POLTICA DE SEGURIDAD DE LA INFORMACION

El objetivo de este Política es en RISKS INTERNATIONAL S.A.S, regular la gestión de la seguridad de la información al interior de La empresa, para la cual es importante establecer directrices que propendan por la seguridad de la información que se maneja en la empresa, en cumplimiento a la normatividad legal vigente, que establece la seguridad y a la protección de datos Habeas Data, según la ley 1266 del 2008, la Ley 1581 del 2012 y el decreto 1377 del 2013. Estas están soportadas en los procedimientos internos que se desarrollan al interior de la empresa, la Política de tratamiento de datos, Política de clasificación de la información, manuales y reglamentos, autorizaciones físicas y electrónica para consulta y reporte ante operadores de información.

ALCANCE: Aplica a todas las áreas, procesos y servicios desarrollados por RISKS INTERNATIONAL S.A.S

Desde: El aviso de privacidad establecido en la página web, donde se promocionan los servicios, dando cumplimiento como expertos normativos, estableciéndose, determinando que para acceder a información, se requiriere de autorización dando cumpliendo con los principios, derechos y deberes que rigen el proceso informático frente a los datos, que son objeto de recolección, obtención, compilación, modificación, administración, procesamiento, intercambio, envío, divulgación y transferencia, a cualquier título, de la información contenida en las bases de datos públicas.

Hasta: Administración de los documentos en archivos correspondientes, atendiendo los procedimientos y políticas preestablecidas por la empresa, protegiendo el uso de las medidas técnicas, humanas y administrativas que sean necesarias, para otorgar seguridad de la información, previniendo riesgos y evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

1.LINEAMIENTOS GENERALES PARA PROTEGER LA INFORMACIÓN DE NUESTROS CLIENTES Y DE LA ORGANIZACIÓN

a. GESTIÓN DE ACTIVOS DE INFORMACIÓN RISKS INTERNATIONAL S.A.S, Establece la importancia de la información confiable, veraz y completa que a través del uso de las plataformas y en cumplimiento de los requerimientos a satisfacción de los clientes y partes interesadas. Por lo anterior maneja, utiliza, en sus procedimientos, captura, almacena, suministra datos, estableciendo los mecanismos de protección de los datos, conforme a la normatividad legal vigente.

b. GESTIÓN DE RIESGO DE LA INFORMACIÓN. RISKS INTERNATIONAL S.A.S, Guardando los más altos estándares y protocolos de seguridad, establecidos en sus buenas prácticas, establece la confidencialidad de los activos de la información, con los colaboradores, clientes, proveedores, que van a ser usuarios de la información y se soporta en Políticas como la de Tratamiento de la información, clasificación de la información y comunicación, manuales y reglamentos; por lo anterior también ha establecido una matriz de riesgos y un plan de contingencia que permita minimizarlos.

2. IMPLEMENTACION DEL SISTEMA DE SEGURIDAD DE LA INFOMACION EN RISKS INTERNATIONAL S.A.S

2.1. ESTABLECER RESPONSABILIDAD EN EL OFICIAL DE SEGURIDAD DE LA INFORMACION:

2.1.1. Es quien responderá ante la Gerencia Ceo y Subgerencia, por el cumplimiento de seguridad de la información, en el desarrollo de todos los procesos que establezca la empresa, como usuarios operadores de información**.**

2.1.2. Establece el cumplimiento normativo legal de la protección de datos personales y sensibles, para lo cual estará actualizará permanentemente, las nuevas normas que surjan al respecto.

2.1.3. Establece un plan de capacitación, socialización y motivación, para que los usuarios operadores de información den un correcto manejo a la misma.

2.1.4. Supervisa y audita, que se implementen las siguientes políticas, manuales y el plan de contingencia de la empresa en temas relacionados con la seguridad de la información, promoviendo la mejora continua:

a. OGE-005 Política de comunicación

b.OGE-007 Política de clasificación de la información

c.OGE-008 Política de Tratamiento de datos

d.MGE-002 Manual de procedimientos para el tratamiento y protección de datos personales

e.MGE-003 Manual SAGRLAFT

f. MGE-004 Manual de Políticas y procedimientos para el tratamiento de datos

g.REG-001 Reglamento de datos sensibles.

