ACCURATIORATINGS CLASIFICADORA DE RIESGO AFILIADA A JCR ER	**Código: ACRA-PSI – 01**	**Aprobado: Directorio 28.12.2017**	**Versión 01**

PLAN DE SEGURIDAD DE LA INFORMACIÓN

Índice

1. Antecedentes

El objetivo del presente documento es describir los controles de seguridad que deben ser implementados, mantenidos, mejorados, modificados, controlados y supervisados en Accuratio Credit Rating Agency Empresa Clasificadora de Riesgo (La Clasificadora), de forma que permita la interpretación clara y precisa de las políticas, medidas y procedimientos que se definan en la misma, con el objetivo de alcanzar niveles aceptables de seguridad.

Se describen los elementos fundamentales que deben ser incluidos y el modo en que es estructurado, así como los aspectos necesarios de modo que aquellos aspectos que no correspondan a las necesidades de protección identificadas podrán ser excluidos y por supuesto, se adicionará cualquier elemento que se considere importante para los requerimientos de seguridad, con independencia de que no esté contemplado en este documento.[1]

2. Base Legal y Normativa Interna

- Reglamento de Empresas Clasificadoras de Riesgo – Resolución Superintendencia Nº 032-2015-SMV/01
- Reglamento de Gestión Integral de Riesgos – Resolución Nº 037-2015 – SMV/01
- Reglamento de Gestión de Riesgo Operacional – Resolución Nº 027-2015-SMV/01
- Manual de Organización y Funciones
- Manual de Procedimientos Operativos
- Código de Conducta

3. Alcance del Manual

El Manual de Gestión de Seguridad de Información (MGSI) está basado en la normativa detallada en el punto 3 “Base Legal y Normativa Interna” trata los puntos principales de la ISO 27001:2005.

[1] La Clasificadora cumplirá todo lo que indique la norma de acuerdo a su tamaño, naturaleza y complejidad del negocio. Aquello que no está incorporado en el presente documento, cuando corresponda, será de estricto cumplimiento.

El manual tiene como objetivo recoger, analizar y definir los lineamientos de la gestión de seguridad de información. Es obligatorio que se asegure que el personal y los colaboradores externos tengan pleno conocimiento de este documento y se implementen dentro de sus actividades.

4. Control del Manual

Es responsabilidad del encargado de riesgos lo concerniente a su elaboración, modificación, distribución y control.

- Distribución del manual: la distribución es interna, para consulta y publicada en la web cuando corresponda.
- Revisión del manual: será revisado como mínimo una vez al año para efectos de actualización, o por cualquier otro motivo que arroje resultados diferentes a los planeados por el Sistema de Gestión de Seguridad de la Información de la Clasificadora.

5. Política de Seguridad de Información

El Directorio de la Clasificadora reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

Es un compromiso del Directorio el adoptar lo establecido en este manual promoviendo la adecuada interiorización, implementación, mejoramiento y entrenamiento para los funcionarios y colaboradores externos.

6. Alcance del Sistema de Gestión de Seguridad de Información (SGSI)

El objetivo es gestionar eficientemente la seguridad de información a través del mantenimiento de la integridad, disponibilidad y confidencialidad de la información administrada por la Clasificadora en sus diferentes actividades, y de los sistemas informáticos donde se almacene y gestione.

7. Responsable de Informes

El responsable de seguridad de información o quien desempeñe las funciones reportará una vez al año al Directorio sobre el desempeño del sistema de gestión de seguridad de información.

8. Metodología de Gestión de Riesgo

Las evaluaciones de la política de seguridad de información y de la ejecución de la misma tiene como objetivos administrar los riesgos institucionales mediante la identificación, evaluación, valoración y seguimiento de los mismos con el fin de prevenir y mitigar los eventos generados por su materialización; su alcance inicia con la identificación del contexto estratégico de la Clasificadora, continúa con la clasificación, evaluación y valoración, y finaliza con el seguimiento de la política de administración de riesgos y aplica para todos los procesos del sistema de gestión de la Clasificadora.

