MINISTERIO DE SALUD DE LA NACION

Administración Nacional de Laboratorios e Institutos de Salud
“Dr. Carlos G. Malbrán”

Política de Seguridad de la Información

Argentina 2024

Índice General

Índice de Abreviaturas

ANLIS. *Administración Nacional de Laboratorios de Salud e Institutos de Salud*

APN. *Administración Pública Nacional*

GDE. *Sistema de Gestión Documental Electrónica de la Administración Pública Nacional*

ICU. *Institutos, Centros o Unidades* de *ANLIS*

PSI. *Política de Seguridad de la Información*

Términos y Definiciones

A

Activos de la información · *Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones* (SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN, 2019)

Amenaza · *Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización* (UNE-EN ISO/IEC 27000:2019, 2019).

C

Confidencialidad · *Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados* (UNE-EN ISO/IEC 27000:2019, 2019)

D

Disponibilidad · *Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada* (UNE-EN ISO/IEC 27000:2019, 2019).

E

Eficacia · *Grado en el cual se realizan las actividades planificadas y se logran los resultados planificados* (UNE-EN ISO/IEC 27000:2019, 2019).

Evaluación de riesgos · *Proceso de comparación de los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables* (UNE-EN ISO/IEC 27000:2019, 2019)

Evento · *Ocurrencia o cambio de un conjunto particular de circunstancias* (UNE-EN ISO/IEC 27000:2019, 2019).

Evento o Suceso de seguridad de la información · *Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles, o una situación desconocida hasta el momento y que puede ser relevante para la seguridad* (UNE-EN ISO/IEC 27000:2019, 2019)

G

Gestión de riesgos · *Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo* (UNE-EN ISO/IEC 27000:2019, 2019)

I

Incidente de seguridad de la información · *Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información* (UNE-EN ISO/IEC 27000:2019, 2019).

Información sensible · *Aquella información que comprende datos que, si son conocidos por terceros sin nuestro consentimiento, implicarán riesgos para nosotros, para nuestra organización o para terceros, tales como conocer datos privados nuestros, de familiares o de empleados de la organización; conocer documentos internos de la organización donde trabajamos, como contratos, versiones preliminares de pliegos de especificaciones técnicas, proyectos en etapa de elaboración, movimientos de efectivo, etc*. (INAP y Jefatura de Gabinete de Ministros Argentina)

Integridad · *Propiedad de exactitud y completitud* (UNE-EN ISO/IEC 27000:2019, 2019).

N

No repudio · *Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron* (UNE-EN ISO/IEC 27000:2019, 2019).

P

Política · Intenciones y dirección de una organización, como las expresa formalmente su alta dirección (UNE-EN ISO/IEC 27000:2019, 2019).

R

Riesgo de seguridad de la información · *Se relaciona con la posibilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a una organización* (UNE-EN ISO/IEC 27000:2019, 2019).

S

Seguridad de la Información · *Preservación de la confidencialidad, la integridad y la disponibilidad de la información* (UNE-EN ISO/IEC 27000:2019, 2019).

T

Tratamiento de riesgos · *Proceso destinado a modificar el riesgo* (UNE-EN ISO/IEC 27000:2019, 2019)

V

Vulnerabilidad · *Debilidad de un activo o de un control que pueda ser explotada por una o más amenazas* (UNE-EN ISO/IEC 27000:2019, 2019).

Sobre el Documento

Documento	Aprobado por:	Fecha de aprobación	Revisión
Política de Seguridad de la Información	Titular de la Administración Nacional de Laboratorios de Salud e Institutos de Salud “Dr. Carlos G. Malbrán” MSc. Pascual A. Fidelio ANLIS		1.0

Historial de Versiones

Aspectos que cambiaron en el documento	Responsable de la solicitud del cambio	Fecha de aprobación	Revisión
Versión inicial del documento	Titular de la ANLIS	15/06/2023	0
Se rediseñó el apartado Sobre el documento y Historial de Versiones. Se modificó la forma establecida para identificar el estado de revisión. En lugar de utilizar dígitos enteros se decidió usar enteros con un decimal (Ejemplo: 1.0; 1.1; etc.) donde la cifra decimal cambia cuando los cambios son menores. En el caso de cambios mayores se modifica en número entero por el subsiguiente. Se actualizó conforme al diseño de la Administración Pública Nacional 2024. Correcciones de redacción y ortografía siguiendo las recomendaciones de la Real Academia Española (RAE).	Titular de la ANLIS		1.0

Introducción

La información es un activo que, como otros bienes y servicios requeridos para el cumplimiento de los objetivos del organismo, resulta esencial para el desarrollo de las actividades de competencia, y a mayor calidad permite una mejor toma de decisiones. En consecuencia, necesita ser protegida adecuadamente.

