COMISION NACIONAL DE INVESTIGACION Y DESARROLLO AEROESPACIAL

DIRECTIVA Nº 021 – 2011-CONIDA/OGA

DISPOSICIONES PARA LA SEGURIDAD DE LA INFORMACION

I. OBJETIVOS

1.1OBJETIVO GENERAL

Preservar la Confidencialidad, Integridad y Seguridad de la información Institucional en todos sus medios de soporte y tratamiento.

1.2 OBJETIVOS ESPECIFICOS

1.2.1 Establecer que los activos de información y los activos de tratamiento de información son criticos y deben ser protegidos de todo tipo de amenazas, sean internas o externas, deliberadas o accidentales.

1.2.2 Realizar un adecuado control de accesos a los recursos informáticos tanto interno como externo.

1.2.3 Establecer disposiciones que aseguren un nivel aceptable de operatividad y disponibilidad de los servicios y procesos críticos, ante fallas de los sistemas de información que sostienen las actividades que desarrolla la CONIDA.

1.2.4 Administrar adecuadamente las incidencias y debilidades de seguridad de información presentadas en los sistemas de información, minimizando sus ocurrencias e impacto en las actividades que desarrolla la CONIDA.

II. FINALIDAD

Contribuir a fortalecer en el personal de la Comisión Nacional de Investigación y Desarrollo Aeroespacial- CONIDA, la cultura de seguridad de la información que se genera, promoviendo su adecuado tratamiento y protección. Proteger los activos de la información de la CONIDA, asegurando la Privacidad, Confidencialidad, Disponibilidad y la Integridad de la información dentro de los sistemas de información, redes, instalaciones de cómputo y procedimientos manuales, minimizando los riesgos y asegurando la continuidad del servicio. Resguardar la privacidad e integridad de la información que fluye y se almacena en los diferentes medios de Tecnologia de Información con los que cuenta la CONIDA, minimizando los riesgos informáticos y asegurando la continuidad de los diferentes procesos de la entidad.

III. ALCANCE

Las normas que se establecen en la presente Directiva son la base para el desarrollo de procedimientos para la definición de estándares de seguridad, que sirven para establecer un ambiente de control efectivo que vele por la seguridad de información y los activos de información de la CONIDA, a nivel de software (sistemas operativos, base de datos, aplicaciones, herramientas), hardware (servidores, PCs, hub, switch, módem, router) y ambientes de conectividad (redes locales, accesos remotos, Internet).

La presente Directiva es de aplicación y estricto cumplimiento para el todo el personal de la CONIDA bajo cualquier modalidad de contrato, así como las personas o empresas que brindan servicios en la CONIDA, contratistas, terceros y todas aquellas personas que directamente tengan acceso a las áreas que intervienen en el proceso de controlar la seguridad de información en todo su ciclo de vida en la CONIDA.

VI. DISPOSICIONES GENERALES

6.1 El requerimiento de Bienes y Servicios, ó los documentos procedentes por la autoridad competente como memorando, solicitud, contrato, autorizados por el Jefe Institucional; son los documentos que inician la acción de compra de un Bien ó prestación de un Servicio.

6.2 El formato de requerimiento de Bienes y Servicios es aprobado por el Jefe Institucional y debe ser llenado en forma correcta, siguiendo las indicaciones que para tal efecto dicte la Oficina de Administración General.

6.3 Todo requerimiento de Bienes y Servicios deberá detallar las características técnicas mínimas si los tuviera.

6.4 La solicitud de adquisición de Bienes y Servicios, memorando ó contrato debe incluir la justificación del mismo que podrá incluirse dentro del requerimiento ó en su defecto en un documento adjunto al requerimiento; si éste fuera el caso, deberá estar suscrita por la persona que solicita y aprobado por el funcionario autorizado.

6.5 Cuando se trate de equipos sofisticados y características especiales; así como de Bienes a adquirirse en el exterior, el órgano solicitante deberá adjuntar una cotización.

6.6 Los requerimientos de bienes y contratación de servicios, considerados en el PAC Institucional, deben tramitarse por el área usuaria, respetando las fechas consignadas en el instrumento.

