

	SEGURIDAD DE LOS SISTEMAS INFORMATICOS Y CONFIDENCIALIDAD	Elab.	Rev.	Aprob.	Cód.
		TI	SIG	GG	S111-SIG-PO-003
	POLITICA		VF		01 / 15-05-2020

SEGURIDAD 111 se compromete a proteger la información institucional de la organización, por medio del cumplimiento de los procedimientos establecidos y alertando sobre riesgos potenciales. EL Coordinador TI, liderará la revisión, cumplimiento y mejoramiento continuo de la seguridad informática. El Coordinador TI **se** encargará de administrar, asignar y velar por el uso adecuado de los recursos tecnológicos e informáticos, que sean propiedad de **SEGURIDAD 111**. Todos los usuarios que se conecte a la red local de la Organización y al que se le asigne algún recurso informático, queda sujeto a las normas y condiciones contenidas de este documento.

- Los usuarios deben de tener instalado el antivirus con licencia activa. Si por algún motivo el antivirus dejara de funcionar, se debe notificar inmediatamente al Coordinador de TI.
- Las únicas personas autorizadas a realizar cambios en la configuración de las computadoras y redes WiFi es el Coordinador de TI de la Organización.
- Los usuarios con acceso a internet deben hacer uso de este servicio con total responsabilidad y exclusivamente para uso laboral. No para su entretenimiento o distracción.
- El usuario no debe copiar información de la Organización para venderla a algún tercero o el uso mal intencionado de la información que perjudique a la Organización.
- El uso de correo corporativo de la Organización, debe ser para uso exclusivo de la Organización. No cadenas o correo personal.
- Si recibe correos electrónicos de personas no conocidas con archivos adjuntos, no descargarlos ya que potencialmente son virus. Notificar al área de TI para bloquear futuros correos del emisor sospechoso.
- No instalar programas, solo el Coordinador TI es el encargado de la instalación.
- Las contraseñas son de uso personal e intransferible.
- El usuario debe copiar sus archivos importantes en la carpeta asignada, para su posterior Backup.
- Actualización de los sistemas operativo en su última versión (indistinto), con el parche de seguridad de última revisión.
- Actualización de los paquetes ofimáticos (indistinto) con sus licencias actualizadas.
- El acceso de equipo informático personal debe ser bajo estudio y permiso del Coordinador TI.
- Se otorgará el acceso a la información que sea indispensable para el cumplimiento de las funciones asignadas.
- La utilización de hardware (mp3, audífonos, bocinas USB, discos extraíbles, etc.) será únicamente aprobada bajo supervisión del área de TI.
- Los equipos computacionales de la Organización no serán usados para entretenimiento, para ganancia personal, para trabajos o labores externos al uso indicado por la empresa.
- Los usuarios podrán usar los equipos para capacitaciones, practicas, reuniones, etc., siempre y cuando hayan sido aprobadas estas actividades por Gerencia General y el Coordinador TI.
- La instalación de hardware y/ software para actividades de índole necesario serán regidas por S111-TI-P-001 (PROCEDIMIENTO - SEGURIDAD EN SISTEMAS) V03.
- El acceso a las páginas web y redes sociales será solamente para provecho de la empresa.
- Los escritorios de cada equipo deben estar limpio y ordenados con no más de 4 accesos directos, incluido en ellos la papelera de reciclaje.
- A los usuarios que se le permita llevar su equipo portátil a su residencia, debe aplicar lo antes expuesto de igual forma.

Los colaboradores de **SEGURIDAD 111**, tienen la responsabilidad de no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja la Organización, es por ello que se compromete en cumplir con las normativas legales vigentes y los procedimientos de seguridad de los sistemas de información.



Daniel Ortiz Ch.
Gerente General
SEGURIDAD 111 SRL

Lima, 15 de Mayo del 2020

DOCUMENTO CONTROLADO: Este documento es propiedad de SEGURIDAD 111 SRL.
Prohibida su reproducción sin autorización.