

 Risk&Solutions GROUP <i>Seguridad Integral con Calidad</i>	POLÍTICA USO DE SISTEMAS DE INFORMACIÓN Y CIBERSEGURIDAD	FECHA: 04/10/2023
		VERSIÓN: 4
	CÓDIGO: P-SIG-08	PÁGINA: 1 DE 2

Risk & Solutions Group Ltda., propende por garantizar el uso responsable de los Sistemas de Información y de todos sus componentes tanto de Software como de Hardware, es por ello que establece los lineamientos de acceso, modificación y utilización de la información enfocados a mantener adecuados niveles de seguridad y uso de la información. Se adopta el lema: “La seguridad de la información es misión de todos”.

El uso responsable de los Sistemas de Información, está fundamentado desde los pilares de la seguridad de la información, del control de registros, del perfil de nuestros empleados y el respeto por los Derechos de Autor, por ello se encuentra prohibido realizar cualquiera de las siguientes actividades:

- Copiar o distribuir software o su documentación, sin permiso del autor, esto incluye programas, aplicaciones, datos, códigos y manuales.
- Instalar cualquier tipo de Software que no cumpla la Ley 603 del 2000 sobre derechos de autor y Propiedad Intelectual.
- Prestar los programas para que sean copiados, o copiar los programas que han sido adquiridos por la compañía.
- Se prohíbe la extracción de información confidencial de la compañía mediante accesos no autorizados de las bases de datos o el uso de dispositivos de almacenamiento externos.
- Uso de plataformas, contenido digital, herramientas de videoconferencias, comercio electrónico, entre otras, que no sean autorizadas por la empresa
- Hacer uso inadecuados de los recursos asignados al desempeño de sus funciones.

Con el fin de garantizar los principios de confidencialidad, integridad y disponibilidad aplicable a la información que maneja Risk & Solutions Group Ltda, tanto en medio físico como magnético, se establece los siguientes lineamientos que todos los colaboradores y terceros con acceso a esta, deben cumplir:

- Cuidar y usar la información a la cual tiene acceso, solo para propósitos del negocio.
- Mantener absoluta reserva y confidencialidad sobre la totalidad de la información, documentos, inventos, proyectos, iniciativas, servicios, resultados de exámenes de polígrafo, investigaciones de seguridad, validación de documentos de identidad, estudios de seguridad, incidentes de seguridad, procesos, programas y procedimientos de seguridad, claves de acceso o password y cualquier tema relacionado con RSG, sus clientes y asociados, que tenga conocimiento o acceso en razón de los trabajos o servicios que realice.
- Presentar, exhibir, divulgar o dar a conocer de cualquier forma información y/o documentación confidencial a terceros no autorizados, para lo cual se requiere autorización por escrito del Representante Legal o Gerente de Área de la empresa.
- Todos los recursos informáticos proporcionados para soportar la ejecución normal de las actividades y el procesamiento de la información, son propiedad de Risk & Solutions Group Ltda., y deben ser usados para propósitos del negocio, las personas que tienen acceso a la información, tienen responsabilidades inherentes a ese hecho que deben conocer y cumplir dichas responsabilidades que están definidas en función del rol que desempeñan en el manejo de la información.
- Toda persona que tenga bajo su responsabilidad un proveedor o contratista, es responsable de identificar los riesgos de la información que va a manejar y tener identificados los controles adecuados para mitigarlos antes de solicitar la autorización de acceso.
- Todos los acuerdos con proveedores o contratistas que implican acceso, procesamiento, comunicación o gestión de los activos de información de Risk & Solutions Group Ltda., deben considerar todos los componentes de la presente política, para velar por la seguridad de acuerdo con lo establecido por la empresa.
- Todas las personas deben considerar el tema de seguridad antes de suministrar información a los clientes o terceros, de los activos de información de Risk & Solutions Group Ltda.