6.7 El responsable de la Oficina de Logística es el encargado de realizar el estudio de mercado y desarrollar el resumen ejecutivo.

6.8 El responsable del área usuaria que realiza el requerimiento, donde se ejecute estudio de mercado, su participación es obligatoria, dejando constancia de ello, con documento pertinente.

6.9 Es responsabilidad de la Oficina de Logística, tener al día el libro de actas donde figuren todas las reuniones y acuerdos de los procesos ADS y AMC.

6.10 La orden de compra y/o servicio que genere un proceso de AMC, donde no se suscribe contrato, debe contener una nota que indique que la presente reemplaza al contrato y que obliga al proveedor a cumplir con los requerimientos técnicos mínimos, caso contrario se eleva al OSCE, la queja correspondiente.

6.11 El responsable del área de tesorería, después de cancelado la adquisición de un bien o servicio, contratado bajo proceso de adjudicación, dentro de los 03 días posteriores, debe hacer llegar a la Oficina de Logística, copia del documento que acredite el pago que debe ser anexado al expediente de contratación.

6.12 El responsable del área usuaria, después de 10 días de recepcionado el bien o servicio, bajo responsabilidad, deberá informar a la Oficina de Logística, del cumplimiento de las condiciones contractuales y funcionamiento optimo del bien o servicio contratado.

6.13 El procedimiento administrativo para la adquisición de un bien o servicio es la siguiente:

- El área usuaria, elabora el requerimiento y con la aprobación de los funcionarios involucrados, lo presenta al Jefe Institucional, para la autorización correspondiente.
- La secretaria de la Jefatura Institucional, aplica numeración al requerimiento aprobado y lo deriva a la Oficina de Administración General.
- Con el visto bueno de la OGA, el requerimiento es entregado a la Oficina de Logística para su procesamiento.

- Existe sospecha razonable de actividad dolosa o trasgresión a las políticas de la CONIDA.
- Cuando es requerido por Ley

6.2 CONFIDENCIALIDAD

Sólo el personal y las personas autorizadas podrán tener acceso a la información clasificada de acuerdo a su confidencia, disponibilidad y/o integridad, teniendo en cuenta los criterios que sobre el particular se establecen en las normas internas.

Toda información interna que no es pública, es por defecto confidencial, salvo que expresamente presente otra clasificación.

6.3 INTEGRIDAD

Toda información que la CONIDA, genera, procesa, resguarda y distribuye, deberá contar con adecuados mecanismos de protección de la información para que no sea alterada voluntaria o involuntariamente de forma no autorizada.

La información deberá ser consistente, fiable y no propensa a alteraciones no deseadas.

6.4 DISPONIBILIDAD

La información necesaria para que realicen las funciones cada unidad orgánica de la CONIDA, deberá estar disponible donde y cuando sea requerida por los usuarios autorizados de la información y deberá ser confiable y encontrarse en la adecuada presentación.

6.5 CUMPLIMIENTO OBLIGATORIO

El cumplimiento de las políticas y estándares de seguridad de la información son obligatorias para todo el personal y será considerado como una condición en los contratos del personal.

La CONIDA se exonera de cualquier responsabilidad por el contenido de cualquier mensaje que se trasmita a través de sus sistemas de información sin la debida autorización.

CONIDA V°B° Oficina de Asesoría Jurídica

6.6 DERECHO DE PROPIEDAD INTELECTUAL

La CONIDA tiene la propiedad exclusiva sobre la patente, derecho de autor y otros derechos de propiedad intelectual de todo aquello que sus empleados y servidores contratados desarrollen para la CONIDA. Esta clausula deberá incluirse expresamente en los contratos.

CONIDA V°B° Oficina de Administración

Todo sistema o conjunto de programas almacenados en los activos de información de la CONIDA, deben ser propiedad de la CONIDA o utilizados bajo licencia o autorización de terceros, según sea el caso.

La CONIDA solo instalará en sus sistemas de cómputo, información y/o software a través de la Oficina de Telemática y Estadística.

La transferencia de información o entrega de software de la CONIDA a Entidades Externas, solo procederá con a través de la Oficina de Telemática y Estadística y esta deberá ser autorizada por la Secretaria General mediante documento oficial.

