ANEXO II

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE INVESTIGACIÓN Y DESARROLLO PESQUERO

ÍNDICE

Seguridad Informática de los Recursos Humanos 2
Gestión de Activos 3
Clasificación de los Activos 5
Autenticación, autorización y control de Acceso 5
Uso de herramientas criptográficas 5
Seguridad física y ambiental 6
Seguridad operativa 6
Seguridad de las comunicaciones 8
Adquisición, desarrollo y mantenimiento de sistemas de información 8
Relación con proveedores 9
Gestión de incidentes de seguridad 9
Aspectos de seguridad para la continuidad de la gestión 10
Cumplimiento 10

Seguridad Informática de los Recursos Humanos

Todo el personal que se desempeñe bajo la órbita del INIDEP, sin importar su modalidad de contratación, es responsable de mantener a resguardo la información que produce y aquella a la que tiene acceso.

Para tal fin, se establece:

1- Todo agente que utilice recursos informáticos deberá conformar el formulario de "uso aceptable de herramientas informáticas" y el formulario de "Acuerdo de confidencialidad en el uso de los activos de información del Organismo". Sin la firma de dichos formularios, no se le brindará acceso a la red y recursos del INIDEP.

2- Se elaborará un plan anual de capacitación en materia de seguridad de la información el cual estará dividido según el rol de los agentes. Para ello se establece que se realizará una capacitación destinada a funcionarios y secretarias, otra para personal científico-técnico, y otra para personal administrativo.

3- El acceso a recursos de información parte del concepto "todo está prohibido", por lo que para acceder a un recurso de información será necesario que el dueño del recurso lo autorice. Se considera que el pedido de acceso a un recurso de información debe ser autorizado por el superior jerárquico de un agente, con rango de Director, y por el dueño del recurso de información o sistema.
   Cada vez que un agente deje de prestar servicios en el ámbito del INIDEP, se realizará la baja de todos los accesos a los sistemas del organismo y vinculados al mismo.
   Anualmente se realizará una revisión de todos los permisos otorgados.

4- Cuando un agente del INIDEP cesa sus funciones dentro del organismo, el área de RRHH o el área interesada, notificará al Área de Informática y Tecnologías de la Información y Comunicación (TICs) para que proceda a la baja del usuario correspondiente.

5- Ante la ocurrencia de un incidente de seguridad, el agente es responsable de informarlo al Responsable de Seguridad de la Información por los canales establecidos. Este, será el encargado de coordinar las acciones de investigación, contención y erradicación del incidente, e informar a la Dirección Nacional de Ciberseguridad (CERT.ar) en caso que corresponda.

Gestión de Activos

Los Activos de información son los bienes relacionados a un sistema de información en cualquiera de sus etapas.

Ejemplos de activos son:

- Información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, resultados de proyectos de investigación, etc.
- Software: Software de aplicaciones, software de sistemas, herramientas de desarrollo, etc.
- Activos físicos: Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.
- Servicios: Servicios informáticos y de comunicaciones.

Clasificación de los activos

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

Confidencialidad:

0. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del Organismo o no. PÚBLICO
1. Información que puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, el Sector Público Nacional o terceros. RESERVADA - USO INTERNO
2. Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros. RESERVADA - CONFIDENCIAL
3. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del Organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

Integridad:

0. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Organismo.
1. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Organismo, el Sector Público Nacional o terceros.
2. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

3. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo, al Sector Público Nacional o a terceros.

Disponibilidad:

0. Información cuya inaccesibilidad no afecta la operatoria del Organismo.
1. Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.
2. Información cuya inaccesibilidad permanente un día podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.
3. Información cuya inaccesibilidad permanente durante cuatro horas podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).
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:** ninguno de los valores asignados superan el 1.
- **CRITICIDAD MEDIA:** alguno de los valores asignados es 2.
- **CRITICIDAD ALTA:** alguno de los valores asignados es 3.

Sólo el Propietario del activo 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.
En adelante se mencionará como “información clasificada” a aquella que se encuadre en los niveles 2 o 3 de Confidencialidad.

Todo activo físico que ingrese al patrimonio del INIDEP deberá ser inventariado por el área de Patrimonio, quien será responsable por su actualización.

