NACIONAL

RESOLUCION 316/2009
SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA (SENASA)

Apruébase la Política de Seguridad de la Información del SENASA.
Del 08/04/2009; Boletín Oficial 17/04/2009.

Visto el Expediente Nº S01:0472845/2008 del entonces MINISTERIO DE ECONOMIA Y PRODUCCION, la Decisión Administrativa Nº 669 del 20 de diciembre de 2004 de la JEFATURA DE GABINETE DE MINISTROS, la Resoluciones Nros. 45 del 24 de junio de 2005 de la SUBSECRETARIA DE LA GESTION PUBLICA 48 del 5 de mayo de 2005 de la SINDICATURA GENERAL DE LA NACION, 228 del 2 de mayo de 2006 y 570 del 29 de agosto de 2006 ambas del SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA, la Disposición Nº 6 del 3 de agosto de 2005 del DIRECCCION NACIONAL DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION, el Acta Nº 1 de fecha 6 de abril de 2009, y
CONSIDERANDO:
Que el Artículo 1º de la Decisión Administrativa Nº 669 del 20 de diciembre de 2004 de la JEFATURA DE GABINETE DE MINISTROS establece que “los organismos del Sector Público Nacional, comprendidos en el Artículo 7º deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo, dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo”.
Que el Artículo 7º de la citada Decisión Administrativa Nº 669/2004 establece que la misma ‘será de aplicación a los organismos comprendidos en los incisos a) y c) del Artículo 8º de la Ley Nº 24.156 y sus modificatorias”.
Que por la Disposición Nº 6 del 3 de agosto de 2005 del DIRECCION NACIONAL DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION se aprueba la “Política de Seguridad de la Información Modelo”.
Que por la resolución Nº 228 del 2 de mayo de 2006 del SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA se conformó el Comité de Seguridad de la Información y se designaron sus coordinadores, asignándose las funciones relativas a la seguridad de los sistemas de información.
Que el Comité de Seguridad de la Información elevó su propuesta de política de seguridad de la información, según consta a fojas 64/69 de las presentes actuaciones, mediante Acta Nº 1 de fecha 6 de abril de 2009.
Que el SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA, organismo descentralizado en la órbita de la SECRETARIA DE AGRICULTURA, GANADERIA, PESCA Y ALIMENTOS del MINISTERIO DE PRODUCCION, integra el Sector Público Nacional y debe, en consecuencia, dictar la Política de Seguridad de la Información de acuerdo a las pautas establecidas en las citadas Decisión Administrativa Nº 669/2004 y Disposición Nº 06/2005.
Que la presente se dicta en uso de las funciones y facultades conferidas por la Ley Nº 24.065 y su Decreto reglamentario, y los Contratos de Concesión a este Organismo.
Que se ha emitido el correspondiente Dictamen conforme lo requerido por el artículo 7 inciso d) de la Ley Nº 19.549.

Que el suscripto está facultado para dictar el presente acto en uso de las facultades conferidas por el Artículo 8º, inciso h) del Decreto Nº 1.585 del 19 de diciembre de 1996, sustituido por su similar Nº 237 del 26 de marzo de 2009.
Por ello,
El Presidente del Servicio Nacional de Sanidad y Calidad Agroalimentaria resuelve:

Artículo 1º.- Aprobar la Política de Seguridad de la Información del SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA, organismo descentralizado en la órbita de la SECRETARIA DE AGRICULTURA, GANADERIA, PESCA Y ALIMENTOS del MINISTERIO DE PRODUCCION, que se detalla en el Anexo que forma parte integrante de la presente resolución.
Art. 2º.- Establecer que la Política de Seguridad de la Información aprobada por el artículo anterior será de aplicación para los agentes de este Servicio Nacional y las personas físicas y jurídicas, privadas o públicas que presten servicios al SENASA.
Art. 3º.- Hacer saber a los sujetos mencionados en el artículo anterior que para todo aquello no previsto por la presente será de aplicación lo establecido por la Disposición Nº 06/2005 de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION.
Art. 4º.- Regístrese, comuníquese, publíquese, dése a la Dirección Nacional de Registro Oficial y archívese.
Jorge N. Amaya.

