POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Se determina como objetivo de esta política, la regulación de la gestión a implementar y ejecutar en la seguridad de la información y ciberseguridad al interior de La empresa y para la protección de la información propia y de los clientes de RISKS INTERNATIONAL.S.A.S, 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 información y ciberseguridad. La aplicabilidad se soportará en los procedimientos internos de la empresa, la Política de tratamiento de datos, Política de clasificación de la información, manuales, reglamentos, autorizaciones físicas y electrónicas para consulta y reporte ante operadores de información y los mecanismos de protección de información T.I.

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, determinando que para acceder a información se requiere 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 los sistemas de información de la compañía y en los registros de datos consultados por clientes y los cuales son de acceso confidencial y reservado.

Hasta: El tratamiento, administración, compilación protección de los documentos en archivos físicos, tecnológicos o de cualquier medio que permita almacenar información sujeta al desarrollo de actividades y servicios prestados por la compañía, en los cuales se implementarán los procedimientos y políticas preestablecidas por la empresa, protegiendo el uso de las medidas técnicas y tecnológicas, humanas y administrativas que sean necesarias, para otorgar seguridad de la información física y TI, 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

1.1. GESTIÓN DE ACTIVOS DE INFORMACIÓN: 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 de las partes interesadas. Se da almacenamiento, recuperación, transmisión y manipulación de datos e información conforme a las regulaciones legales para protección de datos y protección de información TI.

1.1.1. GESTIÓN DE ACTIVOS DE INFORMACIÓN FÍSICA Y T.I.:

1.1.1.1 Adquisición: Planificación, compra o diseño de información pública, privada, servidores y herramientas por la cual se genera el registro de los servicios prestados por Risks International S.A.S, la cual hace relación a documentación, equipos, bases de datos públicas o privadas, informes y demás documentación física o electrónica para el desarrollo de la función.

1.1.1.2 Puesta en marcha: Se registra y soporta la información en medios de protección como los son la nube, servidores, disco duro.

1.1.1.3 Operacional: Monitoreo, mantenimiento, actualización de la información activa en el sistema por parte del Superadministrador, persona o personas encargadas de las verificaciones, transmisión y uso de la información cifrada y relacionada con la prestación del servicio.

1.1.1.4 Eliminación: La información cuenta con una reserva en tiempo de mínimo 5 años y máxima de 7 años, con fundamento en la normatividad vigente; información que será guarda en los servidores del sistema protegidos y vinculados en nube con el servicio de Amazon. Dicha información podrá ser guarda y protegida por una vigencia superior a la aquí estimada a petición del cliente.

1.1.1.5 Actualización: Los activos físicos relacionados con información de clientes se actualizan anualmente (solicitud de documentación contractual), en lo referente a información T.I se actualizará para fuentes vinculantes y restrictivas de manera permanente y en línea y para bases de datos propias semestral y anualmente.

1.1.2 GESTIÓN DE DATA LOSS PREVENTION (DLP)

1.1.2.1 Controles de ingreso a la conexión: Los activos de la compañía tendrán acceso a conexión por medio de Ethernet, con fines de protección y control de ingreso la red de conectividad (internet) de la empresa la Subgerencia operativa, se encargará de realizar cambios de ingreso en la contraseña de red (internet) cada dos (02) días, estas claves de seguridad solo serán de conocimiento de la Gerencia y Subgerencia.

1.1.2.2 Mecanismo de control: La empresa implementará como mecanismos de protección de los activos entregados a los empleados o colaboradores de la siguiente manera:

1.1.2.2.1 Mecanismo primario: A la vinculación del empleado, colaborador o proveedor la empresa configurará el software del activo a entregar con fines de restricción de uso, alteración, modificación, inclusión de software en los equipos o herramientas.

1.1.2.2.2 Identificación de software: Se instalará mecanismo de identificación del software en los activos de la empresa mediante políticas locales de SO, esta vinculación se efectuará en Windows con protección de bloqueo de usuarios y administradores del activo.

