República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Disposición

Número: DI-2022-9703-APN-ANMAT#MS

CIUDAD DE BUENOS AIRES
Miércoles 30 de Noviembre de 2022

Referencia: EX-2022-95376976- APN-DGA#ANMAT

VISTO el EX-2022-95376976- APN-DGA#ANMAT, la Decisión Administrativa N° 641 del 25 de junio de 2021 y la Disposición N° 1 del 14 de febrero de 2022 de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS; y

CONSIDERANDO:

Que, a través de la Decisión Administrativa Nº 641/2021, se aprobaron los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL", que son aplicables a todas las entidades y jurisdicciones comprendidas en el inc. a) del art. 8° de la ley N° 24.156.

Que, a los fines de optimizar las herramientas de protección de los activos y recursos de información de esta Administración Nacional de Medicamentos, Alimentos y Tecnología Médica, la tecnología utilizada para su procesamiento, y dar acabado cumplimiento con la norma referida, deviene necesario y a los fines del cumplimiento de los requisitos de seguridad, se apruebe una Política de Seguridad de la Información.

Que, conforme lo establece el artículo 6° de la decisión administrativa antes mencionada, se deberán adoptar las medidas preventivas, detectivas y correctivas destinadas a proteger la información.

Que a través de la Disposición N° 1/ 2022 de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS se aprobó el "MODELO REFERENCIAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN".

Que, en cumplimiento de lo dispuesto en el Artículo 5° de la DecisiónAdministrativa N° 641/21, oportunamente, se informó a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD, mediante NO-2021-70972143-APN-ANMAT#MS, la asignación de las funciones relativas a la Seguridad de los Sistemas de Información de esta Administración.

Que, en dicho marco, la DIRECCIÓN DE INFORMÁTICA dependiente de la DIRECCIÓN GENERAL DE ADMINISTRACIÓN elaboró la "POLITICA DE SEGURIDAD DE LA INFORMACIÓN DE ESTA ADMINISTRACIÓN NACIONAL" conforme IF-2022-107945503-APN-DGA#ANMAT.

Que la DIRECCION GENERAL DE ADMINISTRACIÓN y la DIRECCIÓN DE ASUNTOS JURIDICOS han tomado la intervención de su competencia.

Que la presente medida se dicta en uso de las facultades conferidas por el Decreto Nº 1490/92 y sus modificatorios.

Por ello,

EL ADMINISTRADOR NACIONAL DE LA ADMINISTRACIÓN NACIONAL

DE MEDICAMENTOS, ALIMENTOS Y TECNOLOGÍA MÉDICA

DISPONE:

ARTÍCULO 1°.- Apruébase la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN" de la ADMINISTRACIÓN NACIONAL DE MEDICAMENTOS, ALIMENTOS Y TECNOLOGÍA MÉDICA que, como anexo IF-2022-107945503-APN-DGA#ANMAT, forma parte integrante de la presente medida.

ARTÍCULO 2°.- Ténganse por asignadas las funciones relativas a la Seguridad de los Sistemas de Información a la DIRECCIÓN DE INFORMÁTICA, de conformidad con lo informado a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, en cumplimiento de lo establecido en el artículo 5º de la Decisión Administrativa N° 641/2021.

ARTÍCULO 3°.-Notifíquese la presente al personal de la ADMINISTRACIÓN NACIONAL DE MEDICAMENTOS, ALIMENTOS Y TECNOLOGÍA MÉDICA. Comuníquese a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

ARTÍCULO 4°.-Publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL. Dése a la Dirección General de Administración y ala Dirección de Recursos Humanos a los fines de lo previsto en el artículo 3°. Archívese.

mm

Digitally signed by LIMERES Manuel Rodolfo
Date: 2022.11.30 17:04:37 ART
Location: Ciudad Autónoma de Buenos Aires

Manuel Limeres
Administrador Nacional
Administración Nacional de Medicamentos, Alimentos y Tecnología Médica

Digitally signed by Gestion Documental Electronica
Date: 2022.11.30 17:04:50 -03:00

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Informe

Número: IF-2022-107945503-APN-DGA#ANMAT

CIUDAD DE BUENOS AIRES
Martes 11 de Octubre de 2022

Referencia: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Introducción

La A.N.M.A.T., entendiendo la importancia de la gestión de la seguridad de la información, se compromete a establecer medidas de control y seguridad orientadas a protegerla. Con el objeto de propiciar la continuidad de los sistemas de información, minimizar los riesgos de las amenazas y contribuir al eficiente cumplimiento de los objetivos de la A.N.M.A.T., todo ello enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la A.N.M.A.T. Para dar cumplimiento de todo lo mencionado precedentemente es necesario un marco normativo, el cual es brindado por la presente Política de Seguridad de la Información.

Se pone de manifiesto, el compromiso de las máximas autoridades de la A.N.M.A.T. y demás autoridades de las unidades organizativas, para promover su difusión, consolidación y cumplimiento, con el fin de que la presente política llegue a formar parte de la cultura organizacional de la A.N.M.A.T.

Se declaran inicialmente las políticas generales de seguridad de la información. Posteriormente como anexos, las políticas particulares y directrices, para consolidar la gestión de la seguridad de la información dentro de la A.N.M.A.T. De esta manera se da cumplimiento a la Decisión Administrativa N° 641/2021 de la Jefatura de Gabinete de Ministros, la cual establece en la sección V. DIRECTRICES, punto 1. Política de Seguridad de la Información del organismo, “Los organismos deben desarrollar una Política de Seguridad de la Información compatible con la responsabilidad primaria y las acciones de su competencia...”.

El presente documento se redactó según la política de seguridad de la información modelo indicada en la Disposición N° 1/2022 de la Dirección Nacional de Ciberseguridad y alineada con los requisitos mínimos de

seguridad de la información para organismos según la Decisión Administrativa N° 641/2021 JGM. Como también se encuentra alineada al código de buenas prácticas de controles para la seguridad de la información de la Norma ISO/IEC 27002:2013.

Objetivos

Establecer un marco de referencia para la protección de la información y continuidad de los procesos y/o servicios, a través del resguardo de la confidencialidad, conservación de la integridad y mantenimiento de la disponibilidad de la información y de todos los recursos tecnológicos de la A.N.M.A.T., utilizados en la transmisión, procesamiento y almacenamiento, frente a posibles amenazas internas o externas, deliberadas o accidentales.

Alcance

El alcance aplica a todo el ámbito de la A.N.M.A.T., a todos sus recursos y procesos, ya sean estos internos o externos vinculados través de acuerdos con terceros.

Responsabilidad

Es responsabilidad de la máxima autoridad de la A.N.M.A.T. o en quien ésta lo delegue, aprobar la presente política de seguridad de la información, promover su difusión, impulsar su implementación y hacer uso de la misma como parte de sus herramientas de gobierno y gestión.