2.2. RESPONSABLE DE LA DIRECCION DE LA POLITICA

La Gerencia CEO y Subgerencia, son comprometidos con los clientes y partes interesadas en la construcción e innovación de plataforma y prestación de servicios con los más altos estándares de calidad, bajo el precepto de prevención de riesgos, a través de:

a. Establecer directrices de estándares de seguridad del acceso, manejo de la información, apoyando este proceso con la asignación de recursos adecuados para implementar, mantener las políticas de seguridad de la información, que generen confianza, satisfacción del cliente y las partes interesadas, toda vez que se brinda un servicio confiable, bajo los preceptos normativos.

b. Determinar el nivel de protección de la información, estableciendo reglas de entrega de las contraseñas de usuario, entregadas por la Gerencia CEO y Subgerencia, a los colaboradores, la cual se cambia cuando este se encuentra incapacitado o se retira permanentemente de la empresa. Una vez está en proceso de separación de la empresa el área de Administrativo y Financiero, revisará los elementos que entrega y dará un Paz y Salvo, al colaborador, de que los equipos que entregan están en óptimas condiciones.

c. Desarrollo de la promoción de las buenas prácticas hacia una activa cultura de seguridad de la información, haciendo monitoreo de consultas; de igual forma, se genera un control de seguridad de la información cuando se registran cambios.

d. Asignación de responsabilidades de custodia operativas: A través de restricción, controles y análisis de riesgos, para preservar la información de las plataformas, a través del área tecnológica, para que los funcionarios en horas laborales hagan un uso responsable de los servicios y equipos proporcionados por la empresa.

e. La información clasificada como reservada o restringida, que genere certificación de confiabilidad de los sistemas de almacenamiento de la información, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio, para lo cual se creó un instructivo acorde al nivel de clasificación de los activos que permite el sistema de cifrado de información para brindarle mayor seguridad, administrando el software o herramienta utilizado para tal fin, la administración de llaves de cifrado.

f. La Gerencia CEO y Subgerencias, dispondrá controles que restrinjan el uso de medios de almacenamiento removibles, que impidan copiar información (USB, Unidad CD, disco duro externo), por lo que solo ellos elaborarán una copia de respaldo mensual de información Back up, la cual la realiza la Gerencia CEO, o Subgerencia, esta información será almacenada y guarda fuera de la empresa, donde estará disponible cuando se requiera, con control físico y medioambiental, que cumpla la norma de integridad y disponibilidad.

g. Se estableció para los colaboradores que No se deben almacenar videos, fotografías o información personal.

h. Registro y monitoreo de parte de la Gerencia CEO, como coactar del diseño de las plataformas y aplicativos establecerá monitoreo, protección para accesos no autorizados a través de mecanismos de control de acceso lógico, que emitan alarmas de control, al igual ordenará, la aplicación de las buenas prácticas en la utilización de las mismas para la prestación del servicio, evitar accesos no autorizados a los sistemas administrados.

2.3. RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

a. Conocer y dar aplicabilidad a las directrices y normatividad legal vigente, en materia de seguridad de la información, establecidas por la empresa en el manejo de las plataformas. Por lo anterior ayudaran a identificar y establecer los riesgos de los activos que regula la información que manejan desde cada puesto de trabajo.

b. Se dispone de un mecanismo para enviar la información cifrada establecida a través del Instructivo de procedimiento para cifrar archivos IFF-002, por ser de clasificada como confidencial y que por su evaluación de riesgo sea necesario usar este tipo de control, usando la clave privada previamente establecida con los clientes, lo que garantiza la identidad del emisor y receptor de la información que ha sido generada, procesada, almacenada y transmitida desde sus plataformas tecnológicas. La responsabilidad de este procedimiento estará a cargo de los jefes de área sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen su uso es confiable.