	POLÍTICA USO DE SISTEMAS DE INFORMACIÓN Y CIBERSEGURIDAD	FECHA: 04/10/2023
		VERSIÓN: 4
	CÓDIGO: P-SIG-08	PÁGINA: 2 DE 2

- Todos los colaboradores y proveedores Risk & Solutions Group Ltda., que tengan acceso a los activos de información, y que requieran contraseña, tienen la responsabilidad de gestionarla y asegurar que no sea expuesta o revelada a personas no autorizadas.
- Todos los empleados y proveedores de Risk & Solutions Group Ltda., deben reportar a su Jefe Inmediato cuando tenga más accesos de los que le corresponde y deben velar porque esta información sea restringida, de acuerdo a la presente política.
- Es responsabilidad de todos los colaboradores, proveedores y contratistas de RSG comunicar cualquier comportamiento inadecuado con relación al manejo de contraseñas, equipos desatendidos, ingresos a sitios no autorizados o cualquier situación irregular con los activos de información, que se considere se encuentran expuestos a personas no autorizadas y/o en riesgo.
- Todos los colaboradores, proveedores y contratistas de RSG deben hacer uso adecuado de los servicios de red a los que específicamente tenga acceso, y este relacionado con el desempeño de su trabajo.
- Todos los colaboradores, contratistas y proveedores de RSG que por su rol tengan información relacionada con los clientes, proveedores, terceros o los mismos empleados son responsables de protegerla.
- Todos los colaboradores, contratistas y proveedores de RSG deben cumplir con los lineamientos que se tengan frente al acceso y uso de la información con derechos de propiedad intelectual.
- Todos los empleados, contratistas y proveedores de RSG, deben tener en cuenta que solo el personal autorizado por Tecnología de la Información, son los encargados de realizar instalaciones de software o hardware en equipos o máquinas pertenecientes a RSG, garantizando así que estos tengan las debidas licencias.
- Todo empleado de RSG que tenga bajo su responsabilidad personas o proveedores que manejen sistemas de información, deben reportar la finalización de contrato a las áreas que generan los accesos para el retiro de los mismos.
- Devolver y/o hacer entrega a RSG toda la información de carácter de confidencialidad como los programas, proyectos, contratos, convenios, exámenes de polígrafo y sus resultados, investigaciones de seguridad, estudios de seguridad, procesos y procedimientos de seguridad y toda la información y/o documentación de cualquier naturaleza a la que tenga acceso en forma directa o indirecta en razón o con ocasión de los servicios prestados a RISK & SOLUTIONS GROUP LIMITADA, sus clientes o asociados de negocio.
- Se podrá divulgar la información confidencial siempre que exista un requerimiento legal o de autoridad competente, para lo cual se debe notificar previamente y por escrito al representante legal de RSG con la información sobre el requerimiento correspondiente y solo se podrá divulgar si RSG lo autoriza.

POLITICAS DE CIBERSEGURIDAD

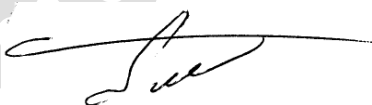
en una empresa son fundamentales para proteger los activos digitales, la información confidencial y garantizar la continuidad del negocio. A continuación, se mencionan las políticas de ciberseguridad que se implementan en nuestra empresa.

1. **Políticas de contraseñas seguras:** establecer requisitos para la creación y actualización regular de contraseñas fuertes, que incluyan una combinación de letras, números y caracteres especiales. Además, se deberá exigir la no reutilización de contraseñas antiguas y la utilización de autenticación de dos factores cuando sea posible, todas estas políticas son necesarias en nuestra web, en correos, redes sociales, y aplicativos corporativos que sean de conectividad y tengan contacto con nuestra data interna, esto con la supervisión del Líder T.I.
2. **Política de acceso y privilegios:** definir los niveles de acceso y privilegios de los empleados en función de sus roles y responsabilidades. Solos se les debe proporcionar acceso a los recursos necesarios para realizar su trabajo, y se deben revisar y actualizar periódicamente los permisos de acceso, los privilegios de conectividad externa son limitados, solo se darán con el consentimiento de la gerencia administrativa.

	POLÍTICA USO DE SISTEMAS DE INFORMACIÓN Y CIBERSEGURIDAD	FECHA: 04/10/2023
		VERSIÓN: 4
	CÓDIGO: P-SIG-08	PÁGINA: 3 DE 2

3. **Política de uso aceptable de recursos informáticos:** Las pautas claras sobre el uso adecuado de los recursos informáticos de la empresa, incluyendo la prohibición de actividades no autorizadas, como descargue de software ilegal, visita a sitios web no relacionados con el trabajo o el intercambio de información confidencial.
4. **Política de seguridad de redes:** las medidas de seguridad necesarias para proteger la red corporativa, como la utilización de firewalls, detección y prevención de intrusiones, cifrado de datos y segmentación de la red para limitar el acceso no autorizado.
5. **Políticas de protección de datos:** la protección de datos confidenciales de la empresa y sus clientes, esto puede incluir el uso de cifrado de datos, la implementación de controles de acceso, la clasificación de datos según su nivel de confidencialidad y la notificación de incidentes de seguridad.
6. **Política de uso de dispositivos móviles:** las prácticas de seguridad que deben seguirse al utilizar dispositivos móviles, como el cifrado de datos, la instalación de software de seguridad y la notificación inmediata en casos de pérdida o robo de un dispositivo corporativo o con datos de la compañía.
7. **Políticas de educación y concienciación:** se generarán boletines programas de formación y concienciación en ciberseguridad para todos los empleados. Esto les ayudara a comprender los riesgos asociados con las amenazas cibernéticas y a adoptar practicas seguras en su trabajo diario en su labor empresarial.
8. **Política de respuestas a incidentes:** plan de respuesta a incidentes que describa los pasos a seguir en caso de una brecha de seguridad o un ataque cibernético. Esto incluye la notificación a el líder TI. En el momento de percibir un ataque o una filtración maligna para la información de la compañía, desconectar nuestro equipo de la red.

Risk & Solutions Group Ltda., ha definido esta política para cumplimiento de todos sus empleados, contratistas y proveedores y velará por su cumplimiento.



JOSÉ CORTÉS CARDOSO
Representante Legal

Cualquier copia de este documento será considerada como copia no controlada