Es responsabilidad de los titulares de las Unidades organizativas, implementar la política de seguridad de la información dentro de sus áreas de responsabilidad y promover su cumplimiento por parte de su equipo de trabajo.

Acatamiento

La presente Política de Seguridad de la Información, expresa declaraciones de acatamiento obligatorio. Es decir, que no son recomendaciones o sugerencias, sino declaraciones que exigen su cumplimiento.

Excepciones

Todas las excepciones a la Política de Seguridad de la Información, deberán ser formalmente documentadas, registradas y revisadas.

La excepción al cumplimiento de la presente Política de Seguridad deberá ser solicitada formalmente por el responsable de la dirección interesada, evaluada y otorgada (en caso de corresponder) por la DIRECCIÓN DE INFORMÁTICA.

Marco Normativo

El marco normativo de la presente Política de Seguridad de la Información se encuentra alineado respecto a la Legislación de la República Argentina.

Leyes relacionadas a la Ciberseguridad:

• Ley 26.388 de Delitos informáticos

• Ley 25.326 de Protección de Datos Personales

• Decreto Reglamentario N° 1558/2001

• Ley 25.506 de Firma Digital

• Decreto Reglamentario N° 182/2019

• Ley 26.904 de Grooming

• Ley 11.723 Propiedad Intelectual y Ley 25.036 Modificatoria de Ley 11.723

Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad:

• Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos

• Disposición 1/2022 Dirección Nacional de Ciberseguridad JGM. Aprueba el “Modelo Referencial de Política de Seguridad de la Información”.

• Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.

• Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.

• Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.

• Resolución 1523/2019. Definición de Infraestructuras Críticas.

Otras normativas relacionadas a la Ciberseguridad:

• Decreto 577/2017. Creación del Comité de Ciberseguridad.

• Decreto 480/2019. Modificación del Decreto 577/2017.

• Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.

• Resolución 141/2019. Presidencia del Comité de Ciberseguridad.

• Disposición JGM 7/2021 Dirección Nacional de Ciberseguridad “Registro de Puntos Focales en Ciberseguridad del Sector Público Nacional”

• Disposición JGM 8 / 2021 Dirección Nacional de Ciberseguridad Guía Introductoria a La Seguridad para el Desarrollo de Aplicaciones Web.

Como también al estándar internacionalmente referido a las buenas prácticas de seguridad de la información:

• Norma ISO/IEC 27002:2013 Código de Buenas Prácticas de Controles para la Seguridad de la Información.

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Declaración de las Políticas y Normativas

Se establece la vigencia del presente documento denominado Política de Seguridad de Información, aprobado por la máxima autoridad de la A.N.M.A.T. Publicada en la webinterna de la A.N.M.A.T. para su consulta y comunicación a todo el personal, para su difusión y conocimiento, como también para terceros cuando se la requiera.

La presente Política de Seguridad de la Información, deberá ser cumplida por todo el personal prestatario de servicios en el ámbito de la A.N.M.A.T., tanto se trate de funcionarios jerárquicos, administrativos, operativos y técnicos, sea cual fuere su modalidad de contratación, nivel escalafonario y situación de revista. Como también deberá ser utilizada como base para establecer el conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en la A.N.M.A.T., en su plataforma tecnológica y demás recursos de los que disponga.

Se establecen una serie de políticas de seguridad específicas, incluidas como anexos en el presente documento, las cuales indican objetivos, responsabilidades y políticas detalladas aplicables a áreas particulares y también de cumplimiento con carácter obligatorio, se indica además documentos modelos y glosario de términos.

La Política de Seguridad de la Información, será revisada anualmente de forma regular con el objeto de permitir su constante actualización. La actividad de revisión incluye oportunidades de mejoras, en respuesta a los cambios organizacionales, a cambios significativos en procesos críticos o a cambios normativos, legales, de terceros, tecnológicos o de otra índole. Los cambios en la Política de Seguridad de la Información deberán ser aprobados por la máxima autoridad de la jurisdicción o en quien ella delegue esa facultad.

La presente Política de Seguridad de Información entrará en vigencia a partir del día siguiente de su publicación oficial.

Política Organizativa de la Seguridad

La A.N.M.A.T. apoyará e impulsará las iniciativas de seguridad que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona y almacena.

Se establecerán responsables del cumplimiento de los distintos procesos y funciones asociados a la seguridad de los sistemas de información dentro de la A.N.M.A.T., como también la supervisión de los aspectos inherentes a la seguridad tratados en la siguiente política.

Se designarán, propietarios de la información y propietarios de activos, quienes serán responsables por el resguardo de los mismos.

Se establecerá la segregación de las funciones asignando distintos perfiles o áreas de responsabilidad para evitar tener conflictos de intereses.

Se promoverá el contacto con otros organismos públicos y entidades privadas para el intercambio de experiencias en materias de seguridad, con el objeto de actualizar e intercambiar conocimientos relativos a seguridad y promover la capacitación continua.

Se contemplará la seguridad de la información en todos los proyectos tecnológicos que lleve adelante la

A.N.M.A.T.

Se establecerán requisitos de seguridad para el uso de dispositivos móviles, al igual que requisitos para implementar el trabajo remoto.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 1.

Política de Uso Aceptable de los Recursos de Tecnología de la Información

Se establecen directivas para el uso adecuado de la información, los sistemas informáticos y entorno tecnológico que posee la A.N.M.A.T., se especifican acciones consideradas prohibidas con respecto al uso del correo electrónico, Internet y demás recursos tecnológicos de hardware y/o de software, cedidos para su uso laboral al personal de la A.N.M.A.T. Se establecen pautas de conducta para regular el uso de los recursos informáticos que se utilizan.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 2.

Política de Recursos Humanos

Se establecerá, la aceptación del cumplimiento del Acuerdo de Confidencialidad y de la Política de Seguridad de la Información en la contratación. Y durante la relación laboral, la responsabilidad del debido cuidado de los activos tecnológicos cedidos para sus labores y la devolución de los mismos al finalizar el vínculo laboral con la A.N.M.A.T.

La Dirección de Recursos Humanos en las etapas de inducción de los agentes, notificará la existencia y el deber de cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ellas surja.

Se establecerá que, ante el incumplimiento de la presente Política de Seguridad de la Información y los procedimientos que en consecuencia se aprueben serán de aplicación los procesos disciplinarios que correspondan de conformidad con la normativa vigente y atendiendo en cada caso la situación de revista y forma de contratación de cada agente.

Todas las direcciones velarán e impulsarán el cumplimiento de la política de seguridad de la información. Asimismo, deberán establecer claramente los niveles, perfiles o permisos para acceder a la información y sistemas para todo personal a su cargo, definiendo los perfiles de trabajo y/o permisos en las áreas de su incumbencia.

