.

Acciones:

- Evaluar la funcionalidad de los equipos de manera periódica.
- Priorizar la sustitución de equipos basándose en criterios de obsolescencia y necesidades operativas.
- Proponer la adquisición de nuevos equipos al Gerente General, con las especificaciones técnicas detalladas.
- Realizar la instalación y configuración de los nuevos equipos.

Estandarización de Tecnologías

Objetivo: Asegurar la estandarización de sistemas y tecnologías dentro del COG.

Responsable: Dirección de Informática.

Acciones:

- Realizar una revisión periódica de las tecnologías en uso.
- Definir las tecnologías estándar aprobadas para cada tipo de servicio (sistemas, servidores, estaciones de trabajo).
- Implementar las tecnologías aprobadas y migrar las infraestructuras existentes a los nuevos estándares.

PROCEDIMIENTOS RELACIONADOS CON LA SEGURIDAD FÍSICA

Protección del Centro de Datos

Objetivo: Garantizar la seguridad física de los equipos críticos ubicados en el Centro de Datos.

Responsable: Dirección de Informática.

Acciones:

- Asegurar que el Centro de Datos esté ubicado en un área restringida, con acceso controlado.
- Promover la instalación de extinguidores, aire acondicionado y respaldo eléctrico (UPS).
- Revisar y mantener periódicamente los sistemas de seguridad instalados.
- Monitorear las instalaciones para evitar acceso no autorizado.



Resguardo de Equipos Tecnológicos

Objetivo: Proteger los equipos tecnológicos del COG de amenazas físicas.

Responsable: Todos los usuarios de equipos.

Acciones:

- Prohibir el consumo de alimentos y bebidas cerca de los equipos de cómputo.
- Reportar inmediatamente cualquier incidente o daño relacionado con los equipos tecnológicos.
- Los equipos portátiles solo podrán ser retirados de las instalaciones por los usuarios asignados, y únicamente para fines relacionados con el COG.

PROCEDIMIENTOS RELACIONADOS CON LA SEGURIDAD LÓGICA

Implementación de Firewalls y Antivirus

Objetivo: Proteger la red y los equipos tecnológicos mediante firewalls y antivirus.

Responsable: Dirección de Informática.

Acciones:

- Instalar y configurar firewalls para proteger la red de ataques externos.
- Realizar un monitoreo continuo de las redes de datos para identificar posibles vulnerabilidades.
- Instalar antivirus en todos los servidores y estaciones de trabajo, actualizándolo de manera periódica.
- Proporcionar capacitación a los usuarios sobre las mejores prácticas para evitar infecciones por malware.

Administración de Cuentas de Acceso

Objetivo: Asegurar la adecuada administración de las cuentas de usuario y accesos a los sistemas.

Responsable: Dirección de Informática.

Acciones:

- Crear cuentas de acceso para nuevos colaboradores y cancelar las cuentas de aquellos que ya no pertenezcan a la institución.
- Mantener un registro actualizado de todas las cuentas de acceso a los sistemas y redes.
- Inactivar las cuentas de colaboradores desvinculados sin eliminarlas, garantizando la integridad de la información.
- Realizar auditorías periódicas de las cuentas de usuario para garantizar su uso correcto y seguro.

PROCEDIMIENTOS RELACIONADOS CON EL RESPALDO Y COPIA DE SEGURIDAD (BACKUP)

Backup de Información en Servidores

Objetivo: Garantizar la protección y disponibilidad de la información institucional a través de copias de seguridad.

Responsable: Dirección de Informática.

Acciones:

- Realizar copias de seguridad diarias de las bases de datos, información institucional y archivos de restauración del sistema.



- Utilizar métodos de backup locales y en la nube para asegurar la redundancia de la información.
- Sincronizar los backups con la aplicación de almacenamiento en la nube asociada al correo electrónico institucional.
- Realizar pruebas periódicas para verificar la integridad y accesibilidad de los backups.