1.1.2.2.3 Eliminación de software: Los activos de la empresa se auditarán cada tres meses por parte del departamento de gestión de calidad, en caso de encontrar en el activo verificado software que no fueron configurados por la empresa en la estación activa de trabajo, se eliminaran las mismas, se instalará un mecanismo de mayor protección con el fin de bloquear por completo el acceso a software no autorizados por la empresa, se efectuará el cambio de claves de acceso. Este procedimiento se dejará bajo constancia en

el formato de revisión, verificación, reparación y cambio de activos o herramientas por parte de quien realice la auditoría al activo, adicional a ello se informará de la irregularidad hallada en el activo y posible riesgo en el uso de la información a la Gerencia, Subgerencia, Dirección Legal y Dirección Financiera y de Recursos Humanos para que estas adelanten el proceso interno de investigación por la falta cometida por el responsable del activo(empleado, colaborador, proveedor entre otros) con fines de aplicabilidad de una posible sanción para el responsable.

1.2. GESTIÓN DE CAMBIOS: La gestión de cambios estará compuesto por las siguientes actividades:

1.2.1. Registro de gestión de cambios: La recepción de una o varias solicitudes de adición, modificación y/o eliminación tendrá que estar debidamente registrada siempre y cuando pueda llegar a afectar directa o indirectamente los servicios o la información protegida por la presente política.
1.2.2. Responsable de verificación de cambio: El responsable o encargado de la Temática de Infraestructura y Seguridad comprobará la correcta implementación del cambio, para lo cual consultará al personal involucrado, es decir, a los Administradores y Especialistas Técnicos y/o al equipo involucrado en el desarrollo del cambio terceros o empleados de la compañía.
1.2.3. POST- IMPLEMENTATION REVIEW (PIR): Después de que transcurra un periodo de tiempo preestablecido tras la implementación de algún cambio, o si es el caso, de su "rollback", se llevará a cabo una revisión técnica post-implementación (PIR - Post-Implementation Review) por parte de el responsable o encargado de la temática de infraestructura y seguridad

1.3. GESTIÓN DE MONITOREO: Esta gestión agrupa un conjunto de actividades relacionadas al procedimiento de Gestión de Cambios que tienen como objetivo la gestión y el seguimiento para la mejora continua. Para ello se deberá realizar el monitoreo de todos los cambios realizados que afecten de manera indirecta o directa la información y/o data; el monitoreo se guiará por el procedimiento mediante la siguiente manera:

1.3.4.1. Llevar un registro detallado de los cambios en implementación o completados.
1.3.4.2. Realizar el seguimiento de cada uno de los cambios realizados y su efectividad de cada uno.
1.3.4.3. Realizar un informe del estado de los cambios: operados/cerrados, en desarrollo y pendientes.
1.3.4.4. Realizar la retroalimentación de las actividades del procedimiento como parte de la agenda del Comité de Seguridad de la información y Ciberseguridad.

1.4. GESTIÓN DE RIESGO DE LA INFORMACIÓN: 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. IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN:

2.1. SOBRE EL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:

El Oficial de Seguridad de la información, será el responsable de desarrollar e implementar la política de seguridad de la información almacenada y/o codificada en medios informáticos; esta política se diseñó para proteger la información, regular los procedimientos o procesos para uso, divulgación, modificación, destrucción o acceso no autorizado de la información y/o datos codificados o no.

La responsabilidad correspondiente al rol del "Oficial de Seguridad de la Información" será asignada a el Gerente General-CEO para efectos de garantizar y liderar la implementación, mantenimiento y mejora del SGSI.

2.1.2. RESPONSABILIDADES DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:

2.1.2.1. Desarrollar políticas, procedimientos y normas para garantizar la seguridad, confidencialidad y la privacidad de la información.

2.1.2.2. Supervisar e informar a los organismos competentes sobre cualquier incidente de información por intrusión y activar las estrategias descritas en la presente política o los procedimientos aplicables para evitar la reiteración de incidentes.

2.1.2.3. Supervisar la correcta y eficaz clasificación de seguridad de la información, de acuerdo a la regulación interna al respecto o los fines propios de la información.

2.1.2.4. Mantener y conservar en los casos de recuperación y reinicio de sistemas, las condiciones y características de la información de acuerdo a lo asignado por el propietario de la misma.

2.1.2.5. Actualizar la información que repose en el registro de inventario de activos

2.1.2.6. Retirar y eliminar la información que deba ser eliminada de acuerdo a las relaciones contractuales existentes y cuando se cumpla el término mínimo de permanencia de la información.

