

## **RS-DC.23/2002**

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

El Superintendente de Valores de El Salvador, considerando:

I. Que con la aprobación del Decreto Legislativo 742, de fecha veintiuno de febrero de dos mil dos, publicado en el Diario Oficial número 57, Tomo N° 354, de fecha 22 de marzo de dos mil dos, el cual contiene la Ley de Anotaciones Electrónicas de Valores en Cuenta, se establecen las condiciones para que el mercado de valores salvadoreño incorpore sistemas de información que permitan la administración de valores.

II. Que para la seguridad de los recursos del inversionista y la confianza de éste en la operatividad de un mercado con valores representados por medio de anotaciones en cuenta, se requiere que las sociedades especializadas en el depósito y custodia de valores, por estar designadas para la realización de el depósito, la custodia y la administración de los valores representados por medio de anotaciones en cuenta, deban implementar políticas y procedimientos de seguridad informática, así como planes ante contingencia, que minimicen los riesgos de pérdida de los valores y la confianza del inversionista.

Por tanto en base al literal k) del Art. 4 y Literal b) del Artículo 22, ambos de la Ley Orgánica de la Ley Orgánica de la Superintendencia de Valores, Art. 80 de la Ley del Mercado de Valores y, el Artículo 16 de la Ley de Anotaciones Electrónicas de Valores en Cuenta, emite las siguientes:

### **NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA DE SOCIEDADES ESPECIALIZADAS EN EL DEPÓSITO Y CUSTODIA DE VALORES.**

#### **I. POLÍTICAS DE SEGURIDAD INFORMÁTICA**

Art. 1.- La presente Resolución establece las normas mínimas de seguridad que deberán establecer y mantener las sociedades especializadas en el depósito y custodia de valores.

Art. 2.- Para efectos de la presente Resolución, deberá entenderse como:

- a) Sistema de Información: conjunto de programas desarrollados internamente o por contratación externa, que automatizan uno o varios procesos, así como también la infraestructura tecnológica que los soporta: Base de Datos, Servidores, Redes y Comunicaciones entre otros.
- b) Respaldo de Datos: proceso de copiado de información a medios digitales para su posterior resguardo.
- c) Restauración de Datos: proceso de recuperación de información desde un archivo almacenado en el servidor o medios magnéticos

## RS-DC.23/2002

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

- d) Políticas de Seguridad: Son todas aquellas medidas que permiten conocer los esquemas de seguridad desarrollados por la empresa en forma general, sin que la información entregada ponga en riesgo la seguridad de la entidad. Estos esquemas pueden desarrollarse en las áreas de sistemas de información, redes, comunicaciones y otras similares.
- e) Plan de seguridad Informática: Conjunto de políticas, normas y procedimientos desarrollados para salvaguardar la información en las empresas.
- f) Correo Electrónico: Herramienta que facilita el intercambio de mensajes electrónicos entre equipos computacionales.
- g) Autenticación: procedimiento que permite validar el acceso de los usuarios a los recursos informáticos.
- h) Control de Acceso: Procesos que permiten validar el ingreso de los usuarios a programas o equipos.
- i) Información Crítica: Toda información indispensable para la gestión operativa y toma de decisiones en una empresa
- j) Recursos Tecnológicos: Componentes de hardware y software necesarios que apoyan la función informática en una organización.
- k) Seguridad Informática: Procedimientos y técnicas de seguridad dedicadas principalmente a proteger la confidencialidad, integridad y disponibilidad de la información.
- l) Plan ante Contingencias: Consiste en el diseño y formulación de planes de acción alternos que permiten la operación en condiciones adversas y proporcionen continuidad a los procesos críticos del negocio
- m) Plataforma Tecnológica: Todos los recursos tecnológicos que tiene una empresa para facilitar el desarrollo de sus operaciones
- n) Interfaces: medio electrónico de interacción entre el usuario y las aplicaciones.
- o) Conexiones Concurrentes: accesos simultáneos a un determinado Sistema

Art. 2.- Las Depositarias deberán elaborar un plan de seguridad informática, el cual deberá regirse por políticas que garanticen la salvaguarda de los recursos de la institución, la confidencialidad de la información y la continuidad de las operaciones.