Dicha información puede presentarse en diversos formatos (impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos o como contenido multimedia, entre otros). Por lo tanto y sin perjuicio del formato en que se encuentre y del soporte que se utilice, debe estar apropiadamente protegida desde su creación, durante todo su ciclo de vida y hasta su eventual destrucción, desuso o archivo definitivo.

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de un rango amplio de amenazas, con el objeto de minimizar los riesgos a los que se encuentra expuesta y asegurar la continuidad de la operación normal de la Administración Nacional de Laboratorios e Institutos de Salud “Dr. Carlos G. Malbrán” (ANLIS).

Dicho estado de protección adecuada se logra a través de la implementación y monitoreo de un conjunto de mecanismos de seguridad y/o de los controles recomendados del Anexo A de IRAM-ISO/IEC 27001:2015 aplicables a la ANLIS que incluyen entre otros, procesos, políticas, procedimientos nuevos o actualizados, estructuras organizacionales, software y hardware junto a procesos de gestión correctamente coordinados. De este modo, logra la preservación de los activos de la información, la eficacia en la operación, cumplir con el marco legal y las normas internas, y preservar la imagen institucional de la ANLIS y del Estado Nacional en su conjunto.

La seguridad de la información es importante para el desarrollo de actividades del sector público y para proteger las infraestructuras críticas de información que proveen productos y servicios esenciales a la sociedad. En este aspecto, el Estado puede proveer los servicios en forma directa o ejercer un rol regulatorio que lo obliga a velar por la seguridad de los datos y servicios tratados.

Objeto

La presente Política de Seguridad de la Información (PSI) constituye las directrices y condiciones de actuación en materia de seguridad de la información que establecen el modo en que la ANLIS debe gestionar y proteger los datos a los que da tratamiento, los recursos tecnológicos que utiliza, y los productos y servicios que brinda. Detalla también lineamientos respecto a la comunicación de esta Política al personal bajo cualquier modalidad de contratación y demás personas involucradas internas y externas, así como respecto a su implementación en todas las dependencias de la ANLIS.

El objetivo principal de esta PSI es definir el propósito, la dirección, los principios, las reglas básicas y los mecanismos de comunicación, todo ello con sus recursos asociados, para la preservación de la confidencialidad, integridad y disponibilidad de la información de la ANLIS vinculada con su Misión, Visión y Objetivos en pos de la Salud Colectiva.

El presente documento se dicta en cumplimiento a la normativa vigente, tanto externas a la ANLIS, como leyes nacionales, decretos y resoluciones que sean aplicables a los datos, los sistemas informáticos y el ambiente tecnológico que utiliza. En otras palabras, es afín a los derechos y obligaciones sin perjuicio de las normativas aplicables de la Administración Pública Nacional (APN). Además, es conforme al marco legal interno de la propia entidad, como políticas, procedimientos, disposiciones, cláusulas contractuales, acuerdos con el personal y terceros, etc.

Una adecuada gestión de la seguridad de la información permite proteger los activos de la información frente a amenazas internas o externas, deliberadas, accidentales o ambientales, y contribuye con el cumplimiento de las normas aplicables.

Alcance

Esta PSI se aplica en todo el ámbito de la ANLIS sobre los activos de la información, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Debe ser comunicada fehacientemente por los medios de comunicación oficiales y cumplida por todas las personas físicas y jurídicas, ya sean internos o externos, vinculadas a la entidad a través de contratos, convenios, acuerdos o algún otro instrumento válido para establecer la relación con terceros, en la medida en que les sea aplicable y en las secciones que le correspondan. En su alcance se encuentran tanto el personal que desempeñe funciones

directivas como administrativas o técnicas, cualquiera sea su vínculo/relación contractual, su nivel jerárquico, su situación de revista y las tareas que desempeñe.

Principios básicos

Los principios de la seguridad de la información, en base a la normativa vigente, que son adoptados por la ANLIS comprendidos en el inciso a) del artículo 8 de la Ley N° 24.156, son la confidencialidad, la integridad y la disponibilidad de la información a la que le dan tratamiento y de los activos de información utilizados para su gestión. La protección de los derechos de los titulares de los datos personales procesados, así como de la información propia de la ANLIS, es un objetivo central de esta PSI.

Los contenidos de este documento están alineados y se complementan con el resto de las políticas y normativas internas de la ANLIS, que entiende la importancia de gestionar eficazmente la seguridad de la información. En consecuencia, declara su compromiso y total apoyo a la gestión de la seguridad de la información como parte integrante de la gestión del resto de los procesos establecidos en su ámbito. Acorde a lo antedicho, la ANLIS se compromete a cumplir, dentro del marco de la seguridad de la información, con la normativa legal y reglamentaria aplicable a todos los niveles, así como a adaptarse a futuras normas y requisitos del contexto interno o externo y a aquellos que emanan de la vinculación con terceros involucrados.

Asimismo, autoridades de la ANLIS se comprometen a liderar la mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia, y asignar los recursos necesarios. El personal de la ANLIS tiene la obligación de dar tratamiento y hacer un uso responsable, seguro y cuidado de los datos que utilizan en sus labores habituales, adoptando todas las medidas a su alcance para protegerlos. Para ello, reciben una concientización periódica y pertinente a su función, y compromiso que asumen para cumplir con esta PSI. La misma está vinculada con la Coordinación Técnica de Capacitación de la ANLIS y/o externos según corresponda y sujeta a la asignación presupuestaria.

El incumplimiento de esta política tendrá como resultado la aplicación de sanciones disciplinarias, conforme a la magnitud y característica del aspecto no cumplido, de acuerdo con el marco legal aplicable a la ANLIS.

Al respecto y de acuerdo a la normativa vigente, se establece como falta el incumplimiento de los lineamientos y prácticas de esta PSI, por parte del personal, en función de lo dispuesto

por el régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1421/02 y sus normas modificatorias y complementarias. Para ello, se establece una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo con la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.

Asimismo, ante el incumplimiento de la PSI se podrá disponer de la rescisión contractual o no renovación de las personas físicas contratadas mediante el régimen dispuesto por el Decreto 1109 de 28 de diciembre de 2017 y sus complementarios y modificatorios. En este sentido se procederá con aquellas personas físicas que bajo cualquier vínculo contractual presten servicios o desarrollen tareas de cualquier índole en esta ANLIS, ya sea pasantes, becarios o bajo cualquier tipo de contratación, los que quedan obligados al cumplimiento de la PSI.

La ANLIS establece sus requisitos de seguridad de la información en el procedimiento correspondiente en base a la evaluación y posterior gestión de riesgos de seguridad sobre sus activos de la información junto a los requisitos legales aplicables y el estudio de la organización.

Revisión y actualización

La ANLIS se compromete a revisar esta PSI anualmente, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicarla y dejarla a disposición de las personas físicas y jurídicas descriptas en el Alcance.

Adicionalmente, procederá a su revisión y eventual modificación, cada vez que se produzca un cambio significativo en la plataforma tecnológica, una modificación de la normativa vigente aplicable, un cambio en los objetivos estratégicos de la ANLIS o cualquier otro evento que lo amerite.

La Dirección de Administración Contable, Mantenimiento y Servicios Generales de la ANLIS será la responsable de llevar adelante las revisiones sean periódicas o ad-hoc, dejándose constancia de ellas en el presente documento. La persona Titular de la ANLIS será responsable de la aprobación de las nuevas versiones, que serán comunicadas en tiempo y forma a los que correspondan para su cumplimiento.