Backup de Estaciones de Trabajo

Objetivo: Asegurar la protección de la información almacenada en estaciones de trabajo.

Responsable: Dirección de Informática y Unidades Administrativas.

Acciones:

- Las unidades administrativas deberán llenar el formulario de solicitud para realizar el backup de estaciones de trabajo específicas.
- Las unidades administrativas, podrán realizar un backup independiente utilizando discos duros externos y servidores locales o sincronizándolo con la nube.
- Verificar que el contenido esté libre de malware y cumplir con los estándares de seguridad de la institución.

PROCEDIMIENTOS RELACIONADOS CON EL INVENTARIO Y REGISTRO DE EQUIPOS

Gestión de Equipos Nuevos

Objetivo: Garantizar la correcta asignación de nuevos equipos a los colaboradores.

Responsable: Administrador de Inventarios y Dirección de Informática.

Acciones:

- El Administrador de Inventarios notificará a la Dirección de Informática cuando los equipos sean asignados a los colaboradores.
- La Dirección de Informática realizará las configuraciones necesarias y documentará el proceso.
- Los usuarios notificarán de los cambios y traslados de equipos según el procedimiento respectivo

Descarga de Equipos Obsoletos

Objetivo: Proceder con la descarga del inventario de equipos obsoletos o dañados.

Responsable: Dirección de Informática y Administrador de Inventarios.

Acciones:

- Emitir un dictamen técnico sobre los equipos que ya no sean útiles o que presenten daños irreparables.
- Notificar a los usuarios para que realicen el procedimiento correspondiente de descarga del inventario.
- Actualizar el inventario de la institución para reflejar la baja de los equipos.

PROCEDIMIENTOS RELACIONADOS CON LA SEGURIDAD DEL CORREO ELECTRÓNICO Y USO DE INTERNET

Uso del Correo Electrónico Institucional

Objetivo: Asegurar el uso adecuado del correo electrónico institucional.

Responsable: Dirección de Informática y todos los colaboradores.



Acciones:

- Utilizar la verificación de doble factor para confirmar la identidad del usuario
- El correo institucional se utilizará exclusivamente para comunicaciones relacionadas con las funciones del COG.
- Prohibir el uso del correo para fines personales, propaganda política, comercial o cualquier otra actividad no relacionada con la entidad.
- Depurar regularmente las cuentas de correo y realizar backups de los mensajes enviados y recibidos.

Uso del Servicio de Internet

Objetivo: Regular el uso adecuado del servicio de internet en la institución.

Responsable: Dirección de Informática y todos los colaboradores.

Acciones:

- Restringir el acceso a sitios web con contenido no relacionado con las funciones del COG.
- Monitorear el uso del internet.
- Prohibir el uso del servicio de internet para actividades ilegales o que comprometan la reputación del COG.

PROCEDIMIENTOS RELACIONADOS CON LA CAPACITACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Capacitaciones sobre Nuevas Tecnologías

Objetivo: Brindar capacitación continua al personal del COG sobre el uso de herramientas tecnológicas.

Responsable: Dirección de Informática.

Acciones:

- Realizar capacitaciones cuando se implementen nuevas tecnologías o se actualicen funcionalidades en los sistemas o generar los video tutoriales respectivos.
- Coordinar con la Subgerencia de Talento Humano las capacitaciones para personal de nuevo ingreso.
- Organizar campañas de concientización sobre seguridad informática para prevenir riesgos.

MEDIOS DE SEGUIMIENTO Y EVALUACIÓN

La Dirección de Informática llevará a cabo revisiones periódicas de los procedimientos establecidos en esta guía, asegurando su cumplimiento y actualizando los lineamientos cuando sea necesario.

RESPONSABILIDAD

Es responsabilidad de todas las áreas técnicas y administrativas del COG asegurar la correcta implementación y seguimiento de los procedimientos establecidos en esta guía. La Dirección de Informática será responsable de coordinar y supervisar todas las acciones aquí descritas.