La metodología que se implementa es la desarrollada en el Manual de Gestión de Riesgo Operacional valorizando los riesgos de seguridad de información de acuerdo a la metodología MAGERIT – versión 2 “Metodología de Análisis y Gestión de Riesgos de Sistema de Información”.

Los criterios de evaluación de riesgos y la escala de riesgos siguen las pautas dictadas en el Manual de Gestión de Riesgo Operacional con su respectivo nivel de aceptación.

9. Controles

La Clasificadora garantiza una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos. El control a través de procedimientos formales, es responsabilidad del dueño del proceso, identificado en el Manual de Procedimientos Operativos, y el aseguramiento, del funcionario de control interno.

a. Seguridad Lógica

Toda comunicación para solicitar altas de usuarios, así como la adición de privilegios de acceso y remoción de usuarios, deberá ser solicitada por escrito por el área autorizada. La vía de comunicación podrá ser correo electrónico, con copia a la Gerencia General.

La Gerencia General deberá comunicar por escrito al área de sistemas el requerimiento de alta de usuarios nuevos por lo menos 24 horas antes de que la necesidad de uso se presente. En respuesta el área de sistemas deberá generar un nombre de usuario para acceso a red y configurarlo en el equipo asignado para la nueva posición.

La adición de privilegios deberá ser comunicada al área de sistemas para que sea habilitada en un plazo no mayor a 24 horas.

La revocación de privilegios, democión y/o remoción de usuarios, la Gerencia General comunicará al área de sistemas el cese de los mismos, inmediatamente producido el evento. El área de sistemas deberá cambiar la contraseña de acceso tanto del usuario de red como del correo electrónico asignado al usuario revocado en un plazo no mayor a 5 horas. El usuario y sus privilegios de red podrán mantenerse en el sistema hasta que se determine el destino de la información generada y sea seguro eliminarlo.

El área de sistemas conserva un listado de los usuarios y los accesos concedidos a éstos en el sistema. Este será revisado trimestralmente, elevando un informe a modo de recordatorio a la Gerencia General.

Cada usuario en la red tiene asignado su propio nombre de usuario y contraseña, con el cual tiene acceso a su respectiva terminal y a la información que le ha sido confiada. El registro de dicho nombre de usuario está asociado directamente al nombre y apellido de la persona física correspondiente.

Los permisos de acceso asignados evitan la ejecución de herramientas no autorizadas en los sistemas de la compañía.

La lógica de IT en la Clasificadora no requiere por el momento un sistema de seguimiento sobre el acceso y uso de sistemas para detectar actividades no autorizadas. Se aplicará cuando corresponda.

El funcionamiento permite al funcionario ver sólo los archivos de información que se encuentran bajo su responsabilidad, cumpliendo con el principio de mínimo privilegio.

No existe permiso de acceso remoto para ningún usuario de la red. La computación móvil está restringida a una computadora portátil a cargo del Gerente General, la cual tiene su espejo en la información registrada en la estación de escritorio asignada al Gerente General.

Los teléfonos inteligentes personales de los trabajadores no tienen información de la compañía, ni tampoco acceso al correo electrónico de la misma.

b. Seguridad de Personal

La Clasificadora define los roles y responsabilidades relacionados con seguridad de información en el Manual de Organización y Funciones y en el presente documento.

El coordinador de administración y ventas es el encargado de evaluar los antecedentes del personal en base a la legislación vigente y a las políticas internas de la Clasificadora.

El responsable de Seguridad de Información designado por la Gerencia General es el encargado de proponer e implementar capacitaciones que son planteadas en un plan anual.

