Superintendencia del Mercado de Valores
de la República Dominicana

CIRCULAR
Núm. 08/2023

A: Los participantes del Mercado de Valores indicados en el alcance del Proyecto de Reglamento de Seguridad Cibernética y de la Información en el Mercado de Valores.

Asunto: Autorización de consulta pública del Instructivo del Proyecto de Reglamento de Seguridad Cibernética y de la Información en el Mercado de Valores.

VISTOS:

a. Ley núm. 249-17, del Mercado de Valores de la República Dominicana, que deroga y sustituye la Ley núm. 19-00 del ocho (8) de mayo de dos mil (2000), promulgada el diecinueve (19) de diciembre de dos mil diecisiete (2017) (en lo adelante, la "Ley núm. 249-17").

b. Ley núm. 167-21, de mejora Regulatoria y Simplificación de Trámites, de fecha doce (12) de agosto de dos mil veintiuno (2021).

c. Ley núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, de fecha seis (6) de agosto de dos mil trece (2013).

d. Ley núm. 200-04, General de Libre Acceso a la Información Pública, de fecha veintiocho (28) de julio de dos mil cuatro (2004).

e. Reglamento sobre Gestión Integral de Riesgos para los Intermediarios de Valores.

f. Segunda Resolución de fecha primero (1ro) de noviembre del año dos mil dieciocho (2018), de la Junta Monetaria, que autoriza la publicación del Reglamento de Seguridad Cibernética y de la Información.

g. Proyecto de Reglamento de Seguridad Cibernética y de la Información, cuya consulta pública fue aprobada por el Consejo Nacional del Mercado de Valores mediante la Cuarta Resolución R-CNMV-2023-10-MV, de fecha veintiuno (21) de marzo de dos mil veintitrés (2023).

CONSIDERANDO:

a. Que el artículo 17, numeral 14), de la Ley núm. 249-17, faculta al superintendente del Mercado de Valores a "dictar las resoluciones, circulares e instructivos requeridos para el desarrollo de esta ley y sus reglamentos".

b. Que la Superintendencia del Mercado Valores en su condición de órgano regulador del Mercado de Valores y de conformidad con el artículo 7 de la Ley del Mercado de Valores, tendrá por objeto promover un mercado de valores ordenado, eficiente y transparente, proteger a los inversionistas, velar por el cumplimiento de esta ley y mitigar el riesgo sistémico, mediante la regulación y la fiscalización de las personas físicas y jurídicas que operan en el mercado de valores.

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

c. Que el superintendente del Mercado de Valores es la máxima autoridad ejecutiva de la Superintendencia del Mercado de Valores, teniendo a su cargo la dirección, control y representación de esta.

d. Que es criterio de la Superintendencia del Mercado de Valores la estandarización de formatos y contenido de documentos, la cual ha demostrado ser eficaz y ha contribuido enormemente al buen desenvolvimiento y a la buena organización del mercado.

e. Que el artículo 61 del Reglamento sobre la Seguridad Cibernética y de la Información, dispone que: "*El superintendente del Mercado de Valores podrá establecer, mediante normas técnicas u operativas, el contenido y otros requisitos aplicables para la elaboración, implementación y manejo del programa de Seguridad Cibernética y de la Información de los participantes del mercado de valores*".

f. Que, por su parte, la Ley núm. 167-21, de Mejora Regulatoria y Simplificación de Trámites tiene por objeto definir y articular las políticas públicas dirigidas a la mejora regulatoria y la simplificación de trámites administrativos.

g. Que, conforme la precitada Ley, se define la consulta pública como un mecanismo de participación ciudadana que se utiliza para transparentar el proceso de producción y revisión de las regulaciones, permitiendo la recepción de comentarios por parte de los diferentes grupos interesados y del público en general.

h. Que, por su parte, la Ley núm. 107-13 sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo establece en su artículo 30 "[l]os estándares mínimos y obligatorios de los procedimientos administrativos que procuran la adopción de reglamentos que poseen un alcance general, cuya finalidad es que la Administración Pública obtenga la información necesaria para su aprobación, además de canalizar el diálogo con los interesados y el público en general, "promoviendo el derecho fundamental a la participación ciudadana como sustento de la buena gobernanza democrática".

i. Que el artículo 23 de la Ley núm. 200-04, General de Libre Acceso a la Información Pública, establece que las entidades que cumplen funciones públicas o que administran recursos del Estado "tienen la obligación de publicar a través de medios oficiales o privados de amplia difusión, incluyendo medios o mecanismos electrónicos y con suficiente antelación a la fecha de su expedición, los proyectos de regulaciones que pretendan adoptar mediante reglamento o actos de carácter general, relacionadas con requisitos o formalidades que rigen las relaciones entre los particulares y la administración o que se exigen a las personas para el ejercicio de sus derechos y actividades."