Los directores y/o jefes de unidades organizativas son responsables ante la desvinculación o cambio de función del personal, que el conocimiento que estos posean sea documentado y transferido apropiadamente, antes de proceder a su desvinculación o cambio de función para evitar afectar el normal funcionamiento de las tareas en su ausencia.

Se establece el compromiso de concientizar y capacitar al personal en temas referidos a las buenas prácticas en seguridad de la información en coordinación con la Dirección Informática. Como también el de promover el entrenamiento especializado y frecuente de quienes desarrollan funciones en áreas de seguridad de la información de la A.N.M.A.T.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 3.

Política de Gestión de Activos

Se establecerá la existencia de un inventario de activos actualizado, debiendo designar responsables. Si bien la implementación de los controles de seguridad, gestión técnica u operativa podrá ser delegada a personal especializado, el responsable seguirá teniendo a su cargo el activo que le ha sido asignado.

Se establecerá el compromiso de devolución de activos asignados previa a su desvinculación, antes de la finalización del vínculo laboral, contrato o acuerdo con la A.N.M.A.T.

Se definen normas de uso de los activos de tecnología según las pautas declaradas en la Política de Uso de los Activos de los Recursos de Tecnología de la Información y la devolución de los mismos cuando el agente se desvincule laboralmente o cuando sea necesario su entrega debido a un cambio en sus funciones.

Se establecerá el tratamiento apropiado para la eliminación de forma segura de los activos de información sobre cualquier medio que pueda contener información de la A.N.M.A.T.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 4.

Política de Control de Accesos

Se controlará el acceso a las redes, servicios, información y a los recursos tecnológicos de la A.N.M.A.T., a través de la existencia de directivas y procedimientos que reglamentan la gestión de usuarios y la gestión de permisos de acceso a la información y a los recursos tecnológicos de la A.N.M.A.T.

Se restringirá el acceso a la información, en concordancia con la clasificación de la misma, sobre la base de la premisa rectora, “Todo acceso está prohibido, a menos que se permita explícitamente” mediante la autorización formalizada de cada dirección indicando los perfiles y permisos de acceso del personal a su cargo a los sistemas y/o recursos de información que sean requeridos para las actividades y tareas que cada empleado o funcionario deba llevar adelante.

Se establecerá el seguimiento de las cuentas con privilegios especiales y la revisión de los permisos de acceso configurados en los sistemas mediante auditorias periódicas, controlando que estos coincidan con los perfiles y permisos informados por cada dirección de la A.N.M.A.T.

Se establecerá la gestión segura de las contraseñas y/o dispositivos de autenticación, como también las responsabilidades de los usuarios sobre el uso de los mismos, por lo cual se establecerá que los agentes, funcionarios y demás usuarios deberán hacer un uso responsable de sus dispositivos y datos de autenticación. Se declara que se encuentra estrictamente prohibido compartir los mismos.

Establecerá que los sistemas de administración de contraseñas, apliquen contraseñas de calidad, por lo cual se deberán establecer criterios de complejidad como ser longitud mínima, caracteres, mayúsculas, minúsculas y caracteres numéricos o especiales para su conformación y cambios de forma periódica. Se promoverá el uso de gestores de almacenamiento de contraseñas para los usuarios finales mediante aplicaciones específicas para tal fin.

Se prohíbe que personal no autorizado haga uso de programas especiales con capacidades de anulación de los sistemas de control y seguridad.

Se promoverá el inicio de sesión seguro mediante la implementación de dos o más factores de autenticación para

acceder a los sistemas y servicios cuando sea posible. Se limitará el acceso al código fuente de los programas de la A.N.M.A.T. solo al personal autorizado.

Se monitorea, inspecciona y controla el tráfico de datos en las redes de la A.N.M.A.T., comunicaciones internas, como también toda comunicación externa entrante hacia las redes de la A.N.M.A.T. y toda comunicación saliente hacia Internet con el objeto de verificar que no se violen las políticas de seguridad establecidas.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 5.

Política en la Gestión de la Criptografía

Se establecerá el uso de la criptografía para asegurar la información y las comunicaciones, el resguardo de las contraseñas, en el almacenamiento de las copias de seguridad, en el cifrado de dispositivos móviles, en las conexiones de trabajo remoto, en la comunicación de los servicios expuestos a Internet y en toda transmisión de datos, dentro y fuera del ámbito de la A.N.M.A.T.

Se establece el uso de certificados digitales en todos los sitios de Internet que publica la A.N.M.A.T. para asegurar un canal de comunicación cifrado.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 6.

Política Físico Ambiental

Se controlará la identificación, ingreso y egreso físico a las dependencias de la A.N.M.A.T., con el objeto de evitar el acceso no autorizado, daño o hurto a las instalaciones e interferencias en las actividades de la A.N.M.A.T.

Se definen perímetros de seguridad y controles extras, para proteger las áreas consideradas como críticas, definiéndose inicialmente éstas como las áreas ocupadas por las oficinas de las autoridades superiores del Organismo, Sala de Comunicaciones, Centro de Procesamiento de Datos, Instalaciones de los Grupos Electrógenos e Instalaciones de Aire Acondicionado, considerando que la exposición, mal funcionamiento o puesta fuera de servicio de las mismas, pueda afectar el normal desempeño de los sistemas de información de la A.N.M.A.T.. A estos fines se establecerán controles adicionales, a través de la existencia de distintos niveles de accesos biométricos, control de seguridad física permitiendo solo el acceso autorizado, seguimiento y control mediante cámaras de seguridad, prohibición de grabaciones de video y fotografías sin la debida autorización y acompañamiento por personal de la A.N.M.A.T. ante la ejecución de trabajos por parte de proveedores.

Se asegura la continuidad operacional del suministro de energía eléctrica y del control ambiental en el centro de procesamiento de datos y sala de comunicaciones, como también la existencia de controles de seguridad para asegurar la protección del cableado de transmisión de datos.

Se establecerá la existencia del inventario de activos físicos que procesan información, indicando su localización física y asignación organizacional y personal para su uso. Se establecerá el registro de las personas y de los activos que son retirados fuera de las instalaciones de la A.N.M.A.T., la adopción de controles y medidas de seguridad extras para el equipamiento informático que es utilizado fuera de la A.N.M.A.T., con el objeto de minimizar el impacto ante la pérdida o robo del mismo.

Se propiciará el mantenimiento periódico del equipamiento informático y destrucción segura de los dispositivos de almacenamiento, cuando el equipamiento no pueda ser reutilizado o donado, con el objeto de no exponer información residual, considerada privada o confidencial en el equipo informático.

Se adoptará la política de escritorios limpios, con el objeto de proteger documentación en papel u otro medio de almacenamiento de información reservada, confidencial o secreta que pudiera existir en el área de trabajo, evitando de este modo su pérdida y divulgación no deseada. Se adoptará también la política de pantallas limpias, a fin de reducir los riesgos de acceso no autorizado y/o fuga de información desde el equipo informático que se encontrase desatendido.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 7.

Política de Seguridad en las Operaciones

Se declararán responsables de las operaciones, quienes deberán documentar procedimientos para gestionar las principales tareas operativas en las instalaciones de procesamiento de información. Se redactará documentación de gestión de cambios, como requisito previo a la implementación de los cambios en la infraestructura y/o sistemas de procesamiento de información.

Se evaluará periódicamente las necesidades de capacidad operacional de los sistemas y la proyección de futuras demandas, con el objeto de garantizar que el crecimiento no ponga en riesgo las actividades operativas ante la falta de recursos.

En los procesos de desarrollo de software, se definirán entornos separados e independientes entre sí, con el objeto de generar software seguro, sin defectos o fallos en el servicio que ofrecen y evitar problemas de indisponibilidad.

Se protegerán los sistemas tecnológicos contra todo tipo de código malicioso, mediante la ejecución de análisis periódicos preventivos de detección y eliminación de malware en las estaciones de trabajo, servidores, como también controles de detección y eliminación de malware en las conexiones de internet y correo electrónico.

La información y los sistemas se deberán resguardar de manera periódica y programada mediante la generación de copias de seguridad y pruebas de restauración.

Se sincronizan los relojes de todos los sistemas para el correcto registro de los eventos de los usuarios y sistemas; respecto de accesos, fallas, instalación y ejecución de software, alertas de seguridad y cualquier otra actividad relevante. Dichos registros de eventos se almacenarán de forma segura para futuras consultas o actividades de auditoría, teniendo especial cuidado con los registros de eventos de usuarios con privilegios de administrativos para evitar su manipulación.

La instalación de software está supeditada conforme a los procedimientos, autorizaciones, conformidades y pruebas previas pertinentes antes que los mismos sean puestos en producción y solo podrá ser efectuado por personal autorizado.

Se evaluará la seguridad de los sistemas publicados, mediante pruebas periódicas de evaluación de vulnerabilidades y elaboración de informes de remediación y mejoría para su corrección.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 8.

Política en la Gestión de las Comunicaciones

Se debe monitoreará, registrará, controlará y restringirá el acceso a las redes que integran la infraestructura de telecomunicaciones de la A.N.M.A.T., independientemente del medio de transmisión implementado.

Segregará y restringirá el tráfico de red de acuerdo a los perfiles y permisos asignados a los usuarios, que fueran declarados por los responsables de las distintas unidades organizativas.

Se controlará el tráfico hacia y desde Internet con el objeto de evitar que la navegación transgreda las normas establecidas en la Política de Uso Aceptable de los Recursos de Tecnología de la Información.

Se promoverá que la autenticación de los usuarios sea realizada implementando múltiples factores de autenticación para asegurar la identidad de los usuarios antes que estos acceden remotamente a las redes de la A.N.M.A.T.

Se implementarán dispositivos de red redundantes para mantener la alta disponibilidad en los servicios de red.

El intercambio de información con entidades externas se deberá realizar a través conexiones cifradas de extremo a extremo y se deberá promover la implementación de certificados digitales para la validación de las dos partes intervinientes y de este modo asegurar la confidencialidad, integridad y la autenticidad de la información que se transmite y envía hacia redes externas.

En los acuerdos entre el A.N.M.A.T. y otras entidades públicas o privadas, relativos al intercambio de información, se especificarán consideraciones técnicas de seguridad para la transferencia segura de datos entre ambas partes, como también se establecerán acuerdos de confidencialidad para la protección de la información que se comparte.

Se considera al correo electrónico un servicio crítico, por lo cual se implementan medidas de protección mediante sistemas redundantes para la gestión del correo electrónico y sistemas de seguridad antimalware y filtros anti-spam, con el objeto de detectar archivos adjuntos maliciosos o correos fraudulentos que intenten robar o dañar los activos de información.

La utilización de servicios de Internet será monitoreada y controlada, con el objeto de evitar que el uso indebido de dichos servicios afecte el rendimiento de la infraestructura de comunicaciones o pongan en riesgo la seguridad de la misma ante la descarga e instalación de archivos. Razón por la cual el uso de Internet, al igual que el uso del correo electrónico laboral estará sujeta a las condiciones de uso descriptas en la Política de Uso Aceptable de los Recursos de la Tecnología de la Información.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 9.

Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

En toda adquisición de sistemas informáticos, como también en todos los proyectos de desarrollo de software, tanto propios o de terceros, se deberá establecer la inclusión de requerimientos de seguridad, como también la existencia de directivas de seguridad para el desarrollo de aplicaciones, las cuales describen requerimientos básicos de seguridad a considerar en todo desarrollo.

Se considera a la seguridad de la información como una parte importante en los ciclos de vida de los procesos de desarrollo y adquisición, por lo cual se deberá contemplar la seguridad en todos los niveles de la arquitectura, negocios, datos, aplicaciones y tecnología; equilibrando la necesidad de la seguridad con la accesibilidad.

Se deberán establecer controles para asegurar los sistemas de la A.N.M.A.T. expuestos a Internet, con el objeto de protegerlos contra actividades fraudulentas, modificaciones y divulgación de datos no autorizados, intercepción, vulneración de la confidencialidad, suplantación de identidad y cualquier otra amenaza existente.

Se deberán evaluar, validar y documentar los cambios, con el objeto de minimizar los riesgos de modificaciones indebidas que pudieran comprometer las operaciones en el entorno productivo, respetando las instancias de desarrollo, pruebas y producción e incorporando de este modo efectivos controles cruzados o por oposición.

Se deberán realizar evaluaciones de seguridad en busca de vulnerabilidades sobre desarrollos de software nuevos o modificaciones, propios o de terceros y del sistema operativo de la plataforma en la que está implementada la misma antes que los mismos sean puestos en producción.

Se deberán establecer programas de ejecución de pruebas funcionales que permitan evaluar los requisitos funcionales y el cumplimiento de los mismos en los sistemas desarrollados.

Se declara que todo algoritmo o código fuente desarrollado internamente o por terceros es de propiedad exclusiva de la A.N.M.A.T., estando prohibida su copia parcial, total y distribución de la misma a terceros sin la debida autorización. Se deberán usar datos de prueba de manera segura para las pruebas funcionales.

La modificación, actualización o eliminación de los datos operativos en producción deberán ser realizadas, solo a través de los sistemas que procesan dichos datos. Se considerarán excepciones, debiendo ser las mismas documentadas e informadas a las partes interesadas siendo estos los propietarios de la información, los responsables de la gestión funcional y técnica y el responsable de los procesos a los cuales afecte la modificación manual, debiéndose registrar detalladamente dicha modificación.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 10.

Política en Relación a los Proveedores

Se incluirán los niveles de servicio (SLA) y acuerdos de confidencialidad en los contratos o convenios con los proveedores. Se establece que todo cambio a realizar por lo proveedores sobre los sistemas e infraestructura deberá ser planificado e

informado previamente al personal técnico del área de competencia, para su evaluación, cálculo del riesgo que implica dicho cambio y confirmación de ejecución por parte del personal técnico de la A.N.M.A.T. para lo cual se establece la gestión de cambios.

Los proveedores que accedan físicamente a las instalaciones para dar soporte, se deberán identificar, registrar sus ingresos y deberán estar siempre acompañados por personal técnico de la A.N.M.A.T. dentro de las instalaciones de la A.N.M.A.T.

Se deberán controlar las implementaciones de los proveedores, monitorear su cumplimiento y la gestión en los cambios, con el fin de asegurar que los servicios que se presten, cumplan con todos los requerimientos acordados previamente.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 11.

Política de Gestión de Incidentes de Seguridad

Se establece que la Dirección de Informática tiene la autoridad para acceder a todo sistema o dispositivo de la infraestructura tecnológica involucrada en alertas o incidentes de seguridad que considere apropiado, para evitar que escale y pudiera afectar la disponibilidad, confidencialidad o integridad de la información y de los recursos tecnológicos de la A.N.M.A.T.

El personal de la A.N.M.A.T., cuando descubra fallas o debilidades, detecte alertas o incidentes de seguridad, tiene la obligación de informarlo a la DIRECCIÓN DE INFORMÁTICA.

Se deberán establecer procesos documentados y asignación de responsabilidades para la adecuada gestión de respuesta a incidentes de seguridad de la información. Se deberá incluir la recopilación y registro de evidencia para su evaluación inicial, análisis del incidente y acciones de remediación, comunicación del estado de situación del proceso de resolución del incidente, registro formal de las acciones realizadas y cierre del incidente, cuando sea necesario se realizará un análisis forense y/o post-incidente, para confirmar la causa y aprender del mismo.

Se deberán documentar procedimientos para la correcta adquisición de imágenes forenses y preservación de la información que pudiera servir como evidencia, ya sea para implementar una medida disciplinaria interna o iniciar una acción legal.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 12.

Política de Gestión de la Continuidad

A fin de contrarrestar la pérdida de la continuidad operativa, se deberá desarrollar e implantar el plan de contingencia para asegurar la continuidad de los procesos de la A.N.M.A.T., para que las operaciones se puedan restaurar en los plazos requeridos.

Para garantizar que los planes operativos de restauración de las operaciones sean ordenados y consistentes entre sí, se deberá tener en cuenta la priorización los procesos críticos, la asignación de responsabilidades, la identificación de las amenazas que pudieran ocasionar interrupciones en los procesos, la documentación de la estrategia de continuidad de las actividades consecuente con los objetivos y prioridades acordados, la comunicación y capacitación del personal, en materia de procedimientos y procesos de emergencia acordados y de recuperación.

Se deberán realizar pruebas y revisiones de los planes de continuidad de las operaciones con el objeto de mantenerlos actualizados ante cambios en los procesos de negocio y en la tecnología involucrada.

Para minimizar el riesgo de la pérdida de la continuidad operativa se deberán implementar arquitecturas y/o componentes redundantes en las instalaciones de procesamiento y transmisión de la información.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 13.

Política de Cumplimiento Normativo y Técnico

Se respetan los requisitos contractuales, regulatorios y legales vigentes. Los empleados aceptan conocer y cumplir con lo dispuesto por la Ley 25.164 (Ley Marco de Regulación de Empleo Público Nacional), Ley 25.188 (Ética en el Ejercicio de la Función Pública), Decreto 41/99 (Código de Ética de la Función Pública), Ley 11.723 (Ley de Propiedad Intelectual), Ley N° 25.506 (Ley de Firma Digital) y Ley 26.388 (Ley de Delitos Informáticos).

Se establece la protección de los registros de datos contra pérdida, destrucción, acceso no autorizado, publicación

no autorizada, degradación del medio de almacenamiento, obsolescencia del formato o medio de almacenamiento.

Se respeta la privacidad de la información personal por lo cual se informa y detallan las actividades que serán objeto de control y monitoreo, a fin de no violar el derecho a la privacidad del empleado. A su vez los empleados conocen las restricciones al tratamiento de los datos y de la información que administran con motivo del ejercicio de sus funciones, por lo cual firman el Acuerdo de Confidencialidad.

Se verifica periódicamente que los sistemas de información cumplan con lo establecido por la Política de Seguridad de la Información, normas y procedimientos de seguridad; las que incluirán la revisión de los sistemas en producción. Esta verificación comprende pruebas de evaluación de vulnerabilidades y/o pruebas de penetración, cuyo objetivo es la detección de vulnerabilidades en los sistemas y la infraestructura.

Se establecen auditorias de cumplimiento en los sistemas de información, infraestructura tecnológica y en los procesos existentes, como también de la revisión independiente del estado de la seguridad realizada por la Unidad de Auditoría Interna o Especialistas de Seguridad externos a la A.N.M.A.T. para garantizar la eficacia de los controles implementados.

Los objetivos, responsabilidades y políticas detalladas de la presente se encuentran desarrolladas en el Anexo 14.

POLÍTICAS ESPECÍFICAS

ANEXO 1.

POLÍTICA ORGANIZATIVA DE LA SEGURIDAD

OBJETIVOS

Designar responsables de los procesos relacionados con la seguridad de la información dentro de la A.N.M.A.T. y establecer un marco para su control.

Incluir requerimientos de seguridad de la información en todo proyecto tecnológico de la A.N.M.A.T.

Promover la cooperación con otros organismos y organizaciones especializados para la obtención de colaboración en materia de seguridad de la información.

Asegurar el uso de dispositivos móviles para el trabajo remoto.

RESPONSABILIDADES

Máxima Autoridad de la A.N.M.A.T. o en quien esta delegue tal competencia.

• Aprobar la presente política de seguridad de la información.

• Promover la difusión y apoyo a la seguridad de la información dentro de la A.N.M.A.T.

• Impulsar la implementación y cumplimiento de la presente política de seguridad.

• Apoyar la implementación de la presente política de seguridad de la información.

DIRECCIÓN DE INFORMÁTICA

• Revisar y proponer a la máxima autoridad de la A.N.M.A.T. para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.

• Solicitar la elaboración de procedimientos y/o instructivos a las distintas unidades organizativas de la A.N.M.A.T. para establecer pautas formales de cumplimiento de las políticas de seguridad.