c. Tener en cuenta las normas de buen uso de acceso a redes y recursos de las redes, sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, por lo que los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la empresa, se harán mediante autorización por parte de la Gerencia CEO y Subgerencia, quienes serán los que asignan las claves para su ingreso. Por lo anterior cuando se enferma o se retira de la empresa definitivamente el colaborador, se bloquean los usuarios.

d. Los colaboradores, en el acuerdo de confidencialidad que firman, se comprometen a no compartir con nadie sus cuentas de usuario y contraseñas, por lo que serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido, de acuerdo con las políticas establecidas en protección de datos personales y sensibles, generados en la empresa. De esta forma apoyaran directamente el Plan de contingencia y continuidad del negocio de la empresa.

e. Los usuarios deben acatar los lineamientos la Política de clasificación de la Información para el acceso, divulgación, almacenamiento, copia y protección de la información física que establezca por razón de sus labores, información enmarcada en buenas prácticas, principios de integridad y veracidad, clasificándolos de acuerdo con la afectación y riesgo en continuidad de negocio

f. Ciclo de vida de la información física y digital de la empresa, en sus procesos, se establecerá durante la recolección de datos, el almacenamiento y disposición final, de acuerdo con la Política de Archivo, la cual siempre estaba bajo llave, en cajas reglamentarias y bien rotuladas si es el caso y se entregara con acta

al Jefe Administrativo y Financiero quien maneja las llaves de la bodega de archivo documental, que busca la cconservación, disposición final, supresión, archivo o destrucción, de acuerdo a lo establecido en los procedimientos de cada área.

g. Los colaboradores usuarios de la información tendrán en cuenta la importancia de confidencialidad de la información al sacar fotocopias, al escanear, impidiendo que se haga una copia extra de dicho documento, por lo que no puede existir papel reciclaje, con información sensible para reutilizar, este se romperá, de no ser así, estarán autorizados a realizar el respectivo reporte de este evento, ante el Jefe de Seguridad de la información. Por lo anterior NO DEBEN:

*Modificar las configuraciones de seguridad de los dispositivos móviles, que les han asignado para contacto con los clientes y partes interesadas.

* No se deben almacenar videos, fotografías o información personal.

* Deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, cafés internet.

h. Implementación de escritorio y pantalla despejada: Se dará la orden a los colaboradores, la importancia de tener el escritorio despejado, para mayor comunidad, control sobre los documentos y equipos de cómputo que se encuentra manipulando; de igual forma la pantalla despejada con solo los documentos necesarios, lo cual está establecido en la OGE-005 Política de comunicaciones, que establece la responsabilidad, de no dejar documentos que contengan información en los escritorios, que cuando se ausenten de su puesto de trabajo, se debe guardar la información y bloquear el computador.

i.Se solicitará al realizar el contrato con los clientes y partes interesadas, la autorización de tratamiento de datos, igualmente se requerirá para la Unidad Antifraude, copia de la autorización de los asegurados.

j. Ante una queja o requerimiento de los clientes, las asesoras comerciales y jefes de áreas, están capacitadas para atender el requerimiento, este queda registrado a través de correos electrónicos, de ser un requerimiento tecnológico, se escala el evento al área de tecnología y cuando se soluciona se notifica a través de correo eléctrico a las personas encargadas de las empresas, que se subsanó la inconformidad

Todas las demás responsabilidades con la protección y tratamiento de la información, derivadas y establecidas en los procesos y procedimientos de RISKS INTERNATIONAL S.A.S. El incumplimiento de estos aspectos generara la desvinculación inmediata del colaborador de la empresa.

2.4. USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION Y OPERACIÓN DE LAS PLATAFORMAS, CON LOS MAS ALTOS ESTANDARES DE CALIDAD: La Gerencia CEO y Subgerencia:

a. Supervisaran la plataforma tecnológica y los servicios de red de la empresa, que sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios.

b. Serán los poseedores de los más altos privilegios sobre las plataforma y servicios innovadores que se les ofrezcan a los clientes y partes interesadas.

c. Ejercerán el control y tendrán acceso a plataformas como Dropbox que contendrán el Sistema de Gestión de Calidad de la empresa.

d. Tendrán el control y manejo de supervisión a encuestas aplicadas a los colaboradores de la empresa en diversos temas.

e. En coordinación con el área tecnológica, participar activamente en la elaboración, prueba, ejecución y de las plataformas.

f. Cuando de generan alertas, usualmente están se visualizan por medio de correo electrónico o soporte en línea, las cuales se atienden de forma inmediata, de no poderse solucionar, se requiere ser escalada al Área de Tecnología y se establece de inmediato acciones de mejora.