Todo activo deberá ser identificado con un propietario, el área de Informática y Tecnologías de la Información y Comunicación llevará un inventario de todos los activos de información tecnológicos que no requieran ser patrimoniados por el INIDEP, por ejemplo: sistemas, base de datos, discos, etc.

Las bajas de activos informáticos por daño, obsolescencia o incompatibilidad tecnológica deberán ser autorizadas por el Área de Informática y Tecnologías de la Información y Comunicación completando el “formulario de Solicitud de Baja”.

El inventario será actualizado según los cambios que surjan, y anualmente se realizará el procedimiento de revisión de permisos.

Al momento que un agente/ funcionario cese sus funciones en el ámbito del INIDEP, deberá ejecutarse el procedimiento de recuperación de los activos de información que contenga en su poder. En caso que corresponda se llevará adelante el procedimiento de eliminación segura de información.

Autenticación, autorización y control de Acceso

El acceso a la información por medio de un sistema de restricciones y excepciones 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 las/los usuarias/os de todos los niveles, desde el registro inicial de nuevas/os usuarias/os hasta la privación final de derechos de las/los usuarias/os que ya no requieren el acceso. La cooperación de las/los usuarias/os es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizarlos 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.

Uso de herramientas criptográficas

El INIDEP establece que toda comunicación con terceros será encriptada, en el caso de sitios web/ web service/ VPN/ etc. con algoritmos robustos como AES256 o SHA256. Así mismo se tomarán medidas para evitar el uso de protocolos de encriptación débiles o que tengan vulnerabilidades conocidas.

Todos los sitios web del INIDEP tendrán que estar bajo el dominio *.inidep.edu.ar a fin de utilizar el certificado SSL correspondiente y así brindar mayor seguridad a las aplicaciones web del INIDEP.

Se implementarán medidas de encriptación de discos en PCs/ notebooks u otros dispositivos en los que se transporte información fuera del INIDEP.

Toda clave que sea almacenada en un activo de información deberá resguardarse encriptada por algoritmos robustos, quedando prohibido el almacenamiento y uso de claves en texto plano.

Seguridad física y ambiental

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Los perímetros de seguridad estarán delimitados por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación, un sistema de alarma de acceso numérico o un escritorio u oficina de recepción atendidos por personas.

Para la protección de sus instalaciones y activos de información el INIDEP establece perímetros de seguridad, dentro de los cuales se define:

- **Perímetro exterior**, zona externa al Organismo delimitada por éste a través de paredes, ventanas, portones, barreras.
- **Oficinas/laboratorios,** zonas internas de trabajo para las diferentes áreas del Organismo delimitadas por paredes, puertas, ventanas.
- **Zona embarcados**, comprende aquella zona exterior al Organismo en la que se encuentran los barcos de investigación. Se encuentra delimitada por los perímetros del barco.

Para el ingreso al Instituto se establece, como única entrada habilitada, la del hall principal con un sistema de control de acceso mediante tarjeta RFID y un sistema con reconocimiento de huella digital, y con personal dedicado al registro de cada ingresante al INIDEP. La entrada a terceros será registrada por el personal de recepción.

El interior y la zona del perímetro exterior del INIDEP es controlado mediante un sistema de CCTV en espacios comunes, respetando la normativa vigente, y teniendo un histórico de almacenamiento de 50 días como máximo de las ubicaciones definidas como clasificadas o críticas.

Todas las oficinas clasificadas como críticas (Centro de Cómputos y Oficinas de Acceso Restringido) están protegidas por sistema de alarma y/o bajo llave.

Seguridad operativa

Las operaciones del INIDEP se desarrollan en forma segura, en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos.

Para ello:

1- La operación dentro del Centro de Cómputos está bajo la responsabilidad del Área de Informática y Tecnologías de la Información y Comunicación. El Centro de Cómputos cuenta con un sistema de alarma de acceso numérico.
Para el caso que un tercero necesite ingresar al Centro de Cómputos se llevará un registro de acceso, y estará acompañado por personal del área de informática.

2- El área de Seguridad informática se encarga de revisar, monitorear y ajustar los requerimientos de capacidad desde la perspectiva de la seguridad de la información.

3- Se establecen accesos restringidos a los ambientes de producción, separando a estos de los ambientes de test o desarrollo.