Lineamientos específicos

Organización de la Seguridad de la Información

La ANLIS asigna a la Dirección de Administración Contable, Mantenimiento y Servicios Generales las responsabilidades relativas a la seguridad de la información, que tendrá a su cargo la coordinación de todas las actividades tendientes a la implementación de la presente PSI. Dicha unidad organizativa velará por una adecuada segregación de funciones, por un abordaje de la seguridad de la información en todos los proyectos y programas de la ANLIS, y por el establecimiento de adecuados procedimientos de seguridad, en base a un plan de tratamiento de riesgos.

Las autoridades de la ANLIS se comprometen a impulsar las iniciativas que el área competente proponga con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que gestiona. Asimismo, requerirá a las áreas competentes la inclusión en contratos, términos de referencia o instrumentos similares, cláusulas que contemplen el cumplimiento de la presente PSI.

Uso de dispositivos móviles personales

La ANLIS adopta medidas para proteger adecuadamente la información institucional dentro de los dispositivos (notebooks, smartphones, tablets, etc.), propiedad del personal de la ANLIS, mediante los documentos que correspondan. Contemplando que, el personal debe recibir la capacitación pertinente y aplicar esas competencias. Mientras que, los dispositivos deben cumplir con configuraciones de seguridad específicas.

Trabajo remoto

La ANLIS adopta medidas para proteger adecuadamente la información institucional mientras se desarrolle el trabajo remoto, mediante los documentos correspondientes. Contemplando que, el personal debe recibir la capacitación pertinente y aplicar esas competencias. Mientras que, los dispositivos deben cumplir con configuraciones de seguridad específicas.

Seguridad Informática de los Recursos Humanos

El personal es considerado un recurso central para la protección de la información, motivo por lo cual es adecuadamente entrenado a través de programas específicos según el tipo de actividad que realice en la ANLIS. A tal fin, se establecen las medidas necesarias en los procesos de selección de personal como una inducción obligatoria relacionada a la seguridad de la información, durante la relación laboral y al momento de la desvinculación, pudiendo inclusive excederlo. En todo momento se protegen los derechos individuales del personal, especialmente aquellos relacionados con la privacidad.

Se establece la obligatoriedad de la suscripción de compromisos de confidencialidad en función de las responsabilidades que correspondan y a las funciones que se desarrollen. Los permisos de acceso son otorgados en función de cada perfil de trabajo y se mantienen actualizados.

Gestión de Activos

La gestión y protección efectiva de los activos en función de su clasificación por criticidad es una prioridad para la ANLIS. Entre los activos se incluyen tanto el hardware, software, procesos, personas, servicios y físicos relacionados a la información, cualquiera sea el soporte y formato, de mayor valoración según el procedimiento correspondiente. Para la clasificación se tienen en cuenta la confidencialidad, integridad y disponibilidad de la información, así como criterios de bases comunes sobre aspectos económicos, servicios, operación, imagen y/o reputación y cumplimiento legal.

Se llevan inventarios actualizados y se exige a todo el personal que se desvinculan la devolución de los activos de información en su poder. En el mismo sentido, se procede a una destrucción segura de cualquier medio que pueda contener información crítica o datos personales, para lo cual, se cuenta con procedimientos adecuados.

Autenticación, autorización y control de acceso

La ANLIS adopta los mecanismos necesarios utilizando los documentos pertinentes para que solo el personal autorizado acceda a los activos de información, bajo la premisa básica de que "*todo está prohibido a menos que se permita expresamente*" para aquellos activos considerados críticos. El acceso a la información se establece en base a la "*necesidad de*

saber", es decir que quienes accedan deben tener un motivo válido para hacerlo en razón de su rol y/o funciones y usando una política de "*Mínimo Privilegio*". Estos privilegios se otorgan en forma expresa, son autorizados por los niveles competentes y se gestionan adecuadamente las altas y bajas de las cuentas y permisos de acceso, con revisiones periódicas. Se requiere del personal, el uso responsable de los dispositivos y datos de autenticación otorgados por la ANLIS para el cumplimiento de sus funciones, que no los compartan y que los mantengan siempre seguros, tanto dentro como fuera de la organización.