CREACION DE COMITÉ DE SEGURIDAD DE LA INFORMACION:

El Comité deberá asegurar que exista un apoyo a la empresa para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, sus responsabilidades serán las siguientes:

a. Coordinar la implementación del modelo de seguridad y privacidad de la Información al interior de la empresa.

b. Revisar los diagnósticos de inventarios de activos de información, realizados por cada jefe de área.

c. Acompañar e impulsar el desarrollo de proyectos de seguridad

d. Coordinar y dirigir acciones específicas, que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la empresa como prestadora de servicios informáticos.

e. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.

f. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

g. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

h. Se creará la implementación del SGSI, el cual se auditara permanentemente y se harán las acciones de mejora pertinentes.

i. Socializar y sensibilización de la seguridad de la información dentro de la empresa.

j. Poner en conocimiento de la empresa, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

K. El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

L. Las demás funciones inherentes a la naturaleza del Comité.

3. IMPLEMENTACION DE PLAN DE CONTIGENCIA Y CONTINUIDAD DEL NEGOCIO:

3.1. AREAS FISICAS Y MEDIOAMBIENTALES SEGURAS: Se implemento el sistema de mecanismos de normas de seguridad física y control de acceso a la empresa así:

a. Control de acceso físico, por medio de llaves eléctricas, para acceder a las dos puertas principales de la empresa.

b. A los visitantes a la empresa, se les dará la Información de la Política de tratamiento de datos, para lo cual ellos deciden si autorizan su registro como visitantes.

c. Se establece como normatividad portar el carné de la empresa al ingresar a la empresa y durante el tiempo de dure la jornada laboral, toda vez que identifica a los colaboradores en caso de pérdida debe informar a la Gerencia CEO o Subgerencia y pagar la reposición.

d. Aislamiento y control de acceso zonas seguras de las áreas restringidas a través de un letrero, que indica solicitar autorización para ingresar, con archivos controlados bajo llave.

e. Tecnología de la empresa, estará ubicada en un área controlado-separada a nivel físico y lógico para desarrollo, pruebas, de control, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información.

f. Se establecieron controles físicos implantados en las instalaciones, como cableado eléctrico, alarma, rejas en las ventanas y sensor de movimiento que quedan activados en la noche.

g. Certificación de la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información, para lo cual el área administrativa y financiera hará un respectivo cronograma de mantenimiento controlado de equipos computadores e impresoras. De igual forma los presidentes de los comités de Prevención y Atención de desastres, COPASST y Seguridad y Salud para el trabajo hacen una inspección de instalaciones y equipos, estableciendo unas recomendaciones a subsanar.

h. En caso de presentarse una contingencia o al realizarse una prueba técnica que afecte el servicio, los responsables de área y clientes se comunicaran vía telefónica o la Gerencia CEO, a través de correo masivo, informara la novedad y el tiempo en subsanarse.

3.2. CONTROLES DE SEGURIDAD DE LA INFORMACION Y RESPONSABILIDADES DE ACTIVOS:

a. Se realiza análisis de la vulnerabilidad sobre las plataformas tecnológicas y se hacen permanentemente acciones de mejora.

b. Se cuenta con sistemas de protección ante software de códigos maliciosos, por lo que se establecerá herramientas de protección antivirus antimalware, antispam, antispyware tanto en los dispositivos de computo. Por lo anterior Deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, cafés internet.

c. Los colaboradores usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos

d. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato al área de tecnología.

e. Se cuenta con un proceso para proteger la información sensible, confidencial, que se almacena mensualmente en un disco duro de respaldo de seguridad de la información, a través de Back up y en la nube.