6.7 LA CLASIFICACION DE LA INFORMACION

La información de la CONIDA deberá ser clasificada por un Comité encargado, siendo uno de sus integrantes el propietario de la información y otros designado por la Oficina de Administración General de acuerdo al nivel de sensibilidad, escogiendo una etiqueta de clasificación apropiada.

solicitante, autorizado por el Director de Línea y visado por el Director Técnico.

6.19.3 El requerimiento para la adquisición de Bienes o prestación de Servicios en el exterior deberá incluir cuando menos una cotización, ésta deberá contener, las especificaciones técnicas, el precio unitario y total, la forma y modalidad de pago, el plazo de entrega y garantía. Se podrá atorgar la buena pro con una cotización en casos de proveedor único ó representante de casa matriz.

6.19.4 El responsable de la Oficina de Logística es el encargado de armar el expediente de contratación, instrumento que debe contener: requerimiento completo, documento que acredite disponibilidad presupuestaria para la adquisición y resumen ejecutivo.

6.19.5 La Oficina de Logística es la encargada de ejecutar los procesos de Menor Cuantía, sin embargo la Jefatura Institucional puede constituir cuando lo estime conveniente un Comité Especial, Ad Hoc, ó Permanente para desarrollar dichos procesos.

6.19.6 El Comité Especial debe estar conformado por tres (03) servidores; titulares y suplentes, en ambos casos uno de ellos deberá pertenecer al área usuaria de los Bienes ó Servicios ú obras, materia de la convocatoria, y el otro del órgano encargado de las contrataciones de la Entidad, necesariamente alguno de los miembros deberá tener conocimiento técnico en el objeto de la contratación.

6.19.7 La Oficina de Logística ó el Comité Especial deberá proceder cuando el expediente se encuentre completo, esto es contenga lo establecido en los numerales 6.19.1, 6.19.2, 6.19.3 de la presente Directiva y adicionalmente el informe de la Oficina de Planificación sobre la existencia de recursos para tal fin.

Si hubiera más de un postor extranjero que cumple con los requisitos exigidos, elaborará un cuadro comparativo para determinar al ganador de la buena pro.

6.19.8 El desaduanaje de los Bienes importados se realizará a través de la Oficina de Logística.

6.19.9 De acuerdo al Artículo 255 del Reglamento de la Ley de Contrataciones del Estado, los proveedores extranjeros de Bienes ó Servicios deberán sujetarse al TUPA del OSCE.

6.19.10 Queda prohibido efectuar la compra de un Bien ó Servicio con cargo a regularizar posteriormente, bajo responsabilidad del encargado de la Oficina de Logística y de quienes autoricen dichas operaciones.

VII. DISPOSICIONES ESPECÍFICAS

7.1 Los Órganos de la Entidad elaborarán su solicitud de Bienes y/o Servicios en función a su Plan Operativo y con la debida anticipación a la necesidad de uso. La solicitud que puede ser a través del requerimiento, memorando, informe, ó cualquier otro documento emanado de autoridad competente deberá ser remitida a la Jefatura Institucional, para su aprobación y dar inicio el proceso de adquisición y/o contratación.

7.2 **Oficina de Planificación y Racionalización**

7.2.1 Es el área encargada del control y afectación presupuestal

por el propietario de la información, así como supervisado por un usuario autorizado interno de la CONIDA.

7.7 DE LA GENERACION Y ACCESOS A REGISTROS (LOGS)

Todos los sistemas informáticos que manejen información clasificada como confidencial, restringida y/o critica de producción de la CONIDA, deberán incluir en su funcionamiento registros (logs) que guarden todo tipo interacción con el sistema así como también, identifiquen a los usuarios, cambios, consultas, horas de inicio y cierre de sesión y acciones realizadas , etc... Estos registros solo serán accesados para fines de control interno.

7.8 DEL ACCESO A LA INFORMACION POR PARTE DE TERCEROS

La CONIDA establece para terceros las restricciones máximas de acceso a la información. El acceso a la información deberá de limitarse a lo mínimo indispensable para cumplir con el trabajo asignado. Las excepciones deben de ser analizadas y aprobadas por la OFTES, que incluye tanto el acceso físico como lógico a los recursos de información de la CONIDA.