El Coordinador de Administración y Ventas es quien identifica el incumplimiento por parte de un funcionario y aplica el proceso disciplinario aprobado por la Gerencia General y debe comunicarse con al área de sistemas cuando el vínculo finalice para que las medidas de cambio de contraseña sean aplicadas y /o se verifique la integridad de la información generada por el trabajador cesado.

c. Seguridad Física y Ambiental

La Clasificadora cuenta con servicio de seguridad física para las instalaciones que ofrece información diaria sobre acceso autorizado a la oficina, de igual forma, reporta inmediatamente cuando un tercero no autorizado accede o trata de acceder a las instalaciones reportando en tiempo real a la Gerencia General y al Coordinador de Administración y Ventas, así como, a la estación de policía de la zona.

La Clasificadora cuenta con controles para mitigar las amenazas físicas, se cuenta con aspersores, detectores de humo, extintores.

Se realiza anualmente la revisión de controles por parte de proveedores (extintores) y administrador del edificio (aspersores y detectores de humo).

10. Clasificación de Activos de Información

La Clasificadora ha identificado los activos relacionados a la tecnología de información y los ha dividido en los siguientes grupos:

a. Activos de información puros (activos digitales, activos tangibles, activos intangibles, software de aplicación y sistemas operativos).

b. Activos físicos (infraestructura de TI, Controles de entorno de TI, Hardware de TI, Activos de Servicio de TI.

c. Activos Capital Humano (funcionarios, colaboradores externos, asesores externos, proveedores).

Las responsabilidades se indican en el Manual de Organización y Funciones, Manual de Procedimientos Operativos, Manual de Gestión de Riesgo Operacional y otros documentos internos.

11. Clasificación de la Información

La Clasificadora realiza la clasificación de la información en las siguientes categorías:

- Información privilegiada: es el tipo de información que solamente un grupo de personas conoce o puede tener acceso a ella. Por lo tanto, es información que no es pública o que, en el mejor de los casos, su conocimiento es muy restringido determinada por las normas del mercado de valores y vinculadas. Respecto a este tipo de información la Clasificadora con el objeto de proteger la información privilegiada procede a:
  - Separar la información confidencial de la que no lo es.
  - Enumerar y nombrar los documentos, asuntos y programas que contienen este tipo de información.
  - Suscribir acuerdos de no divulgación.

- Utilizar manuales para los empleados con el fin de enfatizar el empleo, acceso y protección de la información.
- Llevar a cabo programas de orientación y educación para funcionarios y colaboradores externos.
- Divulgar las medidas de protección.
- Crear barreras físicas de seguridad.
- Tomar medidas adicionales para mantener seguros los documentos confidenciales.
- Prevenir la difusión inadvertida a terceros de este tipo de información.
- Desarrollar entrevistas de salida con las personas que dejen de trabajar en la Clasificadora.
- Limitar el acceso de visitantes.
- Llevar a cabo auditorias rutinarias a la información privilegiada.

- Información pública: es el tipo de información que es abierta para todo el público y de fácil acceso. Por lo tanto, cualquier persona la puede conocer. En este caso, la información está a disposición en todo momento sin requerir mecanismos de control.
- Información personal: información del personal, es de manejo interno y está protegida por la ley de protección de datos.

12. Administración de Operaciones y Comunicaciones

La Clasificadora considera relevante el cumplimiento de lo siguiente:

- Procedimiento de control de documentos
- Procedimiento de control de registro de calidad
- Procedimiento y realización de auditorías
- Procedimientos de control de productos no conformes
- Procedimiento de acciones correctivas

- Procedimiento de acciones preventivas

Con la finalidad de minimizar el riesgo de actualizaciones, cambios o modificaciones no autorizadas, la Clasificadora ha determinado que cualquier cambio en el ambiente operativo que incluya modificaciones en los sistemas de información, instalaciones de procesamientos y procedimientos cuente con:

- Autorización formal previa de los cambios propuestos
- Identificación y registro de los cambios significativos propuestos
- Comunicación de detalle de cambios a todas las áreas pertinentes.

La documentación deberá ser mantenida como mínimo por dos (2) años para efectos de control de auditoría externa.