• Coordinar la interacción con otros organismos en temas referidos a la seguridad de la información.

• Cumplir funciones relativas a la seguridad de los sistemas de información de la A.N.M.A.T., la cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política de Seguridad de la Información.

• Monitorear los cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

• Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.

• Evaluar y coordinar la implementación de controles de seguridad en todo proyecto tecnológico de hardware, software, desarrollo o modificación de sistemas o servicios.

• Actualizar políticas y directivas relativas a la Seguridad de la Información para su aprobación oficial.

• Gestionar los riesgos que afectan a los recursos de información frente a las amenazas existentes.

• Tomar conocimiento y supervisar la investigación de aquellos incidentes relativos a la seguridad.

• Evaluar y aprobar las principales iniciativas para incrementar la seguridad de la información.

• Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

• Promover la difusión y concientización de la seguridad de la información dentro de la A.N.M.A.T.

• Controlar todo acceso a los recursos de tecnológicos de la A.N.M.A.T.

• Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas.

• Monitorear, controlar y evaluar la información recibida por los controles de seguridad.

• Gestionar los incidentes de seguridad de la información y recomendar las acciones apropiadas como respuesta a los mismos.

• Identificar, evaluar y proponer el tratamiento de los riesgos y amenazas a los que se expone la información y los recursos tecnológicos de la A.N.M.A.T.

• Detectar, analizar, remediar y recolectar evidencia forense de incidentes de seguridad, ante actuaciones que ameriten intervención administrativa o judicial.

• Asistir en temas relativos a la seguridad de la información.

• Inhabilitar el acceso remoto a la infraestructura tecnológica de la A.N.M.A.T., cuando se detecte que dicho acceso represente una amenaza que pudiera vulnerar la confidencialidad, integridad y/o disponibilidad de la información o de los sistemas y recursos de la A.N.M.A.T.

• Cumplir con todos los requerimientos de seguridad establecidos para las operaciones, administración y configuración de los sistemas y recursos de tecnología de la A.N.M.A.T.

• Gestionar los requerimientos y necesidades de las contrataciones de bienes y servicios de tecnología de la A.N.M.A.T.

• Controlar el vencimiento de licenciamiento y/o contrataciones.

• Controlar y gestionar el inventariado de activos de TI.

• Efectuar tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada y que contemple la inclusión de requerimientos de seguridad en los sistemas en todas sus fases.

Dirección de Recursos Humanos

• Notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

• Notificar a todo el personal de los cambios que en la presente política se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad y las tareas de capacitación continua en materia de seguridad, en conjunto con la Dirección de Informática.

Dirección de Asuntos Jurídicos

• Revisar y validar las modificaciones de la presente política.

• Verificar el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la A.N.M.A.T. con los empleados y en caso de existir, con los terceros. Asimismo, asesorar en materia legal a la Dirección de Informática, en lo que se refiere a la seguridad de la información.

Unidad de Auditoría Interna

• Revisar y validar las modificaciones de la presente política.

• Practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecida por las políticas, normas, procedimientos y prácticas que de ella surjan.

• Verificar, a través de las auditorías que correspondan, el cumplimiento de la presente Política en las unidades organizativas de la A.N.M.A.T.

• Realizar revisiones independientes sobre el cumplimiento de la presente política.

• Promover, dentro de su ámbito de competencia, la aplicación de la presente política de seguridad de la información.

Unidades Organizativas de la A.N.M.A.T.

• Implementar la Política de Seguridad de la Información dentro de sus áreas de responsabilidad

• Promover su cumplimiento por parte de su equipo de trabajo.

Agentes de la A.N.M.A.T.

• Los usuarios de la información y de los sistemas utilizados para su procesamiento serán responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

POLÍTICAS

1.1. Organización Interna

1.1.1. Compromiso de la Máxima autoridad de la Jurisdicción y Asignación de Responsabilidades de la Seguridad de la Información

La A.N.M.A.T. declara apoyar e impulsar desde el mayor nivel jerárquico las iniciativas de la seguridad de la información dentro del organismo, mediante la aprobación de la presente política de seguridad de la información y su implantación como documento rector de seguridad de la información, con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona dentro del organismo y su infraestructura tecnológica.

La seguridad de la información es una responsabilidad compartida por todas las autoridades políticas, secretarios, subsecretarios, directores de todos los niveles, subdirectores y jefes de unidad o equivalentes.

1.1.2. Segregación de Funciones

Se diseñarán esquemas de segregación de funciones y áreas de responsabilidades en la gestión de los sistemas informáticos.

Se establecerá la separación de funciones en los procesos de asignación de permisos a los activos de información, por lo cual se establecerán distintas entidades, propietario (propietario del activo de información), solicitante (el que solicitará el acceso), autorizante (el que autorizará) y operador (el que concederá operativamente el acceso).

1.1.3. Contacto con las autoridades

Se establecerán procedimientos que especifican cuándo, a qué autoridades se deberá contactar y cómo se deberá informar los incidentes de seguridad de la información identificados de manera oportuna, de acuerdo a lo estipulado en la POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD, en cumplimiento con las normativas vigentes.

1.1.4. Contacto con grupos especializados en seguridad informática y otros organismos

Se promoverá la asistencia y contacto con eventos, grupos, foros y/o asociaciones especializados de

ciberseguridad, con el fin de actualizar los conocimientos sobre buenas prácticas en materia de seguridad del personal de la Dirección de Informática, recibir alertas tempranas, avisos y recomendaciones relacionados con ataques informáticos, compartir e intercambiar información sobre las nuevas tecnologías, productos, amenazas, vulnerabilidades y obtener acceso a información de especialistas sobre consejos de seguridad.

Se propiciará el intercambio de experiencias, conocimiento y/o capacitación para el mejoramiento de las prácticas y controles de seguridad con otros organismos en temas relativos a la seguridad de la información. Teniendo en cuenta que cuando sea necesario realizar el intercambio de información no pública para fines de asesoramiento o intercambio de experiencias se permitirá solo luego de haber firmado previamente acuerdos de confidencialidad.

1.1.5. Seguridad de la información en la gestión de proyectos

Se tendrán en cuenta requisitos de seguridad de la información en la administración de los proyectos, a efectos de garantizar que se reflejen adecuadamente las buenas prácticas de seguridad y las disposiciones de la presente política. La seguridad de la información será parte de todas las fases de las metodologías aplicadas en la gestión de los proyectos de la A.N.M.A.T.

1.2. Política de Dispositivos Móviles y Trabajo Remoto

1.2.1. Dispositivos Móviles

Todo dispositivo móvil perteneciente a la A.N.M.A.T. (notebooks, tabletas, teléfonos celulares y otros), deberá cumplir con medidas seguridad adecuadas para proteger el dispositivo móvil y la información que contiene contra todos los riesgos derivados del uso del mismo.

