House Group

Política de Seguridad de Información, Datos y Contraseñas

OBJETIVO

Esta política establece las directrices para la protección de la información sensible, la gestión de datos y el manejo seguro de contraseñas dentro de TI Media Group SL. Su propósito es garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas tecnológicos, minimizando los riesgos de acceso no autorizado, pérdida de datos o vulnerabilidades de seguridad.

Esta política aplica a todos los empleados, contratistas, socios comerciales y cualquier otro tercero que tenga acceso a la información o los sistemas de TI Media Group SL.

GESTIÓN DE INFORMACIÓN Y DATOS

Confidencialidad: La información debe clasificarse según su nivel de confidencialidad (pública, interna, confidencial o altamente confidencial). Cada nivel de clasificación implica medidas de protección específicas que deben ser aplicadas por todos los usuarios autorizados.

Pública	Información en la Web e informes publicados en Internet
Interna	Datos de clientes
Confidencial	Contraseñas, cuentas bancarias, etc.

Acceso Controlado: Solo el personal autorizado podrá acceder a información clasificada. Los niveles de acceso serán gestionados por el equipo de TI Media Group SL en función de las necesidades operativas.

Pública	Empleados y clientes
Interna	Empleados
Confidencial	Personal con acceso al servidor 2

Protección de Datos Personales: Cumpliendo con las leyes y regulaciones locales, seguimos el Reglamento General de Protección de Datos (RGPD) de la Unión Europea se aplica junto con la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que adapta y complementa el RGPD a nivel nacional.

House Group

GESTIÓN DE CONTRASEÑAS

1. **Creación de Contraseñas**
   Las contraseñas deben tener un mínimo de 10 caracteres y combinar letras mayúsculas, minúsculas, números o símbolos.
   Se prohíbe el uso de contraseñas fácilmente predecibles (como "123456", "password", "nombredeusuario", etc.).
   Las contraseñas no deben reutilizarse en múltiples cuentas de trabajo o personales.
2. **Cambio de Contraseñas:**
   Las cuentas nuevas o las contraseñas restablecidas temporalmente deben cambiarse inmediatamente al primer inicio de sesión.
3. **Almacenamiento de Contraseñas**
   Se prohíbe almacenar contraseñas en documentos o archivos no cifrados.
   El cifrado debe aplicarse a todas las contraseñas almacenadas en sistemas internos y bases de datos.

PROTECCIÓN CONTRA PHISHING Y FRAUDES

Para fortalecer la seguridad de la información y reducir el riesgo de ataques de phishing y fraudes electrónicos, todos los empleados deben seguir las siguientes pautas:

1. **Identificación de Correos Sospechosos**
   Verificar el remitente del correo y desconfiar de aquellos con direcciones inusuales o remitentes desconocidos.
   Estar alerta ante correos que soliciten información personal o financiera, especialmente si el mensaje parece urgente o amenaza con consecuencias negativas.
   Desconfiar de enlaces o archivos adjuntos inesperados. En caso de duda, no hacer clic en enlaces ni descargar archivos.
2. **Reportar Intentos de Phishing**
   Cualquier correo sospechoso debe ser reportado al equipo de administración antes de tomar cualquier acción.
   El equipo de administración registrará estos reportes y tomará las medidas necesarias, como bloquear el remitente o alertar al resto del personal.
3. **Autenticidad de Comunicaciones Internas:**
   Todo correo relacionado con temas sensibles (como solicitudes de acceso a sistemas, cambios en información financiera, etc.) será autenticado internamente para confirmar su legitimidad.

House Group

USO DE SISTEMAS Y DISPOSITIVOS

1. **Seguridad en el Acceso**
   Todos los dispositivos (computadoras, teléfonos móviles, tabletas, etc.) que accedan a sistemas corporativos deben estar protegidos por contraseñas y autenticación de dos factores (2FA).
   Se recomienda activar el bloqueo automático de pantalla después de un período de inactividad.
2. **Uso de Redes**
   Se prohíbe el acceso a sistemas de la empresa desde redes públicas o no seguras sin el uso de una conexión VPN segura.
   Los empleados deben desconectar sus dispositivos de las redes corporativas cuando no estén en uso para minimizar riesgos de seguridad.

RESPONSABILIDADES

1. **Empleados**
   Todos los empleados son responsables de cumplir con esta política y reportar cualquier incidente de seguridad o sospecha de actividad sospechosa al equipo de administración, para que puedan gestionar la situación.
2. **Administración**
   La administración debe garantizar que todos los empleados estén informados sobre esta política, además de tomar las medidas necesarias en caso de incumplimiento.

CAPACITACIÓN Y CONCIENTIZACIÓN

Todos los empleados podrán encontrar la información relacionada con las prácticas seguras en el Manual del Empleado, el cual estará disponible para consulta en todo momento.

VIOLACIONES DE SEGURIDAD

Cualquier violación de esta política será tratada con seriedad y puede resultar en medidas disciplinarias, incluyendo la terminación del contrato de trabajo o colaboración, así como posibles acciones legales según corresponda.

REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

Esta política será revisada anualmente y actualizada según sea necesario para garantizar la protección continua contra nuevas amenazas y para cumplir con las regulaciones aplicables.

Fecha: 04/06/2025