Por tanto:

El superintendente del Mercado de Valores, en el uso de las facultades que le confiere el artículo 17 numeral 14) de la Ley núm. 249-17, resuelve:

1. Autorizar la publicación del aviso en uno o más medios de comunicación impresos de amplia circulación nacional y en el portal institucional, para fines de consulta pública de los participantes del mercado de valores y público, del proyecto de Instructivo del Reglamento sobre la Seguridad Cibernética y de la Información en el Mercado de Valores, cuyo texto se transcribe a continuación:

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

"PROYECTO DE INSTRUCTIVO DEL REGLAMENTO SOBRE LA SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES"

Capítulo I
Aspectos Generales

Artículo 1. Objeto. El presente Instructivo tiene por objeto establecer los procedimientos y requisitos técnicos aplicables que complementarán la elaboración, implementación y manejo del programa de Seguridad Cibernética y de la Información de los Participantes del Mercado de Valores.

Artículo 2. Alcance. Quedan sometidos a las formalidades previstas en el presente Instructivo los Participantes del Mercado de Valores sujetos al cumplimiento del Reglamento sobre la Seguridad Cibernética y de la Información en el Mercado de Valores (en lo adelante, el "Reglamento").

Capítulo II
Requerimientos mínimos para los emisores, auditores externos, sociedades calificadoras de riesgos.

Artículo 3. Requerimientos mínimos. Los emisores, auditores externos y sociedades calificadoras de riesgos deben adoptar un marco de gobernanza de ciberseguridad especial sujeto a la no objeción de la Superintendencia del Mercado de Valores (en lo adelante, la "Superintendencia"). Dicho marco debe incluir los criterios de información definidos en el párrafo III del artículo 4 (Criterios de Información) del Reglamento, las políticas, procesos y estructuras de Gestión de Riesgos definidas con controles pertinentes adaptados a la naturaleza de los Riesgos de ciberseguridad a los que se enfrenta la sociedad y a los recursos de que dispone. Las prácticas efectivas incluyen a modo de referencia:

1) Definir un marco de gobernanza para apoyar la toma de decisiones basadas en la política de Riesgos;
2) Garantizar el compromiso activo de la Alta Gerencia y del consejo de administración sobre los aspectos de Seguridad Cibernética y de la Información;
3) Identificar marcos y estándares para abordar la Seguridad Cibernética y de la Información;
4) Utilizar métricas y umbrales para informar los procesos de gobernanza.

Capítulo III
Contenido Políticas y Procedimientos de los Participantes del Mercado de Valores

Artículo 4. Esquema de las políticas. Las políticas de los Participantes del Mercado de Valores referirán, por lo menos, el siguiente esquema:

1) **Propósito:** debe establecer por qué fueron creados estos documentos y el beneficio esperado de los mismos.
2) **Alcance:** debe indicar el área dentro del Participante del Mercado de Valores a la que le aplica los procesos y actividades establecidos en el documento.
3) **Ámbito:** debe definir su aplicabilidad.

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

4) **Desarrollo**: debe describir el contenido de las políticas, procedimientos y actividades para el control y la Gestión de Riesgo a llevar a cabo por el Participante del Mercado de Valores en materia de Seguridad Cibernética y de la Información.
5) **Responsabilidad:** debe definir quién será responsable de la implementación apropiada de los lineamientos que contenga.
6) **Revisión**: debe establecer los procesos y actividades que conforman la revisión e identificación de brechas y Vulnerabilidades, la frecuencia de ejecución, quien es el responsable de realizarlo y a quien reporta para la toma de decisiones.