Todas las políticas definidas en el manual deberán obedecer a la declaración del objetivo de la misma y al compromiso de la gerencia general para el cumplimiento de estas.

Las Políticas de Seguridad Informática definidas por la depositaria deberán incorporar los objetivos, las conductas, las normas, los métodos de actuación y la distribución de responsabilidades, lo cual se constituirá en un documento de requisitos para la implementación de los mecanismos de seguridad definidos.

## **RS-DC.23/2002**

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

Art. 3.- Todas las políticas de seguridad deberán estar autorizadas por la máxima autoridad de la empresa para garantizar su conocimiento, apoyo y asegurar su cumplimiento, además de la asignación de recursos necesarios para su implementación.

Art.4.- Las Depositarias deberán establecer una estructura organizacional de seguridad que diseñe, organice, implemente y de seguimiento al plan de seguridad institucional con la delimitación de responsabilidades claramente identificadas en la estructura definida y avalada por la alta dirección

Art. 5.- Las Depositarias deberán elaborar e implementar, por lo menos, las siguientes políticas de seguridad informática:

- Que apoyen la concientización para la seguridad del personal y la asignación de responsabilidades individuales
- Para la clasificación de los recursos informáticos y el control aplicado a los mismos
- De control de acceso a los recursos de la organización
- Para el desarrollo de sistemas de información y un efectivo control de cambios a los sistemas de información de Las Depositarias
- Que permitan garantizar la seguridad física y del medio ambiente en la organización
- Para el cumplimiento de regulaciones ordenadas por la Ley y la Superintendencia de Valores

### **Políticas para el intercambio digital de información con usuarios externos**

Art. 6. Las Depositarias deberán implementar políticas de seguridad para el intercambio digital de información con usuarios externos.

### **Políticas para el uso de correo electrónico**

Art. 7.- Para garantizar la confidencialidad de la información que viaja vía correo electrónico se deberá implementar políticas para el manejo de cuentas compartidas, la transmisión de información crítica, el uso personal del servicio y mensajes privados, accesos a e-mail en forma remota, correos en cadena y políticas de retención de que garanticen el uso aceptable de este servicio en las Depositarias, entre otros.

# RS-DC.23/2002

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

## II. PROCEDIMIENTOS Y ESTANDARES DE SEGURIDAD INFORMATICA

Art. 8.- Las Depositarias deberán apoyar su gestión de seguridad informática elaborando, implementando y documentando estándares y procedimientos para la administración de cuentas, administración de recursos informáticos, administración de redes y comunicaciones, seguridad física, plan de entrenamiento en seguridad informática, además de velar por el cumplimiento a regulaciones y requerimientos legales.

### Administración de cuentas y seguridad

Art. 9.-Las Depositarias deberán implementar procedimientos y estándares para la administración de cuentas de usuario; incluyendo en esta administración, la creación, suspensión, reactivación, cancelación y eliminación de las mismas, todo lo cual asegure la confidencialidad del acceso a los recursos tecnológicos pertinentes de la empresa.

Los procedimientos y estándares mínimos que Las Depositarias tiene la obligación de establecer son:

- Identificación del sistema de administración de cuentas utilizado por Las Depositarias
- Establecimiento de los estándares utilizados para la formación de cuentas de usuario
- Implementación de los procesos de suspensión, reactivación, eliminación y cancelación de cuentas de usuario
- Descripción de los procesos que involucran conexiones concurrentes.
- Identificación de los menús de usuarios en las aplicaciones y los privilegios asignados por cuenta
- Determinación de grupos de usuarios asociados a procesos críticos en Las Depositarias
- Establecimiento de propietarios de la información y niveles de responsabilidad asignadas por usuario
- Identificación de los sistemas compartidos utilizados en Las Depositarias
- Establecimiento de acuerdos de confidencialidad para procesos que permitan el acceso a información de Las Depositarias a proveedores y consultores
- Establecimiento de procedimientos para garantizar que el acceso de los clientes a transacciones, consultas y confirmaciones se realice en forma segura y confidencial
- Implementación de procedimientos y estándares para la conformación de los nombres de las cuentas
- Establecimiento de procedimientos y estándares para la administración de contraseñas
- Elaboración procedimientos que permitan orientar al personal en el uso de los servicios informáticos para la inducción a los sistemas de información, programa interno de

## **RS-DC.23/2002**

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

divulgación de seguridad informática, y acuerdos de confidencialidad de la información a la que tendrá acceso.

### **Administración de los recursos de la institución**

Art. 10.- Las Depositarias deberán establecer procedimientos y estándares que permitan una eficiente administración de los recursos para garantizar la confidencialidad, integridad y disponibilidad de los mismos, incluyendo como mínimo:

- Procedimientos para clasificar los niveles de confidencialidad de los recursos y asignar propietarios que respondan por la administración de su seguridad
- Procedimientos para administrar la confidencialidad de la información y garantizar la no divulgación de información sensible por el mal uso de la misma
- Procedimientos y estándares para mantener la integridad de la información al modificar, eliminar e ingresar datos en los sistemas y bases de datos de la organización
- Procedimientos y estándares de los respaldos de datos que deben incluir las estrategias de respaldo y restauración, los sistemas de archivos y almacenamiento, como medidas de seguridad que faciliten la disponibilidad de la información
- Procedimientos y estándares para la autenticación y encriptación de la información donde se especifique como mínimo la metodología utilizada, la administración de clave, validaciones de usuarios y algoritmos utilizados.
- Procedimientos para el almacenamiento y destrucción de información que incluyan procesos para copias de correo electrónico, retención y depósito físico de copias, y copias en medio electrónico y duros
- Procedimientos y estándares para el control y aprobación de cambios en los sistemas de información
- Procedimientos para la separación de ambientes de producción, control de calidad y pruebas para el desarrollo de aplicaciones

## **RS-DC.23/2002**

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

- Procedimientos para el acceso a la información de producción para ser utilizada en ambiente de control de calidad

### **Administración de Redes, Comunicaciones y seguridad**

Art. 11.- Es responsabilidad de toda Depositaria implementar procedimientos y estándares para la administración de redes, comunicaciones y seguridad que permitan el control de acceso a conexiones seguras de empleados, clientes y proveedores.

### **Seguridad Física**

Art. 12.- La seguridad física en las instalaciones de las Depositarias deberán incluir tanto los procedimientos y estándares que permitan combatir amenazas latentes como fuego, agua, temperaturas inusuales, terremotos y otros, como también controlar el acceso físico a edificio e instalaciones propiedad de las Depositarias.

### **Monitoreo de Seguridad**

Art. 13.- Las Depositarias deberán implementar procedimientos y estándares de seguridad que permitan realizar el monitoreo a los registros de acceso de los recursos tecnológicos de las Depositarias.

### **Plan de Entrenamiento en Seguridad Informática**

Art. 14.- Las Depositarias deberán desarrollar e implementar un plan de entrenamiento en seguridad informática que deberá incluir como mínimo: políticas para el desarrollo de personal, programa de inducción, acuerdos de confidencialidad de la información, código de ética para los miembros de la organización y entrenamientos para el uso de recursos para empleados, clientes y proveedores.

### **Cumplimiento a regulaciones y requerimientos legales**

Art. 15.- Las Depositarias deberán elaborar procedimientos para garantizar el cumplimiento a regulaciones y requerimientos legales para la adquisición y utilización de las licencias de los programas instalados en la organización.