Las responsabilidades del personal, en lo que corresponda, están definidos en el MOF y MPO, asignándose en estos documentos una adecuada segregación de funciones. La separación resulta un mecanismo de control que busca asegurar que ningún funcionario tenga la autoridad o capacidad de ejecutar más de lo establecido en el MOF Y MPO y de esta forma, prevenir riesgos económicos y no económicos. Adicionalmente, los usuarios del sistema sólo tendrán acceso a los recursos que son absolutamente necesarios para realizar sus funciones (principio del mínimo privilegio).

El coordinador de administración y ventas o quien sea designado deberá supervisar la contratación, adquisición, implementación y correcto funcionamiento de las aplicaciones y servicios adquiridos a terceros a fin de garantizar la adecuada operatividad del negocio.

La Gerencia General en coordinación con el colaborador externo de TI analizarán la capacidad de procesamiento con una periodicidad semestral para comprobar el nivel de utilización de los sistemas de almacenamiento, estaciones de trabajo y otros con el fin de no tener inconvenientes en la saturación de los mismos.

El sistema de protección contra intrusiones externas y software malicioso existe a nivel del software instalado en el 100% de los equipos con acceso a red. Los usuarios finales no tienen permisos concedidos para la instalación de software de ningún tipo

La red se encuentra protegida por software de seguridad que impide la ejecución de código malicioso no autorizado que pueda poner en peligro la información almacenada.

Los mensajes de correo electrónico que se intercambien con terceras partes no deberán contener información sensible en formato de texto, sino que ésta deberá ser contenida en archivos adjuntos que se encuentren cifrados. La clave de cifrado no podrá ser compartida en el mismo mensaje de correo, sino que deberá ser enviada utilizando un medio diferente del original para evitar su vulneración en el trayecto.

La información confidencial entre el cliente y el analista será remitida por correo electrónico que incluye archivo encriptado con acceso a una contraseña que va por un canal diferente al original.

El acceso es personal, en caso que el analista no se encuentre y lo supla el analista alterno, se deberá informar previamente al responsable de seguridad de información.

La Clasificadora se obliga a mantener los registros de auditoría por el espacio definido por la norma, en caso no existir un periodo establecido, se considera que debe ser como mínimo por dos (2) años. En el caso de los sistemas, estos se supervisan una vez al año.

13. Adquisición, Desarrollo y Mantenimiento de Sistemas Informáticos

Todos los nuevos sistemas o mejoras en sistemas actuales, así como para aplicativos controles y pruebas previas requieren una evaluación de aseguramiento sobre el ingreso, procesamiento y salida de la información.

La información sensible que deba ser transmitida deberá estar encriptada utilizando la herramienta de encriptación del procesador de texto y / o hoja de cálculo. La clave de encriptación no podrá ser menor de 8 dígitos, y deberá ser una combinación de números, signos y letras en mayúsculas y minúsculas sin utilizar nombres propios o palabras del diccionario.

Se ha determinado que toda implementación de aplicaciones debe ser validada antes de entrar en producción. La responsabilidad de los controles es del responsable de riesgos, existiendo un procedimiento formal de control de cambios soportado, en lo que

corresponda, por sistemas informáticos. El control de cambios es documentado de acuerdo a políticas internas de la Clasificadora.

El responsable de riesgos, respaldado por el colaborador externo de tecnología, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objeto de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. La función implica revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

El responsable de riesgos debe promover la realización de pruebas de vulnerabilidades y hacking con una periodicidad establecida por un ente independiente al área objeto de las pruebas con el fin de garantizar la objetividad del desarrollo de las mismas.

El responsable de riesgos debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético,

El colaborador de TI, revisa periódicamente la aparición de nuevas vulnerabilidades técnicas y las reporta a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos (cuando corresponda).

El colaborador de TI en coordinación con el líder de seguridad de información debe generar y ejecutar o supervisar planes de acción para la mitigación de vulnerabilidades técnicas detectadas en la plataforma tecnológica.