Artículo 5. Contenido. Los Participantes del Mercado de Valores deben elaborar políticas y procedimientos para la gestión de la Seguridad Cibernética y de la Información, las cuales se deben encontrar alineadas con su estrategia, reglamentos y leyes, e incluirán de manera enunciativa pero no limitativa, lo siguiente:

1) Seguridad Cibernética y de la Información;
2) Concienciación, educación y capacitación en Seguridad Cibernética y de la Información;
3) Control de Acceso;
4) Seguridad física y ambiental;
5) Temas finales orientados al usuario, tales como:
   a) Uso aceptable de activos en la gestión de activos de la Información;
   b) Escritorio y pantalla limpios;
   c) Transferencia de Información;
   d) Dispositivos Móviles y teletrabajo; y,
   e) Restricciones a las instalaciones y uso del Software.
6) Respaldos de la Información, que no se encuentren comprometidos;
7) Transferencia de Información;
8) Protección contra Software malicioso;
9) Gestión de Vulnerabilidades técnicas;
10) Controles criptográficos;
11) Seguridad de las comunicaciones;
12) Privacidad y protección de la Información personal identificable;
13) Gestión de proveedores;
14) Gestión de activos;
15) Desarrollo seguro de programas;
16) Control de cambios de aplicaciones y equipos de telecomunicación;
17) Plan de Continuidad de Negocio;
18) Política y Procedimientos de Gestión de Riesgos;
19) Gestión de Incidentes o hitos; y,
20) Otros que los Participantes del Mercado de Valores consideren que se deban incluir.

Párrafo. Los Participantes del Mercado de Valores deben contar con declaraciones firmadas por los empleados, contratistas, proveedores, afiliados, usuarios y otras personas que se disponga, en las cuales estos se comprometan a acatar la política y los Procedimientos de seguridad documentados.

Artículo 6. Educación y creación de conciencia. De conformidad con lo establecido en el artículo 11 (Educación y creación de conciencia) del Reglamento, el Participante del Mercado de Valores debe disponer diferentes mecanismos para elevar la conciencia de la seguridad entre los empleados, proveedores de servicios, afiliados o usuarios dentro de los que se citan, como mínimo, los siguientes:

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

1) Proporcionar concienciación y formación en relación a los roles y responsabilidades de forma regular para que los empleados y partes externas entiendan la importancia de los controles, la Integridad, Confidencialidad, seguridad y privacidad de la Información del Participante del Mercado de Valores en todas sus formas;

2) Establecer programas continuos de sensibilización sobre el rol de los empleados en la Seguridad Cibernética y de la Información, el uso correcto de los sistemas de Información e Infraestructura Tecnológica y la gestión de sus Riesgos a través de los programas de inducción, cápsulas informativas, boletines, charlas concernientes a la seguridad y cualquier otro mecanismo de notificación hábil;

3) Efectuar ejercicios simulados de campaña dirigida para mejorar los procedimientos de seguridad;

4) Instaurar programas continuos de capacitación técnica dirigidos a los empleados responsables de la Seguridad Cibernética y de la Información;

5) Verificar regularmente que el personal responsable de la Seguridad Cibernética y de la Información tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación o experiencia y verificar que estas se mantienen con programas de capacitación y certificación en su caso; y,

6) Provisionar los recursos adecuados para apoyar la efectividad de los programas continuos de sensibilización de Seguridad Cibernética y de la Información.

Artículo 7. Clasificación y etiquetado de la Información. Las políticas y procedimientos que desarrollen los Participantes del Mercado de Valores, conforme lo establecido en el artículo 15 (Clasificación y etiquetado de la Información) del Reglamento, como mínimo, debe contemplar lo siguiente:

1) Procedimientos de gestión de documentos físicos y digitales que incluyan las etapas de creación, clasificación, almacenamiento, adquisición, modificación y destrucción de documentos; los mecanismos de control para la protección y acceso de la Información acorde a su nivel de sensibilidad, Confidencialidad y los períodos de retención de los mismos, las responsabilidades de los empleados y proveedores de servicios en torno a la gestión documental;

2) Comunicar a sus empleados los esquemas de clasificación de la Información;

3) Establecer los mecanismos correspondientes (encabezados, pies de página, firmas digitales, sellos físicos o digitales, entre otros) y las etiquetas que identifiquen la clasificación de cada uno de los activos de Información; y,

4) Tomar las medidas correspondientes para evitar que la Información sensible y Confidencial en formato físico salga de las instalaciones sin autorización de los órganos correspondientes para dichos fines.

