DECLARACIÓN DE AUTORIDAD Y COMPROMISO DE CONFIDENCIALIDAD DEL VICEMINISTERIO DE ACUACULTURA Y PESCA, DENTRO DEL MINISTERIO DE PRODUCCIÓN, COMERCIO EXTERIOR, INVERSIONES Y PESCA DE LA REPÚBLICA DEL ECUADOR DE NO DIVULGAR PUBLICAMENTE LA INFORMACION NO PÚBLICA COMPARTIDA POR LA ADMINISTRACIÓN DE ALIMENTOS Y MEDICAMENTOS DE LOS ESTADOS UNIDOS DE AMERICA

La Administración de Alimentos y Medicamentos (FDA) de los Estados Unidos de América está autorizada, por el Artículo 20.89 del Capítulo 21 del Código Federal de Regulaciones, a divulgar información no pública al Viceministerio de Acuacultura y Pesca (VAP), dentro del Ministerio de Producción, Comercio Exterior, Inversiones y Pesca de la República de Ecuador con respecto a productos regulados por la FDA que se originan de empresas dentro de la República del Ecuador, como parte de las actividades de cooperación para la aplicación de la ley o actividades cooperativas reglamentarias.

El VAP comprende que parte de la información que reciba por parte de la FDA podrá contener información no pública exenta de divulgación al público de conformidad con las normas y leyes de los Estados Unidos de América, tratándose de información comercial confidencial; información de secretos comerciales; información personal privada; información sobre la aplicación de la ley; información designada como de seguridad nacional; o información interna de carácter pre-resolutoria. El VAP comprende que la FDA comparte la información con carácter no público en forma confidencial y que es fundamental para la FDA que el VAP mantenga la confidencialidad de la información. La divulgación pública de esta información por parte del VAP podría comprometer seriamente toda interacción científica y regulatoria futura entre la FDA y el VAP. La FDA informará al VAP la condición no pública que reviste la información en el momento de suministrarla.

Por lo expuesto, VAP certifica:

1. que posee autoridad para proteger de la divulgación al público, la información no pública que la FDA suministre al VAP;

2. que no divulgará al público la información no pública suministrada por la FDA sin la autorización escrita del titular de la información, la autorización escrita de la persona que sea sujeto de la información personal privada o una declaración escrita de la FDA en la que comunique que la información ya no reviste carácter de no pública;

3. que informará sin demora, a la FDA sobre todo esfuerzo que se realice a través de un mandato judicial o legislativo para que el VAP suministre la información no pública que haya sido proporcionada por la FDA. Si este mandato judicial o legislativo ordena la divulgación de la información no pública proporcionada por la FDA, el VAP adoptará todas las medidas legales correspondientes, tendientes a garantizar que la información sea revelada de manera tal que se proteja la información de su divulgación publica, e

4. que informará, sin demora, a la FDA sobre toda modificación de las leyes de la República de Ecuador, o de cualquier política o procedimiento pertinente, que podría afectar la autoridad del VAP de cumplir con los compromisos asumidos en este documento.

5. que ha establecido y mantendrá el cumplimiento de estándares consistentes con los Marcos de Gestión de Riesgos y Ciberseguridad [1]del Instituto Nacional de Estándares y Tecnología (NIST) del gobierno federal de los Estados Unidos y/o las pautas de seguridad de la Tecnología de la Información de la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional (ISO/IEC) [2]y estándares que se enfocan en proteger los sistemas de información y la información confidencial compartida;

6. que salvaguardará los sistemas de información que contengan información no pública proporcionada por la FDA de acuerdo con las pautas y estándares actuales del NIST y/o ISO/IEC para garantizar la confidencialidad y la integridad. Confidencialidad significa evitar el acceso no autorizado y la divulgación de información no pública, e integridad significa protegerse contra la modificación o destrucción indebida de la información. La integridad incluye garantizar el no repudio y la autenticidad de la información con base en los términos de seguridad que se encuentran en esta Declaración de autoridad y compromiso de confidencialidad, incluidos los medios para proteger la información no pública;