Por lo cual se establecen las siguientes directivas para asegurar al dispositivo móvil y la información contenida:

a) Etiquetado de teléfonos de contacto para posibilitar su recupero en caso de pérdida.

b) Instalación de software antimalware en el dispositivo móvil.

c) Cifrado del medio de almacenamiento del dispositivo móvil.

d) Mecanismos de borrado seguro de la información en forma remota, en caso de robo o pérdida.

e) Implementación de controles para la gestión remota de dispositivos móviles.

1.2.2. Trabajo Remoto

Todo acceso remoto será solicitado por el responsable jerárquico de la unidad organizativa a la cual pertenece el usuario que será designado a trabajo remoto total o parcial.

Todo acceso remoto será implementado mediante una conexión cifrada, la cual será monitoreada y controlada por los dispositivos de seguridad de la A.N.M.A.T., implementando restricciones de acceso a determinados activos de información dependiendo de la criticidad de la misma y perfil del usuario.

Se establecerán múltiples factores de autenticación para asegurar la identidad de las conexiones remotas a las redes privadas virtuales (VPN) de la A.N.M.A.T.. Si el trabajo remoto fuera efectuado desde afuera del territorio nacional se deberá informar a la Dirección de Informática.

1.2.3. Dispositivos Personales

No se habilitarán dispositivos personales para acceder a la infraestructura tecnológica de la A.N.M.A.T., salvo excepciones puntuales que serán evaluadas por la Dirección de informática, a fin de garantizar que se cumplan las medidas, requerimientos y políticas de seguridad vigentes.

Todo dispositivo personal que fuera autorizado para su acceso a la infraestructura de la A.N.M.A.T. cumplirá las políticas de los dispositivos móviles pertenecientes a la A.N.M.A.T., promoviéndose para estos dispositivos el acceso a un escritorio remoto virtual.

ANEXO 2

POLÍTICA DE USO ACEPTABLE DE LOS RECURSOS DE TECNOLOGÍA DE LA INFORMACIÓN

OBJETIVOS

Establecer el uso adecuado de la información, de los sistemas informáticos y del ambiente tecnológico que posee la A.N.M.A.T., con el objeto de minimizar los riesgos de seguridad que pudieran ser ocasionados por el uso indebido de los recursos informáticos asignados.

Concientizar al personal respecto de las acciones consideradas prohibidas con respecto al uso del correo electrónico, Internet y demás recursos tecnológicos de hardware y/o de software cedidos para su uso laboral al personal en la A.N.M.A.T. y de las pautas de conducta para regular el uso de los recursos informáticos que se utilizan en la A.N.M.A.T., ya sean propios o de terceros.

RESPONSABILIDADES PERSONAL JERARQUICO

Los superiores jerárquicos y/o titulares de unidades organizativas del personal tendrán las responsabilidades de:

• Asegurar que el personal conozca la Política de Uso Aceptable y velar por su cumplimiento.

• Determinar qué recursos tecnológicos son necesarios para que cada una de las personas a su cargo pueda desempeñar las tareas que se le asignaron, esto incluye equipamiento y software, cuenta de acceso al correo electrónico y cuenta de acceso a los sistemas de la A.N.M.A.T.

• Solicitar los permisos de accesos a servidores, aplicaciones o recursos compartidos, especificando el nivel de acceso para cada caso en particular.

• Solicitar la cancelación o modificación de permisos de accesos a servidores, aplicaciones y recursos compartidos, cuando haya un cambio de funciones, desvinculación y/o tareas asignadas a sus supervisados.

• Solicitar accesos especiales a Internet para los agentes a su cargo cuando lo requieran en razón de sus funciones.

• Solicitar el acceso remoto para sus subordinados a la infraestructura tecnológica de la A.N.M.A.T.

• Controlar las acciones de sus subordinados, ya que son responsables por las acciones indebidas que pudieran

realizar los mismos al concederles los respectivos accesos.

• Canalizar toda solicitud a través de los canales formales, es decir a través de Mesa de Ayuda.

PERSONAL EN GENERAL

El personal tendrá las siguientes responsabilidades:

• Conocer y aplicar especialmente lo establecido en la Política de Uso Aceptable de los Recursos de Tecnología de la Información.

• Actuar conforme a los Procedimientos y Políticas y de Seguridad de la Información existentes en el uso de los recursos informáticos asignados.

• Evitar toda práctica que pueda hacer uso sin la debida autorización, de programas o sistemas, que pudieran degradar el rendimiento o dañar la infraestructura tecnológica de la A.N.M.A.T.

• Contactar con la Mesa de Ayuda, toda vez que requieran resolver un problema suscitado con el equipo asignado, referido a conexión de red, incidente con el software de la estación de trabajo (notebook, PC, tableta, etc.), detección de malware o cualquier otro incidente relacionado con el sistema o equipamiento en uso.

• Conducirse con el decoro y obediencia que se requiere en los agentes públicos.

• Cumplir con la política de pantallas limpias, los usuarios deberán bloquear el acceso a su computadora personal cuando se ausente de su lugar de trabajo, aun cuando esta ausencia sea breve.

• Identificar adecuadamente toda comunicación indicando su nombre, correo electrónico, dirección y área a la cual pertenece.

• Evitar la divulgación no autorizada e innecesaria de información a terceros, respecto de los cuales se tiene conocimiento y/o responsabilidad profesional en el marco de sus tareas dentro de la A.N.M.A.T.

POLÍTICAS

2.1. Usos Aceptables

2.1.1. Uso General

Los recursos tecnológicos de la A.N.M.A.T. solo deben ser utilizados para propósitos de uso laboral que guarde relación con las funciones asignadas.

Los usuarios de los sistemas informáticos toman conocimiento que una cuenta de usuario representa una identidad digital. Por lo tanto, cada vez que se utilizan los recursos informáticos de los diferentes sistemas que se utilizan, o se intentan utilizar, se registran los accesos y/o actividades que se realizan con dicha cuenta de usuario. La contraseña utilizada para autenticar una cuenta de usuario, es uso estrictamente personal y confidencial, razón por la cual no debe ser compartida ni aún con su superior jerárquico.

Los usuarios toman conocimiento que las cuentas de correo electrónico, sistemas utilizados y demás recursos informáticos son pertenecientes a la A.N.M.A.T. y que constituyen bienes intangibles, por lo que toda utilización de los mismos podrá ser considerado por terceros, como realizada en representación de la

A.N.M.A.T.

2.1.2. Uso del Equipamiento

La A.N.M.A.T. proveerá a su personal y a toda persona que preste tareas en su ámbito, las herramientas de hardware y software necesarias para su desempeño laboral siendo los depositarios de dichas herramientas responsables de su uso, debiendo los mismos ser utilizados exclusivamente para propósitos relacionados con sus actividades laborales.