Artículo 8. Gestión de identidades y Mecanismo de Control de Acceso. Las políticas y Procedimientos de gestión de identidades y de Mecanismos de Control de Acceso que apliquen

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

Los Participantes del Mercado de Valores a los empleados, personal contratado y terceros que tengan Acceso a los sistemas de Información e Infraestructura Tecnológica, deben incluir:

1) Procedimientos documentados para la administración y autenticación de identidades a nivel institucional:

   a) Procedimientos de validación de identidades previo a la creación de cuentas de usuario; y,
   b) Procedimientos de identificación, autenticación, inicio de sesión y administración de usuarios.

2) Procedimiento documentado de asignación de roles y privilegios por tipo de usuario y componente de la Infraestructura Tecnológica debe considerar:

   a) La política de Seguridad Cibernética y de la Información de la entidad;
   b) El esquema de clasificación de activos de Información; y,
   c) Los requerimientos fijados por los propietarios de los activos de Información y de las aplicaciones críticas del negocio.

3) Procedimiento documentado para el Control de Acceso para los usuarios a los distintos componentes de la Infraestructura Tecnológica del Participante del Mercado de Valores basado en los principios del menor privilegio, el cual debe implementarse en:

   a) Sistemas de Información y aplicaciones del negocio;
   b) Redes de datos y equipos de red;
   c) Base de Datos;
   d) Dispositivos de computación personal para uso institucional; y,
   e) Cualquier otro componente de la Infraestructura Tecnológica que sea determinado por la entidad.

4) Establecimiento de directrices generales para la asignación y utilización de cuentas privilegiadas en los sistemas de Información y aplicaciones del negocio que regularán la asignación y el uso aceptable de las referidas cuentas a los casos que estrictamente lo ameriten tras obtener la autorización escrita por parte del órgano interno aplicable, en las cuales se estipule:

   a) Una revisión previa de los privilegios por parte del personal responsable, con el fin de confirmar que los mismos están aplicados correctamente;
   b) Un registro de las identidades reales de cada uno de los usuarios, así como los identificadores de acceso y el nivel asignado de privilegio;
   c) Una notificación al usuario sobre los términos y condiciones del uso de las cuentas privilegiadas;
   d) En caso de los usuarios cuyos roles asignados ameriten realizar funciones especiales como autorizaciones y otros tipos de transacciones financieras, se debe implementar mecanismos de doble factor de autenticación para la realización de estas funciones; y,
   e) Los procedimientos de revisión periódica de los privilegios asignados.

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

5) Procedimientos documentados para la gestión de las autorizaciones de los accesos a los usuarios considerando, como mínimo, los siguientes aspectos:

   a) Asignación de privilegios de Acceso para cada usuario de manera individual;

   b) Aplicación de los principios del menor privilegio para la asignación de roles predefinidos a los usuarios;
   c) Nomenclaturas y mecanismos que imposibiliten el uso o reasignación de nombres usuarios previamente utilizados;
   d) Revisión periódica a fin de asegurar que los privilegios asignados continúan siendo los apropiados para el desempeño adecuado de las funciones del usuario, incluyendo, pero no limitado a, cambios de funciones departamentales o desvinculación con el Participante del Mercado de Valores, entre otros;
   e) Autorización para usuarios con Acceso privilegiado global en los casos que sea estrictamente necesario; y,
   f) Revocación del Acceso a todo empleado y parte externa como consecuencia de la desvinculación de su empleo, terminación del contrato o acuerdo, o cambios internos de área o funciones.

Párrafo. Los Mecanismos de Control de Acceso deben estar basados en:

   a) Resultados de las evaluaciones de Riesgo Tecnológico del Participante del Mercado de Valores;
   b) Requerimientos de Control de Acceso;
   c) Evaluación de la funcionalidad de los Mecanismos de Control de Acceso; y,
   d) La identificación de otros factores adicionales relacionados con los fabricantes de los equipos y sistemas que conforman la Infraestructura Tecnológica, así como sus niveles de interconexión e interoperabilidad con los sistemas de seguridad física.

Artículo 9. Monitoreo Continuo de la capacidad de los sistemas y la Infraestructura de Tecnología de la Información. En adición a lo dispuesto en el artículo 35 (Monitoreo Continuo) del Reglamento, el Monitoreo Continuo de los Participantes del Mercado de Valores, como mínimo, debe contemplar los siguientes aspectos:

1) Mecanismos para el aseguramiento de la disponibilidad de espacio en disco y la no interrupción del proceso de registro tras alcanzar el límite de almacenamiento;

2) Procedimientos para las proyecciones de demanda, de forma que se pueda programar el incremento de capacidad de los sistemas previo a que se materialice el estancamiento o sobrecarga en los flujos de datos proyectados. Estos deben incluir de manera enunciativa, pero no limitativa, los siguientes aspectos:

   a) Eliminación de datos obsoletos;
   b) Cierre de aplicaciones, sistemas, Base de Datos o ambientes;
   c) Optimización de procesos por lote y planificados; y,
   d) Optimización de consultas de aplicación lógica o de Base de Datos.