7. que destruirá la información no pública proporcionada por la FDA, ya sea en formato electrónico o en copia impresa, una vez que la información haya sido utilizada y ya no sea necesaria para fines oficiales;

8. que restringirá el acceso a la información no pública proporcionada por la FDA a los empleados y funcionarios del VAP que requieran acceso a dicha información no pública para desempeñar sus funciones oficiales de acuerdo con los usos autorizados de la información no pública, a menos que se autorice lo contrario por escrito por FDA. El VAP informará a todos los empleados y funcionarios (1) de la naturaleza no pública de la información; y (2) la obligación de mantener dicha información no pública; y

[1] Los Marcos de Gestión de Riesgos y Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) brindan un proceso que integra las actividades de gestión de riesgos de seguridad, privacidad y cadena de suministro cibernético en el ciclo de vida de desarrollo del sistema y proporciona orientación basada en estándares, pautas y prácticas para las organizaciones para gestionar y reducir el riesgo de ciberseguridad, respectivamente. Estos marcos están destinados principalmente a administrar y mitigar el riesgo de seguridad cibernética para organizaciones de infraestructura crítica en función de estándares, pautas y prácticas.

[2] La Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (ISO/IEC) es un estándar internacional que ayuda a las organizaciones a gestionar la seguridad de sus activos de información. Proporciona un marco de gestión para implementar un sistema de gestión de seguridad de la información para garantizar la confidencialidad de todos los datos corporativos. Se recomienda enfáticamente a las contrapartes extranjeras que cumplan con los requisitos de la norma ISO 27001, o la norma más reciente, y que obtengan la certificación de un organismo de certificación acreditado.

9. que en caso de sospecha o confirmación de un incidente o incumplimiento[3], incluido un incidente de ciberseguridad[4], o cualquier otro tipo de incumplimiento, ya sea intencional o involuntario:

   (a) Protegerá toda la información no pública proporcionada por la FDA, incluida cualquier información no pública creada, almacenada o transmitida para evitar un incidente de información secundaria;

   (b) Informará a la FDA todos los incidentes o incumplimientos presuntos y confirmados que involucren información no pública proporcionada por en cualquier medio o forma, incluidos papel, oral o electrónico, a la FDA tan pronto como sea posible y sin demora injustificada, a más tardar un (1) día después del descubrimiento o detección; y

   (c) Proporcionará a la FDA evaluaciones de impacto y gravedad de incidentes o incumplimiento, cuando ocurran, incluida una descripción de las acciones tomadas, incluidas las medidas de seguridad preventivas empleadas para abordar y remediar el incidente.

Firma de la Agencia Oficial

_____/s/_____ 8/18/22
Andrés Arens Hidalgo Fecha
Viceministro de Acuacultura y Pesca
Viceministerio de Acuacultura y Pesca
Ministerio de Producción, Comercio Exterior, Inversiones y Pesca

Dirección: Malecón Simón Bolivar 100 y Av. 9 de Octubre

Teléfono: 04-2591370

[3] Un incidente se define como "un suceso que (1) pone en peligro real o inminentemente, sin autoridad legal, la confidencialidad de la información o un sistema de información; o (2) constituye una violación o amenaza inminente de violación de la ley, las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable". Los incidentes pueden ser eventos que involucren amenazas de ciberseguridad y privacidad, como virus, actividad de usuarios maliciosos, pérdida de confidencialidad o integridad, divulgación no autorizada o destrucción de información. Para los fines de este acuerdo, el incumplimiento se define como un compromiso real de la seguridad que resulta en la divulgación no autorizada, pérdida, destrucción accidental o ilegal, alteración o acceso a datos protegidos transmitidos, almacenados o procesados de otra manera. Los incumplimientos pueden ser intencionales o inadvertidas.

[4] La ciberseguridad es la prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio.