CAJA DE VALORES

POLÍTICA
DE SEGURIDAD DE LA INFORMACIÓN

(P-59001 versión 03)

ÍNDICE

1. ALCANCE

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, alineado con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Caja de Valores S.A.

Debe ser conocida y cumplida por toda empresa o persona que utilice servicios informáticos brindados por Caja de Valores S.A.

Se deberá tener identificados todos los activos que se utilizan, entendiéndose por ello, los recursos, personas y medios indispensables para la ejecución de uno o más procesos de negocios que sean relevantes en los resultados esperados de estos últimos.
Entiéndase por Activo Informático a toda aquella tecnología electrónica que es utilizada por la organización para poder operar sus procesos o que faciliten a sus clientes la utilización de sus servicios, como por ejemplo: los sitios web que permiten efectuar transacciones con acciones o bonos, entre los que se encuentran los siguientes:

- La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la Seguridad Informática en esta área es velar por la seguridad de accesos y de los cambios que se realicen.
- Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.
- La información: Esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

2. Sección: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo

Administrar y proteger los recursos de información de Caja de Valores S.A. y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Alcance

Esta Política se aplica en todo el ámbito de Caja de Valores S.A., a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a esta organización a través de contratos o acuerdos con terceros.

Responsabilidad

Todos los Directores y empleados, sea cual fuere su nivel jerárquico, son responsables de la implementación de esta Política de Seguridad de la Información dentro de su área de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para empresa o persona que utilice servicios tecnológicos brindados por la Caja de Valores S.A., cualquiera sea su situación de revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

El **Responsable de Seguridad Informática** cumplirá funciones relativas a la seguridad de los sistemas de información de **Caja de Valores S.A.,** lo cual incluye:

- Supervisar todos los aspectos inherentes a los temas tratados en la presente Política.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad;
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información;
- Garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;
- Promover la difusión y apoyo a la seguridad de la información dentro de Caja de Valores y coordinar el proceso de administración de la continuidad de las actividades de la organización.
- Establecerá un Plan de concientización sobre la seguridad de la información a todos los empleados de Caja de Valores.

Los **Propietarios de la Información y Propietarios de activos** son responsables de:

- Clasificarlos de acuerdo con el grado de sensibilidad y criticidad de los mismos,
- documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
- establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.
- definir los perfiles de las personas que tendrán permisos y accesos.
- asegurar la accesibilidad del documento para quienes necesiten consultarlo y estén habilitados para hacerlo.
- comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.

El **Responsable del Área de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la función de:

- Notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
- Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los códigos de Uso Responsable de los Recursos Informáticos y las tareas de acompañar a la capacitación continua en materia de seguridad que se desprendan de esta política

El **Responsable del Gerencia Divisional Informática** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la organización. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El **Responsable de la Gerencia de Legales** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la organización con sus empleados y con terceros. Asimismo, asesorará en materia legal a la organización, en lo que se refiere a la seguridad de la información.

El **Responsable del Área de Cumplimiento Regulatorio** se encargará de implementar los lineamientos emanados del Comité de Riesgos, dar soporte metodológico al resto de la organización en el tratamiento de los riesgos y evaluar periódicamente con sentido crítico el sistema de gestión de riesgos con el objetivo de proponer las mejoras que se consideren oportunas.

Los **usuarios de la información y de los sistemas** utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

2.1. Componentes de la Política de Seguridad de la información

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

Organización de la Seguridad

Orientado a administrar la seguridad de la información dentro de la organización y establecer un marco gerencial para controlar su implementación.

Gestión de Activos

Destinado a mantener una adecuada protección de los activos de la organización.

Recursos Humanos

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la organización o uso inadecuado de instalaciones.

Seguridad de la Infraestructura

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la organización.

Gestión de Comunicaciones y las Operaciones

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Usuarios de la Información

Orientado a controlar el acceso lógico a la información.