3) Rendimiento de las aplicaciones, los sistemas y las redes en relación con los objetivos acordados.

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

Artículo 10. Prevención y detección de intrusos. En adición a lo establecido en el artículo 36 (Prevención y detección de intrusos) del Reglamento, los Participantes del Mercado de Valores deben implementar la prevención y detección de intrusos contemplando, como mínimo, los siguientes aspectos:

1) Mecanismos de detección de intrusos en los sistemas críticos y redes de Información para la detección de actividades y comportamientos inusuales, inaceptables e inesperados en los sistemas de la Información, aplicaciones del negocio y demás componentes de la Infraestructura Tecnológica;

2) Procedimientos documentados para la detección y prevención de Acceso no autorizado por intrusos contemplando los siguientes elementos:

    a) Identificación de las actividades no autorizadas;
    b) Análisis de intrusiones sospechosas;
    c) Respuesta a diferentes tipos de ataques; y,
    d) Procedimientos para la colaboración con los responsables de las operaciones tecnológicas.

Artículo 11. Protección de Software malicioso. Los Participantes del Mercado de Valores deben considerar directrices para la protección de Software malicioso, dentro de las cuales se encuentran, de manera enunciativa pero no limitativa, las siguientes:

1) Procedimiento que establezca la prohibición del uso de Software no autorizado;
2) Implementación de controles que previenen o detectan el uso de sitios web maliciosos;
3) Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a Información no solicitada (por ejemplo, Software espía y correos de *phishing*);
4) Uso y despliegue de soluciones automatizadas para la minimización de los Riesgos asociados al Software malicioso en la organización que contemple un ciclo de detección, identificación, mitigación y recuperación;
5) Procedimientos documentados para la protección contra el Software malicioso que contemplen:

    a) Instalación, configuración, mantenimiento y gestión centralizada de sistemas de protección contra Software malicioso;
    b) Revisión de la efectividad periódica de las soluciones de protección contra Software malicioso para verificar que las mismas no se encuentren infectadas, siguiendo las recomendaciones del fabricante para estos fines; y,
    c) Gestión de Incidentes relacionados con Software malicioso en múltiples niveles (alto, medio, bajo) y su posterior divulgación a los empleados y terceros.

6) Instalación y despliegue de sistemas para la protección contra Software malicioso en todos los dispositivos de computación, tales como, servidores, dispositivos de computación personal, equipos de oficina y cualquier otro dispositivo que forme parte de la Infraestructura Tecnológica del Participante del Mercado de Valores;

7) Realización de análisis y escaneos periódicos a los componentes de la infraestructura, incluyendo los elementos siguientes:

    a) Firmware (incluyendo el BIOS y la memoria);

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

b) Registro maestro de arranque de los discos duros;
c) Archivos esenciales del sistema operativo;
d) Archivos protegidos (archivos comprimidos, protegidos por contraseña);
e) Medios de almacenamiento portátiles;
f) Recursos compartidos de red, incluyendo repositorios de archivos; y,
g) Tráfico de red entrante y saliente a la red corporativa.

8) Procedimiento continuo para el monitoreo de los servidores y dispositivos de computación personal, con el fin de asegurar que el sistema de protección contra Software malicioso no se encuentre deshabilitado en estos equipos, que esté configurado correctamente y que las actualizaciones sean aplicadas.

Artículo 12. Gestión de la red. En adición a lo establecido en el artículo 38 (Gestión de la Red) del Reglamento, la configuración de dispositivos de la red y la gestión de red física del Participante del Mercado de Valores debe considerar lo siguiente:

1) **Configuración de dispositivos de la red:** los controles que se deben considerar de manera enunciativa, pero no limitativa, son:

a) Dispositivos de red configurados de acuerdo con las prácticas estándar y conocidas de administración de la seguridad de dichos dispositivos y los principios de arquitectura de Seguridad Cibernética y de la Información;
b) Procedimiento para la segmentación entre redes con distintos niveles de seguridad;
c) Restricción de Acceso a la consola de configuración de dispositivos de la red, ubicada en centros de datos protegidos o salas de almacenamiento seguras; y,
d) Configuraciones adecuadas de seguridad de los dispositivos de red, según las recomendaciones del fabricante o procedimientos internos definidos para estos fines.