4- El área de Seguridad informática realiza un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo.

5- La red informática del INIDEP cuenta con protección de ataques externos mediante el uso de políticas de firewall. Además se establece:
   - Prohibir el uso de software no autorizado por el área de Informática y Tecnologías de la Información y Comunicación.
   - Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
   - Realizar campañas de concientización para el personal ante ataques de Phishing e Ingeniería Social.
   - Para el caso de sistemas críticos, las actualizaciones son probadas en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas, como por ejemplo un cambio de versión.
   - Los sistemas son actualizados diariamente con las últimas actualizaciones de seguridad disponibles.
   - Todo software que deja de tener actualizaciones de seguridad por parte del fabricante es reemplazado por una versión que cuente con actualizaciones de seguridad.
   - Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

6- Realizar copias de resguardo del software y la información con una periodicidad y modalidad acordes con su criticidad de los datos y con los procesos que se lleven a cabo, probándolas periódicamente y estableciendo un registro de las pruebas de restauración que permitan conocer quién participó del proceso, cuándo y cómo lo hizo y dónde se encuentra la copia.

7- Llevar registro de todos los eventos de seguridad y revisarlo periódicamente con el fin de detectar posibles incidentes.

8- Mantener un control estricto sobre el software y su integridad, en entornos productivos.

9- Identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el software utilizado. En los casos que el mismo sea provisto por terceros, contar con una política de actualización para evitar que se afecte la operación.

10- Gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.

Seguridad de las comunicaciones

La información de la red del INIDEP debe ser protegida y controlada adecuadamente, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del organismo.

Se debe:

- Segregar los grupos de servicios de información, usuarios y sistemas en las redes.
- Controlar el tráfico proveniente de redes de usuarios hacia las redes de los sistemas, ya sean redes internas o públicas según el tipo de servicio.
- Proteger con el uso de algoritmos de encriptación la información que se transfiera dentro del organismo y hacia cualquier entidad externa, incluyendo aquella que se transmita a través de servicios de correo electrónico.
- Usar obligatoriamente la cuenta de correo electrónico institucional a todos los agentes y funcionarios del INIDEP para toda comunicación vinculada con sus funciones, informando los riesgos de este incumplimiento.
- Incluir mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados.
- Incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del INIDEP en todos los acuerdos que se suscriban.
- Incorporar acuerdos y cláusulas de confidencialidad y no divulgación cuando el INIDEP entienda que resulta conveniente para el tipo de información que trate.

Adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad de la información debe contemplarse como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites a través de Internet.

Para ello se debe:

- Especificar lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño), cuando el proceso de contratación sea gestionado por el INIDEP.
- Controlar los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción.
- Proteger los datos utilizados en las pruebas, evitando la utilización de bases de datos reales.
- Utilizar protocolos que garanticen la transmisión o enrutamiento adecuados que eviten la divulgación, alteración o duplicación no autorizadas de transacciones.

- Evaluar la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.
- Proteger la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.
- Controlar y supervisar el efectivo cumplimiento y las actividades realizadas por el cocontratante en aquellas contrataciones de bienes y servicios efectuadas por el INIDEP.

Relación con proveedores

La contratación, cualquiera sea la modalidad, realizada por el organismo para la provisión de un bien o servicio debe incluir en el pliego de bases y condiciones particulares cláusulas de cumplimiento efectivo por parte del cocontratante, relacionadas con la seguridad de la información, desde el inicio del procedimiento contractual y hasta la efectiva finalización del contrato.

Esto comprende:

- la consideración de aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.
- el establecimiento e inclusión en el pliego de bases y condiciones particulares de todos los requisitos de seguridad de la información pertinentes, en los acuerdos que se suscriban con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura tecnológica al INIDEP.
- la supervisión y revisión por parte de los responsables asignados al proyecto de todos los niveles de seguridad acordados.
- la inclusión de cláusulas para mantenimiento del nivel de servicio, especialmente en servicios de provisión crítica, que permitan mantener su disponibilidad.
- la inclusión en el pliego de bases y condiciones de estipulaciones tendientes al cumplimiento de todas las normas legales y contractuales que sean aplicables.

Gestión de incidentes de seguridad

El INIDEP adopta las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.