14. Procedimiento de Respaldo

El respaldo de la información de la Clasificadora se realiza en tiempo real, con información almacenada en la nube y con copias de seguridad físicas realizadas en base incremental diaria, mediante copia de seguridad automatizada programada para ejecutarse fuera del horario de jornada laboral. El medio de copia físico es un disco duro externo conectado al servidor.

Los protocolos de seguridad de la compañía establecen una tercera copia de seguridad con periodicidad mensual de copia de seguridad al 100% adicional a la incremental diaria, incluyendo el sistema operativo, que será almacenada en una ubicación física diferente a las oficinas de la Clasificadora.

La copia de respaldo mensual almacenada en una locación distinta al centro de operaciones principal permite restaurar el servidor central en tiempo récord, y la información almacenada en la nube en tiempo real complementa la puesta en marcha inmediata de los servicios críticos sin pérdida de información por eventos fortuitos en el centro de operaciones principal.

15. Gestión de Incidentes de Seguridad de Información

El funcionario o colaborador externo que considere que se está presentando un incidente de seguridad debe proceder a su reporte al líder de seguridad de información a través de correo electrónico con la siguiente información como mínimo:

- Nombre de quien reporta
- Cargo de quien reporta
- Teléfono o email
- Fecha de reporte
- Fecha del incidente
- Equipo o sistema afectado
- Descripción del incidente

Se tienen establecida la estrategia de respuesta de acción ante incidentes de seguridad de información. La atención de los incidentes debe realizarse considerando como mínimo el siguiente procedimiento formal:

- Evaluar el incidente para identificar su clasificación e impacto
- Recolectar la información necesaria y requerida para determinar la causa del incidente con el fin de definir las acciones correctivas que deban ser aplicadas.

- Asegurar la información y/o evidencia recolectada a fin de guardar la correcta y adecuada cadena de custodia y conservación para fines legales que puedan producirse

16. Cumplimiento Normativo

La Clasificadora asegura el cumplimiento de los requerimientos legales, regulatorios, contractuales en todo lo referente a la seguridad de información entre ello el derecho de autor y propiedad intelectual, por lo que el software instalado cumple con los requerimientos de licenciamiento y aspectos normativos.

En cumplimiento con la normativa de protección de datos personales, la Clasificadora promueve la protección de los datos personales de sus funcionarios, colaboradores externos, proveedores y terceros de los que reciba información.

Se establecerán los términos, condiciones y finalidades para los cuales la Clasificadora como responsable de los datos personales y empresariales obtenidos a través de distintos canales, tratará la información de todas las personas y empresas que, en algún momento, por razones de la actividad que desarrolla, haya suministrado datos. En el caso de delegar a un tercero el tratamiento de datos, la Clasificadora exigirá la implementación de los lineamiento y procedimiento necesarios para la protección de los datos. De igual modo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo controles necesarios para preservar aquella información que la Clasificadora conozca y almacene de ellos, velando porque dicha información sea usada exclusivamente para funciones propias de la actividad y no sea publicada, revelada o entregada a terceros sin autorización.

17. Auditoría Externa

La Clasificadora tomará anualmente o cuando corresponda el servicio de auditoría externa para que revise las áreas de sistemas de información, los estándares y procedimientos. La revisión se realizará una vez al año.

18. Programa de Formación

La Clasificadora brinda los procedimientos, políticas y demás elementos teóricos y prácticos a los funcionarios y colaboradores externos que faciliten la correcta implementación del Sistema de Gestión de Seguridad de la Información.

Se consideran los siguientes temas:

- Se realizarán capacitaciones a todos los funcionarios y colaboradores externos de forma anual evaluando el alcance de los objetivos propuestos y su eficacia.
- Se realizarán capacitaciones a los nuevos funcionarios durante el periodo de inducción
- Se publicarán todos los documentos, normas, procesos y demás temas relacionados, en lugares donde todos los funcionarios y colaboradores externos los puedan consultar y se puedan mantener actualizados.
- Se mantendrán la documentación actualizada mediante la continua revisión, por parte de las personas que se encuentran involucradas en los procesos.