2) **Gestión de la red física:** los puntos de accesos a la red deben estar protegidos por mecanismos de Control de Acceso, como son:

a) Controles físicos para la protección de cables de telecomunicaciones y puntos de Acceso a la red contemplando el etiquetado de los equipos y cableado, ocultamiento del cableado, uso de conductos blindados, bloqueo de los puntos de red para impedir que *hosts* no autorizados, con direcciones MAC desconocidas, se conecten a la LAN, y el aprovisionamiento de fuentes alternativas.

b) Documentación de la arquitectura de red, contemplando lo siguiente:

i. Diagramas de las redes que muestren todos los nodos y conexiones de las redes internas para cada entorno local;
ii. Inventario de equipos de comunicación, sistemas y aplicaciones críticas asociadas, enlaces y proveedores de servicios externos;
iii. Esquemas de las centrales telefónicas, matriz de cableado y equipos desplegados;
iv. Procedimiento para actualización y revisión periódica de la arquitectura de red; y,

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

v. Inspecciones físicas, verificando Integridad de la red y cualquier uso indebido o sospechoso.

Artículo 13. Comunicaciones electrónicas. Las comunicaciones electrónicas incluyen los servicios de comunicación de voz, cuyos procedimientos deben contemplar:

1) Solicitud, aprobación y revocación de acceso al servicio;
2) Términos y condiciones de uso de los servicios;
3) Mecanismos de registro y autenticación de los usuarios,
4) Configuraciones de seguridad conforme al Marco de Trabajo; y,
5) Definición de controles específicos para estos servicios, tales como, el despliegue de herramientas de monitoreo, instalación de componentes de resiliencia y redundancia, segregación y cifrado del tráfico de voz del resto del tráfico de red utilizando VLAN, esquema de gestión de Vulnerabilidades, aplicación de correctivos y actualizaciones de Software, cifrado del tráfico de voz, registro de eventos, así como, la protección de los buzones de voz contra el Acceso no autorizado.

Artículo 14. Gestión de proveedores externos. Los Participantes del Mercado de Valores que contraigan obligaciones contractuales con proveedores externos de productos o servicios tecnológicos, deben asegurar la integración de los requerimientos de Seguridad Cibernética y de la Información, tomando en consideración los aspectos siguientes:

1) Tercerización: Este proceso debe contemplar, de manera enunciativa, pero no limitativa, los siguientes aspectos:

   a) Procedimientos documentados para la gestión de los Riesgos asociados a la contratación de proveedores externos de productos o servicios tecnológicos, los cuales deben incluir lo siguiente:

      i. Identificación y evaluación de la Información crítica que será compartida con los proveedores externos. Este proceso de evaluación debe incluir la clasificación de la Información que puede o no ser compartida con proveedores externos de acuerdo a las políticas de privacidad del Participante del Mercado de Valores;
      ii. Asistencia a las unidades de adquisiciones en la redacción de los documentos de solicitud de propuestas para la adquisición de bienes y servicios para asegurar la inclusión de requerimientos de Seguridad Cibernética y de la Información;
      iii. Selección de proveedores acreditados, fiables y homologados que deberán estar registrados en una Base de Datos de proveedores, categorizando los mismos desde la perspectiva de Seguridad Cibernética y de la Información;
      iv. Revisión de las propuestas técnicas recibidas para asegurar el cumplimiento de las mismas con los requerimientos de Seguridad Cibernética y de la Información del Participante del Mercado de Valores; y,
      v. Asistencia a los comités de adquisiciones en los procesos de negociaciones de los contratos, incorporando los requisitos de Seguridad Cibernética y de la Información en los mismos.

2) Requisitos de seguridad a los proveedores externos: Dentro de los requisitos de seguridad que los Participantes del Mercado de Valores deben efectuar se encuentran los siguientes:

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

a) Revisar los aspectos de Seguridad Cibernética y de la Información de las relaciones del proveedor con sus propios proveedores;
b) Validar que el proveedor mantiene la suficiente capacidad de servicio junto con los planes realizables diseñados para asegurar que los niveles de continuidad de servicio acordados se mantienen después de fallas o desastres importantes; y,
c) Obligar al proveedor de entregar periódicamente un informe sobre la efectividad de los controles y el acuerdo sobre la corrección oportuna de las cuestiones pertinentes planteadas en el mismo.