Uso de herramientas criptográficas

Se utilizan sistemas y técnicas criptográficas para la protección de la información de la ANLIS, con el fin de preservar su confidencialidad, integridad, autenticidad y no repudio para su almacenamiento.

Para ello, se requiere el cifrado de toda la información crítica almacenada en la ANLIS. Asimismo, se protegen las claves criptográficas durante todo su ciclo de vida y se utilizan certificados digitales válidos en los sitios web institucionales.

Seguridad física y ambiental

La ANLIS protege sus activos de información, como instalaciones físicas, incluyendo sus puestos de trabajo, en función de la criticidad de la información que éstos gestionan, mediante el establecimiento de perímetros de seguridad, áreas protegidas y controles ambientales, en la medida en que se considere necesario. También contempla, mecanismos de bloqueo de sesión y de escritorio limpio.

Por otro lado, se monitorean los accesos físicos para permitir solo ingresos y egresos debidamente autorizados y se mantiene un registro actualizado de los activos de información que procesan información. Se implementan y hacen cumplir medidas de seguridad para los activos que deben llevarse fuera de la ANLIS, manteniéndose el registro por parte del lugar de la ANLIS que corresponde el activo de información.

Seguridad operativa

Las operaciones de la ANLIS se desarrollan en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades y desarrollando

procedimientos acordes. Se adoptan medidas para minimizar los riesgos de acceso y cambios no autorizados o pérdida de información y para proteger las instalaciones y plataformas tecnológicas contra infecciones de código malicioso.

Las vulnerabilidades son gestionadas de manera apropiada y se controla la actividad de personas administradoras y operadoras.

Seguridad de las comunicaciones

La ANLIS adopta las medidas necesarias para proteger adecuadamente la información que se comunica por sus redes informáticas y para minimizar los riesgos que pudieran afectar la infraestructura de soporte.

Se asignan cuentas institucionales a todo el personal, quienes están obligados a utilizarlas para toda comunicación oficial vinculada a sus funciones. Mientras que el uso de otras plataformas de comunicación como WhatsApp, Telegram, etc. no debe circular información sensible exceptuando el alcance de la – LEY DE DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA - N° 27. 275 (B.O 29/09/2016) y sus normas modificatorias y complementarias. Dicho personal es informado por sus respectivas autoridades sobre los riesgos de incumplir este requerimiento, y se les exige la firma de acuerdos de confidencialidad y no divulgación, en los casos en los que la ANLIS lo considere necesario.

Seguridad de la información en sitios web y redes sociales Institucionales.

La ANLIS adopta medidas para proteger adecuadamente la información en sitios web y redes sociales institucionales. Algunas de ellas, es utilizar documentación de seguridad de la información en sitios web propios, externos a la institución y redes sociales aprobados por la persona Titular de la ANLIS. Este documento debe contemplar: qué comunicar, cuándo comunicar, a quién comunicar, cómo comunicar, quien comunica según las diferentes vías de comunicación. Además, indica que, la administración del contenido dentro de los sitios web y/o redes sociales es formalmente responsabilidad del Área de Prensa y Comunicación de la ANLIS o el sector de comunicación de cada Institutos, Centros y Unidades (ICU) según corresponda, que debe realizar las publicaciones acordes a dicho documento para los contenidos en medios digitales oficiales. Mientras que, en caso de páginas web de propiedad de la ANLIS, la responsabilidad de la administración del servidor de alojamiento, seguridad y

backup es del Departamento de Sistemas de Información de la ANLIS que debe realizarlo mediante los documentos pertinentes.

Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información

La ANLIS adopta las medidas de seguridad necesarias para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen internamente, utilizando una metodología de desarrollo seguro, e incorpora requerimientos y evaluaciones de seguridad en el proceso de contratación de aplicaciones a terceros. Esto se aplica especialmente a aquellas que se utilicen para brindar servicios o realizar trámites por parte de la ciudadanía e involucren el tratamiento de datos personales.

Se evalúa la seguridad de las aplicaciones antes de ponerlas productivas.