Todo acceso por parte de personal externo deberá de ser autorizado por Director o el Jefe del área, quien asume la responsabilidad por las acciones que pueda realizar el mismo. El personal externo deberá de firmar un "ACUERDO DE CONFIDENCIALIDAD", antes de obtener acceso a información de la CONIDA. Los proveedores tendrán acceso a los sistemas de información de la CONIDA únicamente cuando sea necesario.

7.9 DE LOS CONTRATOS

Todos los contratos a terceros deberán de incluir lo siguiente:

- Cumplimiento de las Disposiciones de Seguridad de Información
- Un acuerdo de confidencialidad
- El derecho de la CONIDA a auditar los controles de seguridad de información
- Determinación de los requerimientos legales de la CONIDA
- Metodología del proveedor para mantener y probar cíclicamente la seguridad del sistema.
- Que el servicio de procesamiento de la información de la CONIDA, objeto de la subcontratación, estén aislados, en todo momento y bajo cualquier circunstancia.

CONIDA V°B° Oficina de Asesoría Jurídica

CONIDA V°B° Oficina General de Administración

Los Contratos relacionados a servicios de tecnología de información, deben de ser aprobados por la OFTES y en el caso de que afecten la seguridad o las redes de la entidad deben de ser aprobados, revisados y autorizados por la OFTES.

Para los contratos de procesamiento de datos externos a la OFTES, se deberá especificar los requerimientos de seguridad y acciones a tomar en caso de violación de los contratos.

Todos los contratos relacionados a servicios de tecnologías de información deben de incluir una clausula donde se establezca el derecho de la CONIDA, a nombrar a un representante autorizado para evaluar las medidas que garanticen la seguridad de información y la estructura de control interno del proveedor.

El proveedor es responsable de informar inmediatamente al responsable del contrato de cualquier brecha de seguridad que pueda comprometer la información de la CONIDA.

Cualquier empleado de la CONIDA, deberá de informar a la OFTES de violaciones a la seguridad de la información por parte de terceros.

VIII. SEGURIDAD FISICA Y AMBIENTAL

8.1 SEGURIDAD DE LOS AMBIENTES

Los ambientes donde se procese, almacene y transmita la información de la CONIDA, deberán ser implementados teniendo en cuenta las políticas, las disposiciones, los estándares y recomendaciones de seguridad física y ambiental de la CONIDA y/o profesionales especialistas en el tema (ambientes, materiales, energía, cercanía a medios inseguros, mecanismos de seguridad y respaldo, etc.)

8.2 CONTROL DE ACCESOS A LOS AMBIENTES FISICOS

Si un empleado renuncia o cesa su labor en la CONIDA, el código y/o dispositivos de control de acceso físico que le fuera otorgado, deberá desactivarse o bloquearse inmediatamente.

Todas las visitas a los ambientes donde se procese, almacene y comunique la información de la CONIDA, deben de ser identificadas y deberá de mantenerse registradas en forma escritas. Estas visitas deberán de ser supervisadas y estar en compañía de un empleado autorizado durante su permanencia en los ambientes de la CONIDA.

El personal de seguridad y/o mecanismos electrónicos serán los agentes de control de las diferentes ubicaciones consideradas sensibles en la CONIDA.

Las visitas públicas a las instalaciones principales de los sistemas de cómputo y/o sistemas de comunicación de la CONIDA, se encuentran terminantemente prohibidas. Para casos especiales, se procederá a llenar una solicitud la misma que será autorizada por la Jefatura de la OFTES y la Oficina que lo solicita.

8.3 DEL TRASLADO DE EQUIPOS DE CÓMPUTO FUERA DE LA ENTIDAD

El retiro o traslado de equipos de cómputo y/o equipos de comunicación de los ambientes de cómputo, instalaciones u oficinas de la CONIDA, solo procederá si se cuenta con la autorización de la Unidad involucrada, de la OFTES, y con conocimiento de la OGA.

IX. SEGURIDAD DEL PERSONAL

9.1 CONCIENTIZACION DEL PERSONAL

La CONIDA deberá comunicar y capacitar a todo el personal contratado bajo cualquier modalidad, respecto a las Disposiciones para la Seguridad de la Información de la Entidad, así como velar por su cumplimiento.