3) Adquisición o arrendamiento de equipos y sistemas tecnológicos: El proceso de adquisición o arrendamiento de equipos y sistemas tecnológicos debe basarse en guías de referencia para la selección y aprobación de proveedores de equipos, aplicaciones y servicios, así como prever los requerimientos técnicos de seguridad aprobados por el comité funcional de Seguridad Cibernética y de la Información o por el órgano correspondiente, asegurando que estos brinden la funcionalidad requerida y no comprometan la Seguridad Cibernética y de la Información sensible del Participante del Mercado de Valores durante su ciclo de vida; y,

4) Inclusión de aspectos de Seguridad Cibernética y de la Información en los contratos con proveedores de servicios, especificando lo siguiente:

a) Restricciones para el intercambio de Información del Participante del Mercado de Valores con terceros;
b) Compromiso por parte de proveedores y subcontratistas para cumplir con los requerimientos de Seguridad Cibernética y de la Información fijados por el Participante del Mercado de Valores y entes reguladores;
c) Requerimientos para el aseguramiento de la protección continúa de la Información del negocio antes, durante y después de la prestación de un servicio;
d) Obligaciones de cada parte contractual de implementar un conjunto acordado de controles incluyendo el Control de Acceso, la evaluación del desempeño, la supervisión, el informe y la auditoría; y,
e) Derechos a auditar los procesos y controles de los proveedores relacionados con el acuerdo.

Artículo 15. Gestión de desarrollo de sistemas. Los Participantes del Mercado de Valores que mantengan en su estructura orgánica un área de desarrollo de sistemas, deben establecer políticas y procedimientos para gestión de desarrollo de sistemas, las cuales contemplarán, como mínimo, las disposiciones siguientes:

1) **Metodología de desarrollo de sistemas:** La metodología de desarrollo de sistemas debe considerar los aspectos siguientes:

a) Documentación de análisis y especificación de los requisitos de seguridad:

i. Especificación de requerimientos, incluyendo los relativos a Seguridad Cibernética y de la Información;
ii. Diseño, codificación y prueba de las aplicaciones en base al Marco de Trabajo de desarrollo seguro de sistemas, aplicaciones y servicios digitales;

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

iii. Cumplimiento con los requerimientos legales y regulatorios, incluyendo los relacionados con la privacidad de la Información, así como, con los requerimientos contractuales con terceros; y,
iv. Adhesión a las políticas internas de Seguridad Cibernética y de la Información.

b) Documentación de requerimientos de desarrollo de sistemas, incluyendo lo siguiente:

i. Uso de buenas prácticas de desarrollo seguro sin que las mismas vayan en detrimento de los tiempos de entrega de los componentes del proyecto;
ii. Evaluación independiente del código fuente de las aplicaciones por parte de empleados que no estén trabajando en el mismo equipo de desarrollo y que cuente con las habilidades y conocimientos en el lenguaje de programación utilizado, así como, en aspectos de Seguridad Cibernética y de la Información;
iii. Desarrollo de pruebas de rendimiento en ambientes de prueba separados de los ambientes de desarrollo y producción;
iv. Responsabilidades individuales para el personal de desarrollo, pruebas e implementación segregadas; y,
v. Política para la revisión y adecuación de la misma conforme al surgimiento de nuevas técnicas y prácticas de desarrollo, entrega y diseño de arquitectura de aplicaciones y servicios digitales, así como el surgimiento de nuevas técnicas y estándares de seguridad.

c) La metodología de desarrollo debe requerir al inicio de cada nuevo proyecto, actividades iniciales que incluyan:

i. Notificación al área responsable de la Seguridad Cibernética y de la Información, sobre el inicio de un nuevo proyecto:
ii. Evaluaciones de las necesidades para la Confidencialidad, Integridad y disponibilidad de la Información;
iii. Aplicación de los esquemas de clasificación de la Información del Participante del Mercado de Valores en el desarrollo de sistemas, servicios y aplicaciones del negocio.

d) Capacitación a los desarrolladores sobre la aplicación de técnicas de seguridad en el desarrollo de sistemas, servicios y aplicaciones digitales;
e) Uso de la metodología seleccionada por parte de terceros contratados para el desarrollo de sistemas y aplicaciones del negocio, así como, para componentes del mismo; y,
f) Monitoreo Continuo de la adherencia de la metodología definida por parte de los equipos de desarrollo en cada una de sus fases.

