BYMA
Bolsas y Mercados Argentinos

GUÍA PARA LA GESTIÓN DE **CIBERINCIDENTES**

Guía para la Gestión de Ciberincidentes

En nuestra búsqueda de fortalecer las medidas de ciberseguridad en infraestructuras críticas del mercado de capitales, nos complace informarles sobre nuestro nuevo canal de comunicación dedicado a la rápida notificación y gestión de potenciales ciberincidentes. La seguridad de la información es una prioridad fundamental para BYMA, y esta guía tiene como objetivo brindarles pautas claras sobre cómo proceder en caso de enfrentar un incidente de este tipo.

Es esencial que se comuniquen con nosotros ante cualquier sospecha de haber sufrido un ciberincidente en conformidad con la **Resolución General 704-E/2017**, la cual establece que las partes involucradas deben colaborar solidariamente al proporcionar información que pueda servir para tareas forenses posteriores.

Recuerden que la seguridad de la información es un esfuerzo continuo y colaborativo. Siempre estaremos disponibles para brindar apoyo y orientación. Su compromiso y diligencia son fundamentales para proteger nuestros activos de información y la reputación de los mercados de capitales.

Canal de reporte de ciberincidente:

- Número de Teléfono de Emergencia: 4316-6000

- Correo Electrónico de Contacto: atencion@byma.com.ar / ciberseguridad@byma.com.ar

Pasos a seguir en caso de sufrir un ciberincidente:

1. **Comunicación Inmediata**: Lo primero y más importante es que te comuniques con nosotros tan pronto como sospeches que pudiste haber sufrido un incidente. En el reporte del incidente, indicar lo siguiente:

- **Tipo de incidente** a informar como, por ejemplo, sitio web comprometido, compromiso de un activo de información, compromiso de una red informática, phishing, spam, ransomware, malware, entre otros.

- La **severidad** percibida del incidente.

- Una **descripción clara y detallada** con los aspectos materiales de la naturaleza, alcance y momento del incidente para que nos ayude en su gestión.

2. **Acciones Iniciales:**

- Aislar el equipo afectado de la red para evitar una mayor propagación.

- Realizar un escaneo de seguridad en el resto de los equipos utilizando una solución antimalware reconocida.

- No pagar rescates ni acceder a las peticiones de los atacantes.

3. **Respaldo y Restablecimiento:**

- Mantener las copias de seguridad actualizadas y realizar su restauración en caso de ser necesario.

- Cambiar todas las contraseñas de los sistemas y correos electrónicos afectados por contraseñas robustas.

- Habilitar la autenticación de dos factores (2FA) en todas las plataformas donde sea posible.

Te adjuntamos el “Formulario de Reporte de Incidentes de Ciberseguridad” ¡Muchas gracias por la colaboración!