### **Sanciones e incumplimientos**

Art. 16.- Las Depositarias deberán establecer sanciones por mal uso de información e incumplimiento a políticas y normas aprobadas y divulgadas en la organización.

## **RS-DC.23/2002**

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

### **III. PROPIEDAD DE LOS EQUIPOS Y PROGRAMAS DE LAS DEPOSITARIAS**

Art. 17.- Dada la naturaleza de los servicios de las Depositarias, éstas deberán adoptar medidas que vinculen con el sistema de información y que garanticen la seguridad para la continuidad del servicio y de los desarrollos futuros que requiera emprender las Depositarias o por exigencia del mercado.

Art. 18.- Las Depositarias deberán ser propietaria del equipo y programas que utilice. Alternativamente, podrá contar con un contrato de arrendamiento para el equipo utilizado.

Art. 19.- En caso de arrendamiento las Depositarias deberán exigir un documento que acredite:

- La propiedad de los equipos; o un su defecto, documento que acredita el arrendamiento.
- El arrendamiento con cláusulas y procedimientos que aseguren la confidencialidad necesaria.
- La garantía de la entrega de un servicio acorde con sus necesidades y la posibilidad de un proceso de retiro ordenado hacia otro proveedor de ser necesario, en caso de tener acceso a la información.
- Acreditación de la propiedad de programas de aplicación (incluyendo las interfases con otras instituciones) o en su defecto, contar con los convenios de concesión en uso, o uso permanente a favor de las Depositarias.

### **IV. PLAN ANTE CONTINGENCIA**

Art. 20.- Las Depositarias deberán contar con un Plan de Contingencia que les permita recuperar sus funciones de la forma más rápida posible, de forma tal que aseguren el adecuado y normal desenvolvimiento de sus servicios, respaldando la información y la integridad de la misma. El Plan de contingencias deberá considerar como mínimo:

- Plan ante contingencias diarias
- Plan de recuperación ante desastres
- Plan de retorno a operaciones normales

Art. 21.- Las Depositarias deberán establecer un Sitio Alterno con la plataforma tecnológica necesaria para que los sistemas de información que soportan las operaciones de las Depositarias operen satisfactoriamente en caso de desastres.

Art. 22.- El Plan ante Contingencias deberá ser puesto a prueba al menos con una periodicidad anual. El Plan ha de contar como mínimo con los siguientes elementos:

## **RS-DC.23/2002**

<b>Emisión</b> 14 de octubre de 2002	<b>NORMAS MINIMAS DE SEGURIDAD INFORMÁTICA PARA SOCIEDADES ESPECIALIZADAS EN DEPÓSITO CUSTODIA DE VALORES</b>	<b>Vigencia</b> 14 de octubre de 2002
---	---	--

- Plan ante contingencias de operaciones diarias actualizado y probado.
- Mecanismos de contingencia en operaciones diarias implantadas y probadas.
- Plan de recuperación ante desastres actualizado y probado.
- Sitio Alterno y plataforma tecnológica probada y lista.
- Infraestructura y tecnología de información disponible para el retorno a operaciones normales.
- Equipos de trabajo capacitados.

Art. 22.- Las actualizaciones que se efectúen sobre los Planes ante Contingencia aprobados por la Superintendencia, deberán ser notificados en forma previa a su implementación, para efectos de realizar las pruebas pertinentes sobre los referidos cambios.

Art. 23.- Las depositarias autorizadas a la fecha de vigencia de la presente Resolución, deberán presentar a esta Superintendencia, en un plazo máximo de 15 días hábiles contados a partir de vigencia de la misma, un Plan de Adecuación para sujetarse a lo establecido por ésta.

Art. 24.- La presente Resolución entrará en vigencia a partir de la fecha de emisión.

San Salvador, a los 14 días del mes de octubre de 2002.

**Omar Ernesto Rodríguez Alemán**  
**Superintendente de Valores**