f. El Área de Tecnología debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

g. Los usuarios NO DEBEN modificar las configuraciones de seguridad de los dispositivos móviles, que les han asignado para contacto con los clientes y partes interesadas.

h. Restricciones a conexiones remotas de los recursos de la plataforma tecnológica de la empresa, únicamente se deben permitir estos accesos a personal autorizado, para el desarrollo de sus labores de la empresa bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega. Por lo que no se podrá utilizar sus equipos de cómputo para desempeñar las actividades personales.

i. Hacen parte de los activos de la empresa, los equipos de cómputos impresoras, discos duros y demás elementos de comunicación, la información que se obtiene de las plataformas, que se procesa, almacenada, con carácter confidencial, remitida a los clientes y partes interesadas. Por lo anterior, se le dará buen uso por parte de los colaboradores y estarán bajo la supervisión de los jefes de área, dando aplicabilidad a las políticas de tratamiento de datos, la clasificación de la información de acuerdo con los controles requeridos para su protección, Política de comunicación, Manuales y reglamentos de protección de datos y las auditorias de control que se realicen al respecto para la mejora continua.

j. Se deben deshabilitar la funcionalidad de recordar campos de contraseñas, el aplicativo de seguridad debe certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

k. Cuando se presente una falla tecnológica y esta sea subsanada, el jefe de Seguridad de la información y el comité, elaboraran el registro documental que describa las No conformidad, causas y acciones correctivas y de mejora implementadas

3.3. NORMAS DE SEGURIDAD DE LOS EQUIPOS DE LA EMPRESA:

a. Todos los computadores tendrán control de claves de acceso.

b. Se establecerá un registro documental aprobado previamente para sacar un computador de la empresa, previa autorización de la Gerencia CEO y Subgerencia.

c. Se deben tomar las medidas de precaución de seguridad necesarias en el transporte de los mismos. De tener perdida o daño se debe informar de inmediato a la Gerencia CEO y Subgerencia, para los tramites internos.

3.4. PROCESOS DE SELECCIÓN ADECUADOS:

a. En el procedimiento de Talento Humano, está establecido el paso a paso de selección de personal, desde la requisición del cargo, el perfil de usuario operador de la información, el acuerdo de confidencialidad o de no divulgación de la información que maneja y sobre las actividades que desarrolla.

b. En la selección del personal, la responsabilidad de los activos de la información, se tendrán en cuenta para la contratación de los colaboradores con un perfil adecuado, integro y competente.

c. Los colaboradores, darán estricto cumplimiento a las políticas, manuales, instructivos y reglamentos que se establezcan en la protección de datos, se harán responsables y acreedores a sanciones por el mal uso o manejo de la información. En esta se determina igualmente la importancia de ser cuidadosos de no divulgar información confidencial entre compañeros, en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad de la información y el buen nombre de la entidad

d. En el proceso de inducción y reinducción, a los colaboradores se les socializara las Políticas, instructivos, manuales y reglamentos de soporte de capacitación para crear conciencia en seguridad de la información, la cual estará en DRIVE- GESTION DE CALIDAD, para ser consultada cuando se requiera.

3.5. MEDIDAS DISCIPLINARIAS Y PENALES: El incumplimiento a los acuerdos de confidencialidad establecidos con los colaboradores, proveedores, clientes y partes interesadas, acarreara sanciones de orden pecuniario, disciplinario y penal.

3.6. AUDITORIAS Y MEJORAMIENTO CONTINUO: Se implementará auditorias, que permitirán establecer:

a. Cumplimiento de requisitos, políticas, manuales, reglamentos y autorizaciones para el manejo de la información.

b. La administración como usuarios operadores de la información, previniendo permanentemente los riesgos asociados al mal manejo

c. Las No conformidades, para lo cual se hará un plan de acción metodológico de acciones correctivas.

La presente política de Seguridad de la Información entra en vigencia al momento de recibido este comunicado.

Atentamente,

_____

CRISANTA AVILA PUIN
Representante Legal

Julio 30 del 2017