Relación con proveedores

La ANLIS incluye en los pliegos de bases y condiciones particulares cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte de los cocontratantes. Estas consideran los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio del proceso contractual hasta su finalización. Los requisitos a incluir son acordes a la criticidad de la información y los servicios (como establecer un nivel mínimo de servicio en caso que corresponda o cláusulas de mantenimiento del servicio, etc.), la evaluación de riesgos y el cumplimiento de todas las normas legales y contractuales aplicables como lo dispuesto en la LEY DE CONFIDENCIALIDAD SOBRE INFORMACION Y PRODUCTOS QUE ESTEN LEGITIMAMENTE BAJO CONTROL DE UNA PERSONA Y SE DIVULGUE INDEBIDAMENTE DE MANERA CONTRARIA A LOS USOS COMERCIALES HONESTOS - Nº 24.766 (B.O. 30/12/1996) y sus normas modificatorias y complementarias, y marco legal sancionatorio correspondiente en caso de incumplimiento.

Relación con terceros

La ANLIS adopta medidas para proteger adecuadamente la información institucional en la relación con terceros. En este sentido, la ANLIS establece un régimen a aplicar con terceros y cocontratantes que atenten contra la protección del objetivo de la seguridad de la información pretendido, sujetos los cuales -por definición- no se hallan sometidos a una

relación de “subordinación laboral” con la APN. En efecto, en las respectivas contrataciones, acuerdos o convenios con ANLIS podrán insertarse cláusulas que aludan a determinados deberes del cocontratante en relación a la preservación de la información y/o documental manejado a propósito de la prestación a su cargo, o cualquiera sea el objeto de la relación convenida. A tal fin se preverán las sanciones a aplicar para el caso de su inobservancia las que podrán ajustarse según la relación jurídico-comercial entablada.

Gestión de incidentes de seguridad

La ANLIS adopta las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información. Las debilidades en los procesos son debidamente comunicadas, identificadas y minimizadas de forma tal que se apliquen las acciones correctivas en el menor tiempo posible.

Cuando el personal detecte un incidente y/o evento de seguridad de la información, lo deben comunicar siguiendo el procedimiento correspondiente. De producirse el incidente, y que éste hubiera afectado información o datos personales de terceros, la ANLIS informará públicamente tal ocurrencia, de acuerdo con lo dispuesto por la normativa vigente y notificará a la Dirección Nacional de Ciberseguridad en un plazo no superior a 48 horas.

Aspectos de seguridad para la continuidad de la gestión

Se contemplan todos los aspectos de seguridad requeridos en los procedimientos de continuidad de la gestión de la ANLIS que se desarrollan, especialmente cuando se trate de información, servicios o sistemas críticos. Se realizan análisis de impacto y se identifican las ventanas de recuperación requeridas en los procesos críticos.

Cumplimiento

La ANLIS cumple las disposiciones legales, normativas y contractuales que le son aplicables y promueve el acatamiento de las políticas y normas de seguridad que se aprueban en su ámbito. En el mismo sentido, atiende y da cumplimiento a las recomendaciones correspondientes a los hallazgos de las auditorías internas y externas que se realicen, adoptando las medidas correctivas que correspondan para la mejora continua.

Bibliografía

INAP y Jefatura de Gabinete de Ministros Argentina. (s.f.). *Introduccion a la ciberseguridad: uso seguro de las tecnologias de la informacion.*

SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN. (18 de 9 de 2019). *Boletin Oficial de la Republica Argentina.* Obtenido de Resolución 1523/2019 Anexo II: https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

UNE-EN ISO/IEC 27000:2019. (Febrero de 2019). *Sistema de Gestion de la Seguridad de la Informacion (SGSI) Visión de conjunto y vocabulario UNE-EN ISO/IEC 27000:2016*. Madrid, España.

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2024-66347841-APN-ANLIS#MS

CIUDAD DE BUENOS AIRES
Martes 25 de Junio de 2024

Referencia: EX-2023-64152363- -APN-DACMYSG#ANLIS - Política de Seguridad de la Información ANLIS versión N° 1.0, año 2024

El documento fue importado por el sistema GEDO con un total de 25 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.06.25 13:21:47 -03:00

Maria Alejandra Aquino
Asesor Legal
Administración Nacional de Laboratorios e Institutos de Salud

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.06.25 13:21:48 -03:00