POLÍTICA DE SEGURIDAD INFORMÁTICA

Seguridad Las Américas Ltda., dedicada a la prestación de servicios de vigilancia y seguridad privada comprometida con la seguridad de la información desde la alta dirección establece las siguientes directrices relacionadas con el buen uso de los recursos informáticos, preservando la confidencialidad, integridad y disponibilidad de la información.

Esta política promueve las buenas prácticas de seguridad informática para todas las personas que de manera directa o indirecta tienen relación con el hardware y software de Seguridad las Américas Ltda.

Los siguientes lineamientos, son de obligatorio cumplimiento para todas las partes interesadas:

CONFIDENCIALIDAD DE LA INFORMACIÓN

- Las configuraciones de red de los equipos solo podrán ser modificadas por el administrador de la red o personal autorizado.
- Los contratistas que tengan acceso a los equipos de cómputo, bases de datos o archivos digitales deben firmar un acuerdo de confidencialidad y protección de la información.
- Está prohibido extraer información de la compañía sin previa autorización de la gerencia.
- No está permitido compartir información confidencial de la organización a terceros sin previa autorización de la gerencia.
- No se permite guardar información personal en los dispositivos asignados por la empresa para el desempeño de sus labores.
- Reportar al jefe inmediato y al responsable de seguridad informática cualquier evento que pueda comprometer la seguridad de la información y sus recursos informáticos, por ejemplo: virus, daño o pérdida de datos, correos sospechosos y otras actividades inusuales.
- El área de seguridad informática realizará seguimiento y analizará acciones pertinentes cuando se hayan detectado amenazas informáticas.

ACCESO A TECNOLOGÍAS DE LA INFORMACIÓN

- Es responsabilidad del usuario mantener la privacidad y control de los accesos y contraseñas asignados para ingresar a plataformas tales como: correo electrónico, bases de datos, acceso a equipos de cómputo y dispositivos móviles.
- El uso de WhatsApp deberá estar asociado a la línea corporativa y la copia de seguridad deberá estar vinculada a la cuenta corporativa registrada.
- El uso de WhatsApp se limita únicamente a fines laborales y relacionados con el cargo o funciones asignadas.
- No está permitido compartir información confidencial, datos sensibles o estratégicos por WhatsApp sin autorización previa.
- Se deben seguir las políticas de protección de datos personales conforme a la Ley 1581 de 2012 u otras normas aplicables
- El acceso al servidor es restringido, y solo personal autorizado por la gerencia puede tener acceso a él.
- El uso y funcionamiento del correo electrónico corporativo será de uso exclusivo para las tareas o actividades laborales asignadas.
- Las comunicaciones institucionales realizadas por correo electrónico se emitirán únicamente a través de las cuentas de correo corporativas.
- El uso del internet solo estará autorizado para fines laborales.
- Queda estrictamente prohibido reproducir y/o descargar música en cualquier formato en los equipos asignados por la compañía, así mismo, descargar o enviar imágenes, mensajes sexuales, políticos, religiosos o étnicos.
- Todos los puertos USB se encuentran inhabilitados, ya que esto puede ocasionar virus en los equipos y en el servidor.

POLÍTICA DE SEGURIDAD INFORMÁTICA

- Solo la persona encargada de seguridad informática tendrá acceso al RACK.
- Solo se permitirá a terceros el acceso a la red de la organización para las actividades que requieran verificación por parte de entes externos.
- Los usuarios son responsables de mantener su imagen profesional dentro de internet, así como proteger la imagen y reputación de Seguridad las Américas Ltda.

USO DE EQUIPOS DE CÓMPUTO

- Es responsabilidad del usuario el bloqueo de la pantalla del computador cuando no esté en uso.
- Está prohibido utilizar los recursos informáticos (Hardware, Software y datos) y de telecomunicaciones para otras actividades que no estén directamente relacionadas con las funciones del colaborador.
- Está prohibido Instalar cualquier tipo de software en los equipos de cómputo sin previa autorización de la Gerencia Administrativa.
- Está prohibido modificar la configuración del software antivirus, firewall o políticas de seguridad establecidas por la organización. Esta actividad solo puede ser ejecutada por el responsable de la seguridad informática.
- Seguridad las Américas Ltda. Promueve el respeto de los derechos de autor, por lo tanto, no aprueba la instalación, ni el uso de software sin licencia.
- En ninguna circunstancia los empleados de Seguridad las Américas Ltda. Pueden utilizar los recursos informáticos para realizar actividades personales.
- Solo el personal autorizado o responsable de la seguridad informática puede intervenir físicamente en los equipos de cómputo de la organización.
- En caso de requerir el traslado del equipo de cómputo asignado por la empresa, deberá solicitar la autorización por parte de la Gerencia o sus delegados.
- No está permitido llevar al sitio de trabajo computadores portátiles personales, en caso de ser necesario, se requiere solicitar la respectiva autorización.
- Las claves y/o contraseñas de seguridad deberán cumplir los parámetros establecidos en el P-SAM-025 Procedimiento de Seguridad Informática.

CIBERSEGURIDAD

- Evite abrir archivos y enlaces sospechosos que puedan llegar a su correo electrónico.
- No conectar dispositivos a redes Wifi-distintas a las corporativas.
- Se deberá solicitar los permisos correspondientes para conexión remoto desde dispositivos personales u otros.
- El usuario deberá hacer buen uso de plataformas, contenido digital, herramientas de videoconferencia, entre otros durante su jornada laboral.
- El responsable de seguridad informática deberá eliminar el acceso a la información de los colaboradores, terceros y usuarios externos al finalizar su contrato o acuerdo comercial

Representante Legal