

Política de IT & Ciberseguridad - Luría's Burger

Uso de Recursos Informáticos

El uso de los equipos, correo electrónico e internet proporcionados por Luría's Burger se destina exclusivamente a fines laborales. Queda prohibido el uso para actividades ilícitas, descarga de software no autorizado o uso personal excesivo.

Política de Contraseñas

Las contraseñas deben tener un mínimo de 8 caracteres, incluyendo mayúsculas, minúsculas, números y símbolos. No se deben compartir con terceros y deberán cambiarse al menos cada 6 meses.

Correos Electrónicos y Phishing

Todo el personal debe verificar los remitentes de correos antes de abrir enlaces o adjuntos. El departamento de IT nunca solicitará contraseñas por email. Ante la duda, contactar con soporteTI@luriasburger.com.

Instalación de Software

Solo se permite la instalación de aplicaciones autorizadas por IT. El uso de software externo no aprobado podría comprometer la seguridad de los sistemas y será considerado una infracción.

Seguridad en Teletrabajo

Para empleados con modalidad remota, es obligatorio el uso de VPN corporativa, evitar redes Wi-Fi públicas sin protección y mantener los equipos actualizados con antivirus activo.

Protección de Datos Personales

El tratamiento de datos personales se ajusta al Reglamento General de Protección de Datos (RGPD). Queda prohibido transferir datos sensibles por canales no cifrados.

Gestión de Incidencias de Seguridad

Cualquier sospecha de incidente de seguridad (phishing, malware, pérdida de dispositivos) debe ser notificada de inmediato al departamento de IT para su evaluación y respuesta.

Uso de Dispositivos USB

El uso de memorias USB queda restringido a dispositivos verificados y bajo escaneo antivirus previo. No se permite el uso de dispositivos de origen desconocido.

Política de IT & Ciberseguridad - Luría's Burger

Concienciación y Formación

Luría's Burger realizará campañas periódicas de formación en ciberseguridad para todo el personal. Se incluirán cursos básicos y tests de concienciación sobre las principales amenazas digitales.