9.2 ETICA Y DISCIPLINA

El personal que labora en la CONIDA bajo cualquier modalidad de contrato, así como las personas o empresas (terceros) que brindan servicios, deberán firmar un Acuerdo de Cumplimiento sobre las Disposiciones para la Seguridad de Información, un Acuerdo de Confidencialidad. Además el personal de la CONIDA, deberá firmar y cumplir el Código de Ética Institucional de la Función Pública.

9.3 RESPONSABILIDADES DEL PERSONAL

Todo el personal de la CONIDA, contratado bajo cualquier modalidad, es responsable de la seguridad de la información a la que tiene acceso, según las funciones que realice.

9.4 PROCESO DE SELECCIÓN Y CONTRATOS DE PERSONAL

Dentro del proceso de selección del personal que prestará servicios a la CONIDA, bajo cualquier modalidad de contrato, se deberá establecer criterios de evaluación relacionados a la seguridad de información.

X. CONTRATOS CON TERCEROS

10.1 CONTRATOS

En los contratos que se celebren con terceros se deberán incluir la prohibición de divulgar los aspectos relacionados con las propiedades de la información y de su seguridad (Confidencialidad, Integridad y Disponibilidad) así como también la no divulgación de los acuerdos de la información y de todo activo a la que fuera autorizado a tener acceso.

Los Contratos relacionados a servicios de tecnologías de información y a procesamiento de datos externos, que afecten la seguridad o las redes de la CONIDA, deben de ser revisados por la OFTES y autorizado por la OGA.

XI. ADMINISTRACION DE ACTIVOS DE INFORMACION

11.1 INVENTARIO DE ACTIVOS DE INFORMACION

Los activos de información de la CONIDA deberán ser clasificados de acuerdo a los niveles de protección requeridos y protegidos contra acceso no autorizado. La confidencialidad e integridad de la información es asegurada, según la clasificación brindada por los propietarios y responsables de dichos activos, la disponibilidad será establecida mediante acuerdos de nivel de servicio.

11.2 CLASIFICACION Y TRATAMIENTO DE ACTIVOS DE INFORMACION

Los activos de la información de la CONIDA, deberán ser clasificados por las Direcciones Técnicas o Jefes de área propietarios de la información, de acuerdo a su nivel de confidencialidad, integridad y disponibilidad, eligiendo una etiqueta de clasificación apropiada.

11.3 DISPOSITIVO DE ALMACENAMIENTO

El uso de dispositivos para el almacenamiento de información deberá ser autorizado por los propietarios de la información y deberá ser exclusivamente para fines laborales y de conservación de la información de la CONIDA.

11.4 PROPIETARIOS Y RESPONSABLES DE LOS ACTIVOS DE INFORMACION

Por cada activo de información se deberá designar un empleado o área propietaria responsable del activo, que deberá velar por la seguridad del mismo y por el mantenimiento de los controles apropiados.

CONIDA V°B° Oficina de Asesoría Jurídica

11.5 REUSO O ELIMINACION DE EQUIPOS

Los equipos que sean dispositivos de almacenamiento que contengan información de la CONIDA, se deberá asegurar que dicha información ya ha sido sobrescrita o eliminada, luego de dicha comprobación podrá procederse a su rehúso o eliminación.

CONIDA V°B° Oficina General de Administración

XII. SEGURIDAD DE LA COMUNICACIONES

12.1 CONEXIÓN DE COMPONENTES DE RED

La conexión de todo componente de la red de la CONIDA, deberá ser realizada bajo procedimientos y estándares de seguridad que protejan a los equipos y a la información que circula por las redes internas y externas de la CONIDA.

12.2 TRASLADO DE ACTIVOS DE INFORMACION

El retiro y/o traslado de activos de información de los ambientes de procesamiento, almacenamiento y comunicación de información de la CONIDA, solo procederá con la

autorización del responsable de los activos y será utilizando los medios de transporte autorizados por la CONIDA.

12.3 SISTEMAS DE TELEFONIA

Los anexos internos, teléfonos directos, fax y directorios telefónicos de la CONIDA deberán ser utilizados sólo para las actividades de la entidad.