2.1.2.7. Autorizar y asegurar el acceso a las personas que tengan derecho sobre la información.

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

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

2.1.2.10. Supervisar y auditar, 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 DIRECCIÓN DE LA POLÍTICA

RISKS INTERNATIONAL S.A.S, se compromete 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 y ciberseguridad, 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, a los colaboradores, la cual se cambia cuando este se encuentra incapacitado o se retira permanentemente de la empresa. Una vez esté 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. La asignación de claves y usuarios a los clientes, se encuentra a cargo de los Administradores de la plataforma.

d. 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.

e. 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.

f. 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.

g. Se dispondrán controles que restrinjan el uso de medios de almacenamiento removibles, que impiden copiar información (USB, Unidad CD, disco duro externo) de los equipos o elementos tecnológicos de la compañía por parte de sus colaboradores o empleados.

h. Las copias de respaldo se realizarán por la Gerencia CEO, cada 6 meses mediante disco duros, los cuales cuentan con parámetros de seguridad, estos elementos quedarán en custodia de la Gerencia en los lugares que este estime en las actas correspondientes; los soportes de Back up de información de las herramientas se efectúa diariamente por el departamento de tecnología, en proceso automatizado con respaldo de los servidores del funcionamiento de las herramientas.

i. Se determina como restricción a los empleados o colaboradores el uso de los equipos tecnológicos con fines personales o para el uso de información personal (archivos, fotografías, videos y demás datos).

j. Registro y monitoreo el diseño de las plataformas y aplicativos establecerá monitoreo y 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 y CLAVES:

a. Conocer y dar aplicabilidad a las directrices y normatividad legal vigente, en materia de seguridad de la información y ciberseguridad, 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 información 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, estas serna debidamente protegidas 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 de la compañía , quien mediante los empelados asignados harán la entrega de usuarios y claves para su ingreso a la herramienta al cliente, quien debe remitir para su asignación los datos de correos corporativos, números de identificación ciudadana de la persona a la que se le va asignar el usuario y clave, número telefónico de la persona que se va a encargada de usuario, cargo del empleado o colaborador al que se le asignara el usuario. Con fines de protección y seguridad del sistema y los mecanismos de información los usuarios serán bloqueados al retiro del empelado o colaborador de sus funciones por parte del cliente, quien Debra notificar o comunicar de su restiro a la compañía para adelantar los tramites de seguridad de claves y usuarios.

d. Los empleados o colaboradores de la empresa quedan obligados a no compartir cuentas, usuarios y claves bajo el acuerdo de confidencialidad que firman a la vinculación contractual con la empresa, por lo que serán responsables de proteger la información a la cual accedan y procesan, para evitar su pérdida, alteración, destrucción o uso indebido, de acuerdo con las políticas establecidas para la protección de información física y TI, generados en la empresa. De esta forma apoyaran directamente el Plan de contingencia y continuidad del negocio de la compañía.

e. Los usuarios deben acatar los lineamientos de protección de la información física, TI y los accesos adjudicados a los usuarios ya sean determinado como clientes, empleados o colaboradores, los mismos no podrán divulgar, almacenar, copiar información con fines distinta a los determinados como uso del

servicio o para prestación del servicio. Se obligan a proteger la información física y TI que se establezca por razón de sus labores contractuales ya sean de carácter laboral, comercial, civil, alianzas o fusiones comerciales. Esta información estará en marcada en las buenas prácticas profesionales, comerciales y mercantiles, bajo el principio de integridad y veracidad, clasificándolos de acuerdo con la afectación y riesgo en continuidad de negocio

f. Los empleados y colaboradores que hagan uso de los elementos de reproducción o duplicación de información física o TI, efectuaran la misma bajo el requisito legal de confidencialidad de la información, tomando cada una de las medidas preventivas al usar los medios o mecanismos de duplicación como lo son fotocopiadoras, escanear, celulares corporativos para la toma de imágenes con el fin de evitar la duplicidad en los elementos a utilizar.

- Modificar las configurar de seguridad de los dispositivos móviles, que les han asignado para contacto con los clientes y partes interesadas a los empleados.
- Deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público o privado que no pertenezca a la compañía.

g. Ante una queja o requerimiento de los clientes por asignación o uso de usuarios y claves, las asesoras comerciales y jefes de áreas, están capacitados para atender el requerimiento, este queda registrado a través de correos electrónicos, de ser un requerimiento tecnológico, se escala el evento al área correspondiente. Su respuesta y solicitud será comunicada a través de los medios acordados en el contrato con el cliente a las personas encargadas o asignadas por el este, correo que contendrá información clara y expresa a la solución dada.

2.4. USO DE ALTOS PRIVILEGIOS Y APROVECHAMIENTO ADMINISTRATIVO Y OPERACIONAL DE LAS PLATAFORMAS, CON LOS MÁS ALTOS ESTÁNDARES DE CALIDAD:

a. La Gerencia-CEO y el Departamento de Tecnología, 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 y/o de los empleados o colaboradores.

b. La empresa será la poseedora de los más altos privilegios sobre las plataforma y servicios innovadores que se les ofrezcan a los clientes y partes interesadas.

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

d. Se aplicarán y controlara la supervisión a encuestas realizadas 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. La generación de alertas en las que clientes o terceros interesados requieran guía de solución serán atendidas por correo electrónico (asesor comercial) o por intermedio de soporte en línea, requerimientos que serán atendidos en tiempo real, en aquellos casos en que la solicitud debe ser atendida por el departamento de tecnología, quien tenga la calidad de primer conocedor del caso dentro de la empresa, lo escalara con el departamento de tecnología para que el mismo tome las medidas pertinente de solución o mejora en el sistema, de las medidas tomadas se informará vía correo electrónico a la empresa cliente con un término de un (01) a tres (03) días según la complejidad del requerimiento.

2.5. CREACIÓN DE COMITÉ DE SEGURIDAD DE LA INFORMACIÓN y CIBERSEGURIDAD:

El Comité deberá asegurar que exista un apoyo a la empresa para soportar la administración y desarrollo de iniciativas sobre seguridad de la información y ciberseguridad, este comité estará conformado por la Gerencia General-CEO, la Subgerencia Operativa, la Dirección Tecnológica, Dirección Legal y de Cumplimiento, la Dirección Financiera y de Recursos Humanos y la Dirección de Gestión de Calidad sus responsabilidades serán las siguientes:

a. Coordinar la implementación del modelo de seguridad y privacidad de la Información y ciberseguridad 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 específicas 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 auditará permanentemente y se harán las acciones de mejora pertinentes.

i. Socializar y sensibilizar a los empleados, colaboradores de la seguridad de la información y ciberseguridad dentro de la empresa.

j. Poner en conocimiento de la empresa, los documentos generados al interior del comité de seguridad de la información y ciberseguridad 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 que se presenten en el desarrollo de las labores de mitigación, prevención, aplicación, control de riesgo y todas aquellas que sean inherentes a la naturaleza del Comité.

3. IMPLEMENTACIÓN DE PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO:

3.1. ÁREAS FÍSICAS Y MEDIOAMBIENTALES SEGURAS: Se implementó 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 tres (04) puertas principales de la empresa y cerca eléctrica que se encuentra ubicada en la puerta de entrada principal de las instalaciones físicas. Las puertas de ingreso de las oficinas administrativas tienen código de seguridad de ingreso.

b. A todas aquellas personas que tengan la calidad de visitantes, al arribo e ingreso a las oficinas se les pone de presente la minuta de registro de ingreso, se solicita un documento de identificación (el cual debe contener nombre, cédula) este documento se queda en poder de la compañía hasta el registro de salida del visitante, como soporte para el tránsito por la zona autoriza del visitante este deberá portar el carnet entregado al registro de su ingreso en un lugar visible.

c. Se establece como normatividad portar el carné de la empresa al ingresar a la empresa y durante el tiempo de duración de la jornada laboral, toda vez que identifica a los colaboradores en caso de pérdida, debe instaurar la denuncia de pérdida ante el ente judicial competente y asumir el costo de reposición del carnet. De la pérdida del carnet el empleado o colaborador debe informar al Departamento de Recursos Humanos, mediante el formato establecido por el sistema de gestión de calidad al cual adjuntará copia de la denuncia y de la consignación realizada en la cuenta de la empresa por el valor del carnet estimado en la suma de Cincuenta Mil pesos M/cte ($50.000).

d. Aislamiento y control de acceso zonas las cuales se identifican como restringidas a través de señalización, que indica solicitar autorización para ingresar, con archivos controlados bajo llave.

e. Tecnología de la empresa, estará ubicada en un área controlada-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. Al igual que serán de acceso restringido y se encontrarán en oficinas con mecanismo de seguridad de ingreso.

