POLÍTICA Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

LARM busca garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información de la Compañía y de las partes interesadas, mediante la implementación de políticas, procedimientos y controles que soporten el cumplimiento de la misión corporativa y los estándares legales, regulatorios y contractuales aplicables.

Esta política aplica a todos los aspectos administrativos, de gestión, logísticos y de control de la organización, e involucra a directivos, colaboradores, proveedores, terceros y cualquier persona que tenga acceso a información o activos de LARM.

COMPROMISOS DE LA COMPAÑÍA

LARM se compromete a:

- Cumplir con los requisitos legales y contractuales relacionados con la seguridad de la información.
- Integrar la seguridad de la información en la cultura de gestión de riesgos de la compañía.
- Garantizar que los requisitos de seguridad se incluyan en los procesos contractuales con colaboradores y terceros.
- Sancionar disciplinaria y contractualmente cualquier acción que atente contra la seguridad de la información.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- Confidencialidad: la información solo será accesible a personas autorizadas.
- Integridad: la información será exacta, completa y confiable.
- Disponibilidad: la información estará disponible en el momento y forma que se requiera.
- Privacidad: se protegerán los datos personales conforme a la normativa vigente.

POLÍTICAS ESPECÍFICAS

- Instalación de Software
  - Prohibida la instalación de software no autorizado o sin licencia.
  - Toda instalación debe contar con aprobación de la Dirección y ser realizada por personal de TI.

- Uso de Dispositivos de Almacenamiento Externo
  - Prohibido el uso de dispositivos externos sin autorización.
  - Al finalizar su uso, deben eliminarse los datos, ejecutar limpieza con antivirus y devolver el dispositivo al encargado.

LARM Ecuador
Quito - Ecuador
(593) 987906424
ecuador@larmgroup.com

LARM Colombia
Carrera 13 # 96-67 Of. 607
Bogotá- Colombia
(57)601-7041159| (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

- Uso de Internet y Monitoreo
  - La gerencia puede monitorear y bloquear accesos a sitios inapropiados (contenido sexual, apuestas, sustancias ilícitas, violencia, discriminación, redes sociales, etc.).
  - Está prohibido evadir controles técnicos, realizar ataques informáticos o navegar en páginas no autorizadas.

- Uso del Correo Electrónico y Comunicaciones
  - Prohibido el envío o reenvío de correos con contenido ofensivo, político, discriminatorio, pornográfico o spam.
  - El correo corporativo no debe usarse para fines personales.

- Copias de Seguridad
  - Se realizan respaldos automáticos diarios de bases de datos y archivos críticos.
  - Los responsables de activos deben garantizar la correcta gestión, retención y custodia de copias.

- Almacenamiento de Datos
  - Todos los archivos y documentos corporativos deben almacenarse únicamente en SharePoint.
  - Cualquier excepción requiere autorización del Country director.

- Manejo de Contraseñas
  - Contraseñas de sistema: cambio obligatorio cada 6 meses.
  - Contraseñas de usuario: cambio obligatorio cada 30 días.
  - Deben cumplir con complejidad mínima (8 caracteres, mayúsculas, minúsculas, números y especiales).
  - Prohibido compartir, almacenar en texto plano o enviar contraseñas por medios inseguros.

- Registro de Actividad y Supervisión
  - Todos los eventos, excepciones y fallas quedan registrados y protegidos contra manipulación.
  - Los registros serán revisados periódicamente.

- Acceso a Datos Sensibles de Empleados
  - Limitado al área de Gestión Humana y Dirección General, salvo cargos específicos autorizados.
  - Aplican medidas de seguridad reforzadas.

LARM Ecuador
Quito - Ecuador
(593) 987906424
ecuador@larmgroup.com

LARM Colombia
Carrera 13 # 96-67 Of. 607
Bogotá- Colombia
(57)601-7041159| (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com

- Seguridad de la Información y Recurso Humano
  - Durante procesos de selección, contratación, permanencia y desvinculación, se garantiza la protección de datos personales.
  - Todo colaborador firma acuerdo de confidencialidad.
  - Al finalizar la relación laboral, se revocan accesos y contraseñas asignadas.

- Confidencialidad con Terceros
  - Todo proveedor o aliado debe firmar acuerdos de confidencialidad.
  - El incumplimiento puede dar lugar a sanciones y terminación contractual. (general)

- Selección de Encargados para Transmisión de Datos Personales
  - Se deben evaluar medidas de seguridad, capacidad y políticas del encargado.
  - Se formaliza contrato de transmisión y se realizan auditorías periódicas.

- Revisiones de Seguridad
  - La seguridad informática será revisada periódicamente mediante inspecciones internas y externas.

PROCESO DE ATENCIÓN DE INCIDENTES

Reporte inmediato del incidente a la Dirección con informe en 24 horas.
Notificación a autoridades (cuando aplique, ej. SIC en Colombia).
Reunión con la dirección para análisis técnico, identificación de fallas y adopción de correctivos.

LARM Ecuador
Quito - Ecuador
(593) 987906424
ecuador@larmgroup.com

LARM Colombia
Carrera 13 # 96-67 Of. 607
Bogotá- Colombia
(57)601-7041159| (57) 3123062432
colombia@larmgroup.com
www.larmcolombia.com