12.4 PROTECCION DE LA INFORMACION EN LA RED

Se deberá implementar controles de prevención, detección y eliminación de software malicioso que ingrese a la red de la CONIDA.

12.5 CONEXIÓN A INTERNET

Todos los accesos a Internet a través de las redes de la CONIDA, serán exclusivamente para fines laborales y otorgados solo al personal que por su función lo amerite, con previa autorización de su Dirección.

12.6 CORREO ELECTRONICO

Se otorgará el uso de correo electrónico al personal de la CONIDA, sólo para fines laborales; que deberá contar con mecanismo de protección contra archivos adjuntos y mensajes no autenticados.

12.7 ENCRIPTACION / DESENCRIPTACION

Toda la información confidencial clasificada de CONIDA, deberá ser protegida en su almacenamiento y transporte electrónico, con algoritmos de encriptación vigentes y aprobados para su utilización por la CONIDA, de acuerdo a la clasificación que se le asigne el Comité.

12.8 MANEJO DE CLAVES DE ENCRIPTAMIENTO

Se deberán implementar medidas de seguridad que garanticen la confidencialidad de las claves de encriptamiento usadas por la CONIDA.

12.9 UBICACIÓN Y ACONDICIONAMIENTO DE OFICINAS CON EQUIPOS DE CÓMPUTO

Las oficinas con equipos de computo de la CONIDA, deberán ser implementados teniendo en cuenta las recomendaciones de seguridad fisica de entidades especializadas y/o especialistas en el tema (ambientes, materiales, cercanía a medios inseguros, transporte, etc.)

12.10 ACUERDO CON REGULACIONES Y LEYES

Los controles de seguridad física para los ambientes donde haya equipos de cómputo deberán de cumplir con las regulaciones existentes acerca de fuego, incendios, inundaciones y seguridad. Así como con los requerimientos contractuales de los seguros contratados.

XIII. DESARROLLO, ADQUISICION Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

13.1 PROCESO DE DESARROLLO Y MANTENIMIENTO

El proceso de desarrollo y mantenimiento de sistemas de información, sus privilegios y relaciones deberá ajustarse a las políticas, procedimientos, estándares y metodologías implantadas por la CONIDA.

Las áreas usuarias en coordinación con la Dirección propietaria de la información deberán justificar y sustentar la solicitud de desarrollo o modificación de un sistema o aplicación.

El desarrollo y/o mantenimiento de sistema deberá concordar con las políticas, estándares, procedimientos y normas desarrolladas para los diversos acuerdos que existan en el desarrollo de sistemas de información de la CONIDA.

El acceso a programas y sistemas estará restringido a usuarios autorizados. La actividad resultante será revisada periódicamente por la OFTES.

Las aplicaciones que están en fase de Desarrollo deberán estar separadas de las aplicaciones que se encuentran en fase de producción.

13.2 ADQUISICION DE SISTEMAS DE INFORMACION

En el proceso de adquisición de sistemas de información se deberán especificar y cumplir los requisitos de seguridad de información, que garanticen la integridad de los sistemas existentes en la CONIDA, lo cual deberá estar especificado en los contratos con los proveedores.

Cuando se requiera implementar sistemas que procesen información importante critica, sensible y confidencial para la CONIDA, será obligatorio contar con una especificación formal escrita, formalizada a través de un acuerdo escrito entre los propietarios de la información y el personal que desarrolla el sistema (interno y/o externo), con validación y aprobación de la OFTES.

13.3 AMBIENTES DE DESARROLLO Y PRODUCCION

El ambiente de desarrollo deberá de mantenerse siempre separado del ambiente de producción, debiendo existir controles de acceso adecuados para cada uno de ellos.

Solo las personas autorizadas por la Jefatura de OFTES, podrán ingresar a los ambientes de producción y realizar cambios de dichos sistemas.

13.4 PASE DE PROGRAMAS A PRODUCCION

Todo proceso de incorporación de un sistema o conjunto de programas a producción, debe estar regulado mediante procedimientos formales que incluyan, al menos, las actividades de requerimiento, evaluación, desarrollo, implantación de medidas de seguridad, prueba, aprobación y puesta en producción, bajo un adecuado nivel de segregación de funciones.