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 horas de 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 recomendaciones o cambios de mejoras.

h. En caso de presentarse una contingencia o al realizarse una prueba técnica que afecte el servicio, los responsables de área y de los clientes, se comunicarán vía telefónica o se emitirá por parte de la Gerencia General CEO, correo masivo informando la novedad y el tiempo en corrección de la misma.

3.2. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN 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 o privado no autorizado por la empresa.

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 dentro de la empresa y 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 cómputo, 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 empleados y colaboradores quienes estarán bajo la supervisión de los Jefes de Área o de la Gerencia para los cargos de Dirección, manejo y confianza, dando aplicabilidad a las políticas de tratamiento de datos y seguridad informática, 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 ciberseguridad, las auditorías 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, elaborará 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 tres (03) controles de claves de acceso.

b. Se establecerá un registro documental aprobado previamente para sacar un computador de la empresa, previa autorización de la Gerencia 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 y Subgerencia, para iniciar los trámites de denuncia cuando corresponda y activar los mecanismos de contingencia internos con el fin de mitigar riesgos de pérdida duplicación de la información del equipo.

3.4. POLÍTICA Y/O PROCEDIMIENTO PARA LA APLICACIÓN DE PARCHES

Para la aplicación de parches dentro de la organización se conforman de la siguiente manera:

3.4.1. ESTACIONES DE TRABAJO:

Los parches de las estaciones de trabajo se realizará de conformidad con las estimaciones y el cumplimiento de parte del equipo de desarrollo de Microsoft, las actualizaciones acumulativas se publican cada segundo martes del mes.
Por esta razón Risks International S.A.S., el responsable o encargado de la temática de Infraestructura y de Seguridad es quien implementará la instalación de los parches acumulativos el segundo sábado de cada mes, con el fin de realizar investigaciones de los errores que pueden ocurrir al actualizar las estaciones de trabajo.

3.4.1.1. MODALIDAD DE INVESTIGACIONES:

3.4.1.1.1. INVESTIGACIÓN POR INTRANET
Estas investigaciones se realizan en sitios oficiales como https://support.microsoft.com o sitios a fines para encontrar errores comunes o que dejen inhabilitados las estaciones de trabajo y realizando así la búsqueda de soluciones para estos.

3.4.1.1.2. ACTUALIZACIÓN DE EQUIPOS DE PRUEBAS
Dentro del área de tecnología de la organización se realiza la actualización de un equipo para revisar las fallas que puedan provocar la instalación de parches de seguridad, en caso de presentar problemas se realiza una solución en los sitios https://support.microsoft.com o corrección manual de estos errores.
En caso de que los errores generados sean de alto impacto para el funcionamiento del equipo se realizará la desactualización de los parches de seguridad a la versión anterior y postergando para el siguiente sábado, realizando el mismo procedimiento descrito anteriormente.

3.4.2. SERVIDORES
El objetivo de los parches de seguridad es corregir o actualizar el software base de los servidores donde se alojan las aplicaciones misionales ubicadas en el Centro de Datos, a través de la instalación de parches con el fin de garantizar su operación.