ANEXO
SEGURIDAD DE LA INFORMACION POLITICA GENERAL DEL SENASA
I. INTRODUCCION
La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.
Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.
II. OBJETIVO
El objetivo de la presente Política de Seguridad de la Información es el de crear un conjunto de reglas básicas que rijan el comportamiento del personal del Organismo en el uso de la información para el desarrollo de sus tareas.
Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
III. RESPONSABLES DEL CUMPLIMIENTO
Todo el personal del Organismo y los terceros, que interacman de manera habitual u ocasional, que accedan a información sensible y/o a los recursos informáticos en el desarrollo de sus tareas habituales.
IV. INCUMPLIMIENTOS
Las medidas disciplinarias forman parte del conjunto de medidas disciplinarias del Organismo.
Todas las definiciones de la presente Política de Seguridad de la Información están alineadas con los estándares nacionales e internacionales vigentes para la práctica de seguridad de la información.
V. ESTANDARES Y MARCO LEGAL
Alineación con Normas Nacionales e Internacionales.
Todas las definiciones de la presente Política de Seguridad de la Información están alineadas con los estándares nacionales e internacionales vigentes para la práctica de seguridad de la información.
VI. TERMINOS Y DEFINICIONES
A los efectos de la presente Política se aplican las siguientes definiciones:
• Información: se refiere a toda comunicación o representación de conocimiento inherente a las misiones y funciones del SENASA, en cualquier forma, con inclusión de formas

textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
• Seguridad de la información: se entiende como la preservación de las siguientes características:
Confidencialidad: la información será accesible solo a aquellas personas autorizadas a tener acceso a la misma.
Integridad: consiste en salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad: acceder a la información y a los recursos relacionados con la misma.
• Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
• Tecnología de Información: se refiere al hardware y software operados por el Organismo o por un tercero que preste servicios al Organismo, sin tener en cuenta la tecnología utilizada, ya sea de computación de datos, telecomunicaciones u otro tipo.
• Propietario de la Información: se vincula con la generación y/o administración; o disposición, de la información, entendiéndose por “propietario” a cualquier área del Organismo que posea la responsabilidad respecto de su manejo y preservación, conforme a sus funciones y competencias.
• Compromiso de Confidencialidad: instrumento por el cual la persona física o jurídica declara conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad de las personas físicas o jurídicas.
VII. POLITICAS DEL ORGANISMO ASPECTOS GENERALES
• Organización de la Seguridad: orientado a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación, así como para la distribución de funciones y responsabilidades.
Fomentar la consulta y cooperación con Organismos especializados paca 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 del Organismo.
• Administración de Activos: destinado a mantener una adecuada clasificación y protección de los activos del Organismo.
Clasificar la información para señalar su sensibilidad y criticidad.
Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.
• Seguridad de los Recursos Humanos: orientado a reducir los riesgos de error humano, robo, fraude, o uso inadecuado de las instalaciones, además de definiciones de puestos de trabajo y asignación de recursos. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse (NDA-Non Disclosure Agreement-) y verificar su cumplimiento durante el desempeño del individuo como empleado.
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 Información del Organismo en el transcurso de sus tareas normales.
• Seguridad Física y Ambiental: destinado a impedir accesos no autorizados, daños e interferencia a las dependencias e información del Organismo.
Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
Controlar los factores ambientales que podrían perjudicar el conecto funcionamiento del equipamiento informático que alberga la información del Organismo.
Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.
• Administración de Comunicaciones y Operaciones: dirigido a garantizar el

funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
Establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones.
Implementación de separación de funciones cuando corresponda.
• Sistema de Control de Accesos: 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.
Registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en los sistemas.
Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
• Adquisición, Desarrollo y Mantenimiento de Sistemas de información: orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
Definir y documentar las normas y procedimientos que se aplicaran durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
Definir los métodos de protección de la información crítica o sensible.
• Administración de Incidentes de Seguridad de la información: minimizar el daño producido por incidentes y anomalías en materia de seguridad, monitorear dichos incidentes y aprender de los mismos.
• Administración de la Continuidad de las Actividades del Organismo: orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.
Asegurar la coordinación con el personal del Organismo y los contactos extremos que participaran en las estrategias de planificación de contingencias.
Asignar funciones para cada actividad definida.
• Cumplimiento: destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.
Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

LEGISALUD ARGENTINA

Copyright © BIREME ✉ Contáctenos