Todo pase a producción deberá estar registrado en forma escrita y firmada por todos los involucrados, desde la Dirección que autoriza, el programador responsable y el operador que realizará o supervisará la puesta en producción.

CONIDA V°B° Oficina de Asesoría Jurídica

CONIDA V°B° Oficina General de Administración

13.5 PROCESO DE CONTROL DE CAMBIOS

Será necesario ceñirse a lo estipulado en la metodología de desarrollo de aplicaciones informáticas adoptadas por la Institución.

Se deberá de mantener el procedimiento de control de cambio, el mismo que permitirá asegurar que todos los cambios del modelo y ambientes de producción hayan sido revisados y aprobados por las Jefaturas correspondientes.

XIV. CONTINUIDAD DE SERVICIOS DE LOS SISTEMAS DE INFORMACION

14.1 PLAN DE CONTINUIDAD

La CONIDA deberá delegar la responsabilidad a cada área que genera información y de las áreas que administran los activos de información para que envíen información acerca de sus amenazas y riesgos cuando requieran a la OFTES, para que esta defina un Plan de Contingencias y Continuidad de los Servicios de los Sistemas de Información e implantarlo una vez aprobado, para garantizar la operatividad y disponibilidad de los sistemas y servicios brindados, ante cualquier falla o interrupción en los mismos.

14.2 RESPALDO DE LA INFORMACION

La OFTES es responsable de salvaguardar toda información critica o sensible contenida en los sistemas del data center de la CONIDA, debe ser respaldada en medios adecuados (magnéticos, ópticos etc.) mientras dure su vigencia.

XV. MANEJO DE INCIDENCIAS DE SEGURIDAD DE INFORMACION

15.1 RESPUESTA ANTE INCIDENCIAS

Se deberá contar con planes de respuestas ante incidencias y debilidades de seguridad que afecten la operatividad de los sistemas informáticos de la CONIDA y que permita restaurar los servicios afectados en el menor tiempo posible.

15.2 ADMINISTRACION DE LAS INCIDENCIAS

Se debe instalar mecanismos para monitorear y cuantificar los tipos, ocurrencias e impacto de las incidencias, que permitan implementar controles para minimizar su frecuencia e impacto en los servicios que brinda la CONIDA.

XVI. SANCIONES Y RESPONSABILIDADES

16.1 Las violaciones a las disposiciones de la presente esta Directiva de Seguridad de la Información serán revisadas. En caso de ser probada la falta esta deriva en sanciones o penalidades de conformidad con la normatividad vigente.

16.2 Son directamente responsables de la aplicación y cumplimiento de la presente Directiva: los Directores Técnicos, Jefes de Oficina o quienes hagan sus veces, además del propietario de la información son pasivos a la aplicación de la sanción detallada en numeral anterior.

CONIDA V°B° Oficina de Asesoría Jurídica

16.3 La Oficina de Telemática y Estadística es responsable de la difusión y supervisión de la presente Directiva.

XVII. GLOSARIO DE TERMINOS

CONIDA V°B° Oficina General de Administración

- ACTIVO.- Es todo elemento que contribuya a la captura, procesamiento, presentación y almacenamiento de la información. Estos se dividen en:
  - Activo de Información.- Archivos y Bases de datos, documentación del sistema, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes de continuidad, información archivada.
  - Activo de software.- Software de aplicación y del sistema operativo, herramienta y programas de desarrollo.
  - Activo fisico.- Equipo de procesamiento de información, de comunicaciones, medios electrónicos (magnéticos, ópticos u otros).
- AMBIENTE DE ALMACENAMIENTO.- Área acondicionada para resguardar la información, copias de respaldo y documentación.
- AMBIENTE DE COMUNICACIÓN.- Área acondicionada donde se establece comunicación entre los equipos y los sistemas de información.
- AMBIENTE DE PROCESAMIENTO.- Área acondicionada donde se ingresa, se procesa y se distribuye la información.
- ASIGNACION Y CONTROL DE PRIVILIEGIOS.- Consiste en otorgar facultades de acceso a la información a un usuario autorizado, de acuerdo a las funciones delegadas.

