BYMA
Bolsas y Mercados Argentinos

POLÍTICA
DE SEGURIDAD DE LA INFORMACIÓN

P-81000 – versión 04

ÍNDICE

INTRODUCCIÓN

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 **Bolsas y Mercados Argentinos S.A. (en adelante "BYMA").**

Debe ser conocida y cumplida por todo colaborador de BYMA, sea cual fuere su nivel jerárquico y su situación de revista.

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.

1. OBJETIVO

Establecer los lineamientos para administrar y proteger los recursos de información de BYMA 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.

2. ALCANCE

Esta Política se aplica en todo el ámbito de BYMA, 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.

3. GENERALIDADES Y DEFINICIONES

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

<u>Responsabilidades</u>

Destinado a que todos los Directores y colaboradores, sea cual fuere su nivel jerárquico, sean 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.

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.

Desarrollo Organizacional y Gestión de Personas

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.

4. DESARROLLO

4.1 Responsabilidad

La Política de Seguridad de la Información es de aplicación obligatoria por todo colaborador de BYMA, cualquiera sea su situación de revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

BYMA tiene designado un Responsable de Seguridad de la información, quien velará por el cumplimiento de esta Política. A tales fines, contará con la colaboración y asesoramiento de las diferentes Áreas y Gerencias de la Entidad, ello según el siguiente esquema de funciones:

La **Gerencia de Seguridad** es el área encargada de la ejecución, seguimiento e implementación de las siguientes funciones relativas a la seguridad de los sistemas de información de BYMA , lo cual incluye:

Supervisar todos los aspectos inherentes a los temas tratados en la presente Política.

Procurar la segregación de funciones al momento de la gestión de accesos a los sistemas y distintas plataformas.

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 BYMA 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 BYMA.

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.

La **Gerencia de Desarrollo Organizacional y Gestión de Personas** o quién desempeñe esas funciones, cumplirá la función de:

Notificar a todo colaborador 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

La **Gerencia de Tecnología** 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.

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 colaboradores y con terceros. Asimismo, asesorará en materia legal a la organización, en lo que se refiere a la seguridad de la información.

El **Responsable de Riesgo Integral** se encargará de implementar los lineamientos emanados del Comité de Riesgo, 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 riesgo 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.

4.2 Organización de la seguridad

4.2.1 Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de BYMA.

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.

4.2.2 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.

4.2.3 Compromiso de la Dirección con la seguridad de la información

La seguridad de la información es una responsabilidad de la organización compartida por todas las Autoridades (Directores y Síndicos), Funcionarios y colaboradores. La organización

contará con un Comité de Tecnología y Seguridad de la Información cuyos integrantes serán designados por el directorio de la entidad y funcionará de acuerdo con el reglamento del mismo.

4.3 Gestión de activos

4.3.1 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.

4.3.2 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.

4.3.3 Responsabilidad

Los Propietarios de los Activos son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir las funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo con lo establecido en la presente Política.

Todos los activos deben ser inventariados y contar con un propietario nombrado. Los

propietarios deben identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

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 debe 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.

4.4 Desarrollo Organizacional y Gestión de Personas (DOyGP)

4.4.1 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 a los colaboradores 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.

4.4.2 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 los colaboradores e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como colaborador.

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.

4.4.3 Responsabilidad

La Gerencia de DOyGP se asegurará que sean incluidas las funciones relativas a la seguridad de la información en las descripciones de puestos de los colaboradores, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Acuerdos de Confidencialidad con organizaciones externas y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

La Gerencia de Legales participará en la confección del Acuerdo de Confidencialidad a firmar por toda organización externa que desarrolle funciones para BYMA, participará también en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

4.5 Seguridad de la infraestructura

4.5.1 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.

4.5.2 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.

4.5.3 Responsabilidad

La Gerencia de Seguridad Informática definirá junto con la Gerencia de Tecnología y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental que se definan.

La Gerencia de Tecnología asistirá a la Gerencia de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo con las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la organización.

Las Gerencias Operativas definirán los niveles de acceso físico del personal de la entidad a las a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la organización cuando lo crean conveniente.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Tecnología y Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

Todos los colaboradores de la organización son responsables de la protección de la información según lo detallada en el Código de uso responsable de recursos informáticos.

4.6 Gestión de comunicaciones y operaciones

4.6.1 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.

4.6.2 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.

4.6.3 Responsabilidad

La **Gerencia de Seguridad Informática** tendrá a su cargo, entre otros:
Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.
Definir procedimientos para el manejo de incidentes de seguridad y para la administración

de los medios de almacenamiento.
Definir y documentar una norma clara con respecto al uso del correo electrónico.
Controlar los mecanismos de distribución y difusión de información dentro de la organización.
Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la organización.
Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

La **Gerencia de Tecnología** tendrá a su cargo lo siguiente:
Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones.
Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
Asegurar el registro de las actividades realizadas por el colaborador operativo, para su posterior revisión.
Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
Participar en el tratamiento de los incidentes de seguridad, de acuerdo con los procedimientos establecidos.

La Gerencia de Seguridad Informática junto con la Gerencia de Tecnología y la Gerencia de Legales de la organización, evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

4.7 Gestión de provisión de servicios

4.7.1 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.

4.7.2 Objetivo

Los proveedores que brinden servicios informáticos deberán cumplir con los requisitos de seguridad establecidos conforme a las políticas, normas y procedimientos de BYMA. 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.