Para ello es necesario:

- identificar las debilidades en los procesos de gestión de información del organismo, de manera de adoptar las medidas que prevengan la ocurrencia de incidentes de seguridad.
- contar con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.
- adoptar una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.

- instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.
- notificar a la Dirección Nacional de Ciberseguridad de la ocurrencia de incidentes de seguridad, en un plazo no superior a CUARENTA Y OCHO (48) horas de su detección.
- recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia.
- en el caso en que el incidente de seguridad hubiere afectado activos de información y hubiere comprometido información y/o datos personales de terceros, se deberá informar públicamente tal ocurrencia.

Aspectos de seguridad para la continuidad de la gestión

Los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales deben contemplar todos los aspectos de seguridad de la información involucrada.

Para ello se debe:

- identificar los requisitos necesarios para cumplir todos los requerimientos de seguridad de la información ante un evento inesperado que impida seguir operando, con foco en los servicios esenciales que preste el organismo.
- establecer, documentar, implementar y mantener los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.
- verificar, revisar y evaluar a intervalos regulares los controles de continuidad de la seguridad de la información.
- implementar mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.

Cumplimiento

En todos los casos el INIDEP debe cumplir con las disposiciones legales, normativas y contractuales que le sean aplicables, con el fin de evitar sanciones administrativas y/o legales y que los empleados incurran en responsabilidades civiles o penales como resultado de su incumplimiento.

Esto implica:

- la identificación, documentación y actualización periódica de los requisitos legales y contractuales para cada sistema de información que utilice.
- el cumplimiento de la Ley No 25.326 de Protección de los Datos Personales y sus normas reglamentarias y complementarias.
- la revisión periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.
- la supervisión del cumplimiento de todos los requisitos de seguridad contenidos en la legislación aplicable, incluyendo las directrices del presente documento, y en las

políticas y procedimientos del organismo, por parte de los responsables de cada área del organismo, respecto a su personal y a la información que gestiona.

- considerar la adopción de las medidas correctivas que surjan de auditorías y revisiones periódicas de cumplimiento de los presentes requisitos, sean estas realizadas por personal del área, de organismos competentes o de terceros habilitados a tal fin.

Anexo III

PROCEDIMIENTOS Y FORMULARIOS

Formulario	F – SI – 1	Uso Aceptable de Herramientas Informáticas
Formulario	F – SI – 2	Acuerdo de Confidencialidad en el Uso de los Activos de Información
Procedimiento	P – SI – 1	Plan Anual de Capacitación
Procedimiento	P – SI – 2	Gestión de Perfiles y Permisos para el Acceso a los Activos de Información
Formulario	F – SI – 3	ABM de Acceso a Activos de Información
Procedimiento	P – SI – 3	Respuesta a Incidentes
Procedimiento	P – SI – 4	Clasificación de Activos de Información
Formulario	F – SI – 4	Inventario de Activos de Información - Clasificación
Procedimiento	P – SI – 5	Mantenimiento de Activos Patrimoniales – Hardware y Software
Formulario	F – SI – 5	ABM de Hardware y Software
Procedimiento	P – SI – 6	Protección de la Comunicación, el Transporte y el Almacenamiento de los Activos de Información
Procedimiento	P – SI – 7	Acceso de personal y terceros – Zonas de seguridad
Formulario	F – SI – 6	Solicitud de acceso para personal externo
Procedimiento	P – SI – 8	Copias de Resguardo de los Activos de Información
Procedimiento	P – SI – 9	Adquisición, desarrollo, testeo y mantenimiento de sistemas de información
Procedimiento	P – SI – 10	Continuidad de la operación – Gestión de Crisis

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2022-112710391-APN-INIDEP#MEC

MAR DEL PLATA, BUENOS AIRES
Viernes 21 de Octubre de 2022

Referencia: ANEXO-CONTROLES DE SEGURIDAD DE LA INFORMACION INIDEP

El documento fue importado por el sistema GEDO con un total de 13 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.10.21 13:46:52 -03:00

Enzo Mastroliberto
Supervisor Informático
Instituto Nacional de Investigación y Desarrollo Pesquero

Digitally signed by Gestion Documental Electronica
Date: 2022.10.21 13:46:52 -03:00