2) **Entornos de desarrollo de sistemas:** Los entornos de desarrollo de sistemas deben implementar mecanismos para asegurar la privacidad y protección de los datos de carácter personal en los ambientes de preproducción (aseguramiento de la calidad) y producción dentro de los que se encuentran:

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

a) Controles para la protección del código fuente contra el Acceso, modificación y divulgación no autorizada a través de los entornos de desarrollo de sistemas del Participante del Mercado de Valores, así como, la remoción de Información, tales como: detalles de autenticación, comentarios de los desarrolladores en las aplicaciones e informaciones sensibles previo a su despliegue en los entornos de producción;
b) Aplicación estricta del control de versiones mediante la gestión de configuraciones, el registro de Acceso al código fuente y el mantenimiento de un repositorio de versiones anteriores debidamente documentado;
c) Mecanismos de prevención de descarga y ejecución de código malicioso en los entornos de desarrollo;
d) Política de resguardo de copias del código fuente, cuando fuese desarrollado por terceros, a través de mecanismos digitales de custodia;
e) Control de versiones mediante la gestión de configuraciones, el registro de Acceso al código fuente y el mantenimiento de un repositorio de versiones anteriores y experimentales debidamente documentado.

3) **Aseguramiento de la calidad:** El desarrollo de los sistemas debe realizarse siguiendo normas y pruebas de calidad que procuren que los controles y requisitos de Seguridad Cibernética y de la Información acordados sean implementados durante el ciclo de desarrollo del mismo, lo cual incluye:

a) Procedimientos documentados de aseguramiento de la calidad, contemplando las actividades de verificación de la seguridad durante el ciclo de vida de desarrollo de los sistemas y aplicaciones, los cuales deben incluir lo siguiente:

i. Verificación de los requerimientos de seguridad de la aplicación conforme a la evaluación de Riesgos;
ii. Mecanismos para asegurar el correcto funcionamiento de los controles de seguridad desarrollados conforme a los requerimientos; y,
iii. Mecanismos para el aseguramiento del uso de las metodologías de desarrollo de sistemas del Participante del Mercado de Valores por parte de los empleados involucrados en el desarrollo.

b) Identificación y documentación de defectos o fallos de seguridad encontrados en los sistemas, así como, de los correctivos aplicados, previo a su despliegue en los entornos de producción; y,
c) Documentación de defectos y Vulnerabilidades encontradas en los sistemas, aplicaciones y servicios digitales del Participante del Mercado de Valores, la finalidad de que las mismas sean corregidas de manera oportuna y validadas por el responsable de desarrollo de sistemas.

2. Informar a los Participantes del Mercado de Valores que la Superintendencia del Mercado de Valores puede solicitar auditorías en materia de Seguridad Cibernética y de la Información, en función de cualquier hallazgo o si ocurre un evento que así lo requiera.

3. Informar a los Participantes del Mercado de Valores que la Superintendencia del Mercado de Valores puede organizar ejercicios para identificar vulnerabilidades o debilidades en la entidad sobre Seguridad Cibernética y de la Información.

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5

4. Informar a los Participantes del Mercado de Valores y al público que quedan incorporados al presente Instructivo los términos definidos por la Ley núm. 249-17 y sus reglamentos de aplicación.

5. Otorgar un plazo de cuarenta y cinco (45) días hábiles para recabar la opinión de los participantes del mercado de valores, sectores interesados y público, a partir del día hábil siguiente a la publicación de la presente.

6. Instruir a la Dirección de Regulación e Innovación de la Superintendencia del Mercado de Valores a publicar la presente Circular en la página web de la institución.

En Santo Domingo, Distrito Nacional, capital de la República Dominicana, a los trece (13) días del mes de julio del dos mil veintitrés (2023).

Ernesto Bournigal Read
Superintendente

SUPERINTENDENCIA DEL MERCADO DE VALORES DE LA REPÚBLICA DOMINICANA

EBR/cp/cg/gf/jv

Dirección de Regulación e Innovación

Av. César Nicolás Penson No. 66, Gascue, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http://www.simv.gob.do | info@simv.gob.do | RNC: 4-01-51572-5