4.7.3 Responsabilidad

La Gerencia de Seguridad Informática tendrá a su cargo, entre otros:

- Establecer las configuraciones de seguridad mínima que deberán cumplir los proveedores.

- Definir el máximo nivel de acceso que se le puede otorgar a un proveedor.
- Documentar los desvíos a lo establecido en materia de seguridad con relación a algún proveedor.

La Gerencia de Tecnología tendrá a su cargo lo siguiente:

- Implementar las configuraciones de seguridad mínima que deberán cumplir los proveedores
- Evaluar a los proveedores desde el cumplimiento de las políticas, normas y procedimientos de seguridad.
- Velar por el cumplimiento de los proveedores
- Comunicar los incidentes que ocurran relativos a la Seguridad de la Información.

La Gerencia de Legales será responsable de:

- Contemplar en los contratos con los proveedores lo exigido por Seguridad Informática
- Establecer sanciones posibles por su falta de cumplimiento de los proveedores o de sus empleados.

4.8 Gestión de plataforma productiva

4.8.1 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.

4.8.2 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.

4.8.3 Responsabilidad

La Gerencia de Seguridad Informática junto con el Propietario de la Información, con la posibilidad de asesoría de la Unidad de Auditoría Interna – conformada y designada por BYMA, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

La Gerencia de Seguridad Informática, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, la Gerencia de Seguridad Informática definirá junto con la Gerencia de Tecnología, los métodos de encriptación a ser utilizados.

Asimismo, la Gerencia de Seguridad Informática cumplirá las siguientes funciones:
- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

- La Gerencia de Tecnología propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

- La Gerencia de Seguridad Informática incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. La Gerencia de Legales participará en dicha tarea.

4.9 Usuarios de la información

4.9.1 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.

4.9.2 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.

4.9.3 Responsabilidad

La Gerencia de Seguridad Informática estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades (logs); y el ajuste de relojes de acuerdo con un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Asegurarse de que se realice periódicamente un control sobre la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar periódicamente el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

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.

La Gerencia de Tecnología cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de “enrutadores”, “gateways” y/o

firewalls adecuados para subdividir la red y recomendar el esquema apropiado.

- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades (logs) de usuarios de acuerdo con lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

4.10 Monitoreo

4.10.1 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.

4.10.2 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.

4.10.3 Responsabilidad

El Comité de Tecnología y Seguridad de la Información será responsable de implementar los medios y canales necesarios para que la Gerencia de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

La Gerencia de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Tecnología y Seguridad de la Información, a los propietarios de la información.

4.11 Gestión de la continuidad

4.11.1Objetivo

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.

4.11.2 Responsabilidad

La Gerencia de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

El Responsable de Riesgo integral, con el acompañamiento de la Gerencia de Tecnología, 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.

Los Responsables de cada proceso revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades de la organización aún no reflejadas en los planes de continuidad.

Los responsables de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Tecnología y Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la organización frente a interrupciones imprevistas.

4.12 Relación con otras partes interesadas

4.12.1 Objetivo

Direccionar a las partes interesadas (mercados, proveedores de servicio y cualquier otra organización asociada) para conformar un ecosistema propenso para que definan, implementen, se comuniquen periódicamente para defenderse y monitorearse en forma conjunta de las amenazas del ciberespacio.

4.12.2 Responsabilidad

La Gerencia de Seguridad Informática deberá coordinar con las diferentes partes interesadas las definiciones de seguridad que se deberá alinear en forma conjunta, monitorear e identificar incidentes que puedan afectar alguno de los que componen el ecosistema.

La Gerencia de Tecnología deberá identificar las terceras partes que participan del ecosistema, establecer la tecnología necesaria para que las terceras partes puedan alinearse con los sistemas de BYMA y a su vez exigir a las otras partes la puesta a disposición de sus tecnologías para poder interconectarse en forma segura.

5. ANEXOS

No contiene.

6. DOCUMENTACIÓN DE REFERENCIA

- ✓ Resolución General 704 de la Comisión Nacional de Valores, y sus modificatorias – Ciberseguridad y Resiliencia
- ✓ PG-73004 - Gestión de relaciones con otras partes interesadas del ecosistema
- ✓ R-81000 – Reglamento del Comité de Tecnología y Seguridad de la Información
- ✓ N–81000 – Marco de resiliencia y ciberseguridad - BYMA

CONTROL DE CAMBIOS

FECHA	CAMBIO-MOTIVO
Septiembre 2019	*Este documento fue aprobado en la reunión de directorio del 17 de enero de 2018.* *La presente versión del documento fue generada con el fin de incluir la traducción al idioma inglés.* *Se generó una nueva versión para incorporar a los anexos el documento apto para su publicación en la WEB.*
Diciembre 2020	*El documento fue revisado y aprobado en CTSI de BYMA el 12/11 sin presentar modificaciones.*
Septiembre 2022	*Nueva versión de política en base a la nueva estructura organizacional.*

Importante: completar los siguientes datos sólo en el caso de tratarse de una copia impresa controlada. Las copias controladas sólo pueden ser generadas por un distribuidor designado en el sistema y distribuidas a los destinatarios preestablecidos.

Copia controlada N° _____

Distribuidor: _____
Destinatario: _____
Ubicación de la copia: _____
Fecha de impresión: _____

_____
Firma del distribuidor