GUÍA
INFORMÁTICA

Proceso: Procesos de Apoyo

Código: INF-GUÍ-01

Versión: 01

Página 6 de 8

GLOSARIO

1	Acceso físico	La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.
2	Acceso lógico	Ingresa al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.
3	Activos de Información	Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.
4	Aplicaciones o aplicativos	Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores, tabletas o celulares.
5	Archivos de Restauración del Sistema	Los archivos de restauración son la copia de las unidades necesarias para que se ejecute el sistema operativo, son la herramienta para recuperar el sistema operativo de un error grave o restaurar el equipo si la unidad de disco duro o el equipo dejan de funcionar.
6	Bases de Datos	Las bases de datos son el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, el COG cuenta con la base de datos de los diferentes sistemas informáticos en uso.
7	Centro de Datos	Área física donde se encuentran resguardados los equipos electrónicos que conforman los sistemas informáticos, así como la infraestructura de apoyo conformado por sistemas de aire acondicionado, sistema de soporte de energía eléctrica (UPS)
8	Certificado de Seguridad SSL	Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.
9	COG	Comité Olímpico Guatemalteco
10	Configuración Lógica	Conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.
11	Contenido	Todos los tipos de información o datos que se divulgan a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.
12	Contraseñas	Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.
13	Copia de máquina virtual del servidor cloud	Es una copia de seguridad del servidor cloud que incluye toda la configuración de la máquina virtual que permite disponer de una forma ágil y sencilla de una solución de respaldo
14	Copia de respaldo o backup	Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.
15	Correo electrónico institucional	Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos, que se encuentra alojado en un hosting de propiedad de la Entidad y servidores cloud. Los cuales pueden usarse en servidores virtuales o adquirir licencias a proveedores de servicios de correo electrónico
16	Cuenta de acceso	Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.



GUÍA
INFORMÁTICA

Proceso: Procesos de Apoyo

Código: INF-GUÍ-01

Versión: 01

Página 7 de 8

17	Dispositivos/Periféricos	Aparatos auxiliares e independientes conectados al computador o la red.
18	Dominio	Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.
19	Espacio en disco duro	Capacidad de almacenamiento de datos en la unidad de disco duro.
20	FADNS	Federaciones o Asociaciones Deportivas Nacionales
21	Firewall / Corta	Es un equipo y/o sistema cuya función es prevenir y proteger la red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que ya entre redes u ordenadores de una misma red.
22	Herramientas ofimáticas	Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas. En el Comité Olímpico Guatemalteco se hace uso de la Herramienta Microsoft Office.
23	Hosting	Un hosting es un servicio de alojamiento web que te permite publicar un sitio web o aplicación en Internet
24	Información / Documento electrónico	Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.
25	Información confidencial	Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.
26	Información Institucional	Entiéndase como información institucional aquella relativa a las operaciones realizadas por cada una de las dependencias del COG, su producción, almacenamiento y gestión está a cargo de cada uno de los colaboradores y contratistas. Información que se encuentra alojada en los equipos de cómputo
27	Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos.
28	Licencia de uso	Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatarario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.
29	Mantenimiento preventivo	Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.
30	Medios de almacenamiento extraíble	Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick).
31	Plataforma web	Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.
32	Recurso informático	Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.
33	Red de datos	Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.



GUÍA
INFORMÁTICA

Proceso: Procesos de Apoyo

Código: INF-GUÍ-01

Versión: 01

Página 8 de 8

34	Riesgo	Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.
35	Servicio informático	Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.
36	Servidor:	Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red, pero también pueden acceder a él a través de la computadora donde está funcionando.
37	Servidores Cloud o Servidores en la nube	Un servidor en la nube es un tipo de servicio de informática en la nube que suelen entregar proveedores de terceros a través de una red accesible, es una potente infraestructura física o virtual que entrega aplicaciones, procesa información o proporciona almacenamiento de datos.
38	Sistema de información	Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
39	Software antivirus	Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocidos como malware.
40	Software de gestión	Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por modulo cruzado de los procesos del negocio.
41	Software malicioso	Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.
42	UPS	Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.