Gestión de Plataforma Productiva

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su adquisición, desarrollo y/o implementación y durante su mantenimiento.

Monitoreo

Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos

Gestión de Continuidad

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Relación con otras partes interesadas

Evitar los riesgos asociados al ecosistema conformado por la interacción con otros mercados, proveedores de servicio y cualquier otra organización asociada" o algo así me parece más fácil de interpretar.

3. Sección: ORGANIZACIÓN DE LA SEGURIDAD

Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de **Caja de Valores S.A.**

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades de la organización pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información

Objetivo

Administrar la seguridad de la información dentro de la organización y establecer un encuadre gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la organización.

4. Sección: GESTIÓN DE ACTIVOS

Generalidades

Los activos de información deben ser clasificados de acuerdo con la sensibilidad y criticidad de la información que contienen o bien de acuerdo con la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la Organización.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Definir los propietarios de los activos y su proceso de actualización periódica

Se debe asegurar que la información reciba un nivel de protección apropiado. La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad:

- **Confidencialidad:** nivel de exposición y exigencia de autorización que tiene que tener la información
- **Integridad:** nivel exigido de controles sobre las modificaciones realizadas a esa información.
- **Disponibilidad**: nivel de necesidad para la operación de la información

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- **CRITICIDAD BAJA**
- **CRITICIDAD MEDIA**
- **CRITICIDAD ALTA**

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deben tener acceso a la misma.

5. Sección: RECURSOS HUMANOS

Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello, que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.

Establecer los acuerdos de Confidencialidad con toda organización externa con la que corresponda.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

6. Sección: SEGURIDAD DE LA INFRAESTRUCTURA

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos para tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la organización.

Proteger el equipamiento de procesamiento de información crítica de la organización ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la Organización.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Responsabilidad

Todo el personal de la organización es responsable del cumplimiento de las buenas prácticas de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas según lo detallada en el Código de uso responsable de recursos informáticos.

7. Sección: GESTIÓN DE COMUNICACIONES Y OPERACIONES

Generalidades

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

8. Sección: GESTIÓN DE PROVISIÓN DE SERVICIOS

Generalidades

Se deberá identificar todos aquellos proveedores que presten servicios relacionados con las áreas de Tecnología y Seguridad de la información para clasificarlos por su riesgo y poder exigir el cumplimiento de las políticas, normas y procedimientos que cumplen cada área

Objetivo

Los proveedores que brinden servicios informáticos deberán cumplir con los requisitos de seguridad establecidos conforme a las políticas, normas y procedimientos de Caja de Valores. En este sentido, los proveedores serán informados formalmente de las normas aplicables en cada caso, debiendo asumir la responsabilidad, tanto directa como derivada, de los hechos y actos de sus empleados o dependientes.

9. Sección: GESTIÓN DE PLATAFORMA PRODUCTIVA

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software

de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Minimizar el riesgo de fallas en los sistemas. Se requiere planificación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido.

10. Sección: USUARIOS DE LA INFORMACIÓN

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Los Propietarios de la Información estarán encargados de:

-Evaluar los riesgos a los cuales se expone la información con el objeto de:

- determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
- definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.

-Aprobar y solicitar la asignación de privilegios a usuarios.

-Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

-Definir un cronograma de depuración de registros de auditoría en línea.

11. Sección: MONITOREO

Generalidades

Las principales tecnologías utilizadas para el procesamiento de la información deben ser monitoreadas en forma segura y completa que permita identificar posibles intrusiones o funcionamiento malicioso o por lo menos que queden los registros necesarios para que pueda efectuarse un análisis forense de las acciones que se realizaron sobre los entornos tecnológicos.

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

12. Sección: GESTIÓN DE LA CONTINUIDAD

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Responsabilidad

Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la organización.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la organización.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la organización.

CONTROL DE CAMBIOS

FECHA	CAMBIO-MOTIVO
Septiembre 2019	*Versión adaptada para publicación externa.*