- AUTENTICACION.- Proceso que permite verificar la identidad de un usuario cuando este intenta acceder a un sistema de información.
- CLASIFICACION DE INFORMACION.- Es un proceso que permite asignar un nivel de protección adecuado a los activos de información, de acuerdo a su nivel de confidencialidad, integridad y disponibilidad.
- CLAVE DE ACCESO.- Conjunto de caracteres alfanuméricos, conocidos exclusivamente por el usuario propietario y que le permite el acceso a la información de la entidad.
- CLAVE DE ENCRIPTAMIENTO.- Código que permite acceder a la información de los sistemas encriptados.
- COMPONENTE DE RED.- Es todo equipo o medio informático o de comunicación que pertenece a la red de la entidad.
- CONFIDENCIALIDAD.- Evitar el acceso a la información sensible a personas no autorizadas.
- CONTROL DE ACCESO.- Es la verificación que permite identificar si un usuario está autorizado acceder a determinados medios informáticos de la entidad.
- CUSTODIO DE LA INFORMACION.- Es el empleado o la unidad que protege y resguarda la información.
- DISPONIBILIDAD.- Asegurar que los usuarios autorizados tengan acceso a la información y a los métodos de procesamientos asociados, cuando sea necesario.
- ENCRIPTACION.- Medida de seguridad que permite codificar y decodificar la información de la CONIDA, de tal manera que no sea legible o fácil de entender por personas no autorizadas.
- GENERACION Y ACCESO A REGISTROS (LOGS).- Consiste en recopilar los datos mínimos necesarios para generar registros a fin de poder reconstruir una acción, transacción u operación para fines de auditoría.
- INTEGRIDAD.- Garantizar que información disponible no sea alterada en forma intencional o accidental.
- PERFIL DEL USUARIO.- Es el nivel de autorización a la información de la entidad, que se le asigna a un empleado de acuerdo a las funciones encomendadas.
- PLAN DE CONTINUIDAD.- Conjunto de procedimientos a seguir en caso se presente una ocurrencia inesperada, permitiendo asegurar la continuidad de los procesos en la entidad.
- PROPIETARIO DE LA INFORNACION.- Es el empleado o la Unidad dueña de la información que lo fuera asignada para el desempeño de las actividades a su cargo.
- RIESGO INFORMATICO.- Es la posibilidad de ocurrencia de alguna situación inesperada que no permita operar normalmente los medios de tecnología de información.
- SEGREGACION DE FUNCIONES.- Es la delimitación de tareas o áreas de responsabilidad que permita controlar y/o reducir el mal uso o modificación no autorizada de los sistemas de información y/o servicios.
- SEGURIDAD DE INFORMACION.- Es un conjunto de políticas procedimientos, mecanismos y estándares que permiten preservar la confidencialidad, integridad y disponibilidad de los activos de información.
- SISTEMAS DE INFORMACION.- Conjunto de elementos, relacionados con la información, que interactúan entre sí para apoyar actividades de la entidad.
- SOFTWARE MALICIOSO.- Programas no autorizados que ingresan a la red para causar daño a la institución (virus informáticos, gusanos, caballos de Troya, bombas lógicas, etc.).
- TECNOLOGIA DE INFORMACION.- Es el conjunto de elementos que brindan soporte directo o indirecto a los procesos de la CONIDA. Está compuesto por infraestructura (equipos, redes, sistemas base y aplicaciones) e información (bases de datos, procesamiento y transmisión de información).
- TERCEROS.- Se considera como terceros a las personas o entidades que brindan servicios a la CONIDA, bajo diferentes modalidades de contrato.

- USUARIO DE LA INFORMACION.- Es la unidad o la persona autorizada que usa la información.
- ENTIDADES EXTERNAS.- Son todas aquellas entidades públicas y personales naturales, asociaciones, etc...

- ANCHO DE BANDA.- En sistemas digitales, el ancho de Banda digital es la cantidad de datos que pueden ser transportados por algún medio en un determinado periodo de tiempo (generalmente segundos). Por lo tanto a mayor ancho de banda, mayor transferencia de datos por unidad de tiempo (mayor velocidad).

Abogado
Daniel Fernando Bolaños Galindo
Director de Administración General
CONIDA