Con el fin de garantizar la continuidad y satisfacción de los servicios prestados dentro de las plataformas misionales los parches de seguridad deben seguir los siguientes pasos:

a. El responsable o el encargado de la temática de Infraestructura y de Seguridad se reunirá con el Oficial de Seguridad de la información para definir y elaborar el plan de trabajo para la instalación mensual de parches.

b. De acuerdo a lo acordado en las reuniones, se enviará correo electrónico a los usuarios funcionales de los ambientes de desarrollo, informando el listado de parches a instalar, la fecha y hora de aplicación de los parches.

c. Los usuarios funcionales remitirán al responsable o el encargado de la temática de Infraestructura y de Seguridad para la instalación de los parches en el ambiente de desarrollo, teniendo en cuenta las observaciones recibidas para la instalación de los parches. El responsable o el encargado de la temática de Infraestructura y de Seguridad aplicará los parches en el ambiente de desarrollo. Una vez finalizada esta actividad se tendrá que enviar el informe respectivo al Oficial de Seguridad de Información, el cual debe mostrar los parches que fueron instalados.

d. Una vez instalados los parches en el ambiente de desarrollo, el responsable o el encargado de la temática de Infraestructura y de Seguridad revisará el correcto funcionamiento general de las

aplicaciones, software base, cadenas de conexión, tareas programadas, sistema operativo y SQL, entre otros, haciendo seguimiento y Monitoreo de las Aplicaciones Misionales.

e. Se deberá analizar si existen o no errores en las aplicaciones.
   i. En caso de que sí existan errores: Se ejecuta el plan de roll back indicado en el servidor de pruebas y debe realizarse la actividad descrita en el literal "a".
   ii. Si no existen errores en las aplicaciones, se debe gestionar el cierre de la solicitud y continuar con la actividad descrita en el literal "f".

f. El responsable o el encargado de la temática de Infraestructura y de Seguridad iniciará la instalación de los parches en ambiente de producción, indicando el listado de parches a instalar, la fecha y hora de aplicación en el ambiente de producción

g. Una vez instalados los parches en el ambiente de producción, el Usuario de pruebas revisará el correcto funcionamiento general de las aplicaciones, software base, cadenas de conexión, tareas programadas, sistema operativo y SQL, entre otros. El usuario funcional verificará el funcionamiento y operación del aplicativo e informará de las observaciones que surjan. El responsable o el encargado de la Temática de Infraestructura y Seguridad realiza el monitoreo a las aplicaciones por medio del procedimiento indicado para tal fin.
h. El responsable o el encargado de la temática de infraestructura y seguridad verificará la existencia o no de errores en las aplicaciones:
   i. Sí existen errores: Se ejecutará el plan de roll back en los servidores y se tendrá que regresar a la actividad descrita en el literal "a".
   ii. No existen errores: Se gestionará el cierre de la solicitud y se dará por terminado el procedimiento.

3.5. PROCESOS DE SELECCIÓN ADECUADOS:

a. En los procedimientos de selección y vinculación del personal de plan o externo de la empresa, se da trámite de explicación y capacitación de la responsabilidad de los activos de la información de la compañía entiéndase esta como equipos y otros elementos que contengan medios de información física o TI. Se tendrá en cuenta para la contratación de los empleados o colaboradores con un perfil adecuado, íntegro y competente.

c. Los empleados y colaboradores, darán estricto cumplimiento a las políticas, manuales, instructivos, circulares, comunicados y reglamentos que se establezcan en la protección e integridad de datos, información física, TI. En caso de presentarse fallas probadas de protección del responsable, se podrán aplicar 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 empresa.

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

3.6. MEDIDAS DISCIPLINARIAS Y PENALES:

El incumplimiento a los acuerdos de confidencialidad establecidos con los colaboradores, proveedores, clientes y partes interesadas, acarreará sanciones de orden pecuniario, disciplinario y penal establecidos en los contratos, reglamentos y en la normatividad vigente y aplicable para el asunto.

3.7. AUDITORÍAS Y MEJORAMIENTO CONTINUO. Se implementará auditorias, que permitirán establecer:

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

b. La administración en calidad de usuarios operadores de la información, previniendo permanentemente los riesgos asociados al uso indebido de los datos, información, TI y demás relacionados con el fin proteger estos.

c. En caso de presentar No conformidades, se creará y ejecutará un plan metodológico de acciones correctivas.

La presente política de Seguridad de la Información y Ciberseguridad, entró en vigencia en el año 2016, por lo cual, dando aplicabilidad a los planes de mejoras, la actualización de su versión entra en vigencia a partir del 01 de enero de 2021, con tránsito de obligatoriedad para la empresa, sus empleados, colaboradores, proveedores, clientes y terceros interesados en los servicios de RISKS INTERNATIONAL S.A.S.

Atentamente,

Representante Legal