El usuario está obligado a dar el debido tratamiento para el cuidado de dichas herramientas, de forma tal de evitar cualquier daño físico, lógico, conexión, desconexión o traslado sin la debida autorización.

Queda prohibida la conexión a la infraestructura tecnológica de la A.N.M.A.T. de cualquier equipo informático no perteneciente a la misma sin la debida autorización.

2.1.3. Uso de los Sistemas de Software

Solo los usuarios que fueran autorizados pueden acceder a los sistemas y a la información de la A.N.M.A.T. para el desarrollo de sus actividades laborales. Cualquier acceso no autorizado o intento de acceso no autorizado será considerado como una posible violación a la Política de Seguridad de la Información.

Los usuarios que por alguna razón consideren que necesitan accesos adicionales, deberán canalizar el pedido de acceso adicional a través de su coordinador o director mediante pedido a la Mesa de Ayuda.

Todo personal que instale o posea software no autorizado por la A.N.M.A.T., quedará sujeto al régimen de sanciones del Reglamento de Investigaciones Administrativas y/o que corresponda, y podrá ser objeto de las denuncias penales pertinentes por violación a la ley propiedad intelectual y de las pautas de ética en la función pública.

El área de Soporte Técnico es responsable de la instalación, configuración, puesta en funcionamiento y mantenimiento de todo el equipamiento y software existente en la A.N.M.A.T.. Cuando las unidades organizativas requieran para el desempeño de sus tareas, software específico, deberán remitir la solicitud de instalación a la Mesa de Ayuda mediante los canales formales. Todo aquel software que se encuentre instalado sin la debida autorización o almacenado en carpetas locales o compartidas que no guarde correspondencia con el software autorizado por la A.N.M.A.T. podrá ser desinstalado y/o eliminado.

2.1.4. Uso de la Información

La información perteneciente a la A.N.M.A.T. será utilizada únicamente dentro del marco de las actividades propias de la misma, quedando terminantemente prohibida la utilización de la misma en beneficio propio y todo tipo de divulgación a terceros, sin previa autorización de la A.N.M.A.T. La violación de lo dispuesto en la presente cláusula será considerada como falta grave en los términos del Artículo 33 inciso b) de la ley N° 25.164, sin perjuicio de la responsabilidad civil y penal que por el hecho corresponda.

La A.N.M.A.T. se reserva el derecho de auditar los archivos en las carpetas de los usuarios, ya sean en los servidores compartidos y en los dispositivos de almacenamientos externos o internos (discos locales de

almacenamiento en las estaciones de trabajo) pertenecientes a la A.N.M.A.T.

Los usuarios que cambien de función o se desvinculen laboralmente de la A.N.M.A.T., están obligados a entregar a su superior, toda la información y documentos electrónicos que hubieran elaborado en el cumplimiento de función hasta el momento que la desempeñaba, de forma tal que dicho cambio no genere problema alguno en la continuidad de las tareas que se venía desarrollando.

Todos aquellos archivos de documentos que se encuentren en carpetas locales o compartidas que no guarden relación con las funciones desempeñadas (por ejemplo, archivos de música, películas, fotografías, etc.) podrán ser eliminados.

Queda prohibida realizar cualquier actividad contraria a los intereses de la A.N.M.A.T., tal como publicar información reservada, confidencial o secreta, acceder sin autorización a recursos compartidos o archivos, e impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes.

Queda prohibido utilizar y/o entregar información de la A.N.M.A.T. fuera del ámbito de la Dirección propietaria de la misma, sin autorización expresa de la Dirección de pertenencia.

Queda prohibido difundir información que no sea de carácter público que se gestiona en la A.N.M.A.T., es decir información de carácter secreta, confidencial o reservada.

Queda prohibido destruir o corromper activos de información, ya sean datos, documentos, programas o sistemas informáticos de la A.N.M.A.T. o cualquier acción que impida el acceso legítimo a los mismos, siendo tal acción considerada una falta grave, pudiendo ser pasible a un proceso penal por infracción al Art. 10 de la Ley 26.388 de Delitos Tecnológicos.

2.1.5. Uso de las Contraseñas

Los usuarios se comprometen a mantener las contraseñas en secreto, ya que la contraseña es considerada información secreta y personal, no debiendo ser compartida, ni aún con su personal jerárquico. Cuando existiera indicio que la confidencialidad de la contraseña hubiera sido comprometida, se informará y solicitará el cambio de la misma, inmediatamente.

La composición de la contraseña no estará basada en datos que se pudieran prever u obtener fácilmente, mediante información relacionada con la persona, como ser nombres, números de teléfono, número de oficina, fechas de cumpleaños, etc.

El usuario no reutilizará o reciclará viejas contraseñas, como tampoco almacenará contraseñas en papel, archivos de texto, planillas de cálculo o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.

Se promueve el uso de gestores de contraseñas, software instalado en las estaciones de trabajo (computadoras personales y notebooks) para la correcta gestión de las mismas.

2.1.6 Uso de Internet

La A.N.M.A.T. otorga acceso a Internet a los agentes que por necesidad laboral requieran acceder a información o contenidos en beneficio del desarrollo de sus actividades.

Por lo tanto, el personal de la A.N.M.A.T. podrá hacer uso de Internet para mejorar y facilitar su actividad laboral, para acceder a información científica, técnica, comunicación con otros organismos oficiales, instituciones académicas o acceso relativo a temas inherentes con la función que desempeñan. También podrá hacer uso del servicio de Internet para otros fines que no sean los estrictamente laborales siempre y cuando se utilice para acceder en un tiempo razonable a sitios de uso común como ser servicios de correos electrónicos personales, gestión de servicios públicos o sitios de uso para la vida cotidiana de las personas como ser de educación y de salud, a menos que el responsable jerárquico de la unidad organizativa solicite inhabilitar dicho acceso.

El servicio de acceso a Internet no es irrestricto, el mismo es restringido y controlado, ya que se bloquean sitios clasificados con determinadas categorías. Por lo cual, con el objeto de minimizar el riesgo de violación a la seguridad a través del uso incorrecto del servicio de Internet, se requiere el cumplimiento de las siguientes pautas:

a) Queda prohibida la evasión de los controles de navegación por medio de software especializado o por medio de sitios de terceros que actúan como servidores intermediarios (proxies externos).

b) Queda prohibido el uso de streaming para entretenimiento, dado que dicha práctica puede afectar considerablemente el ancho de banda disponible en la A.N.M.A.T., degradando el tiempo de respuesta y generando dificultades de conectividad en las áreas que procesan información Institucional.

c) Queda prohibido descargar archivos de software sin la debida autorización.

d) Queda prohibida la carga o descarga de cualquier material que infrinja la Ley N° 11.723 de Propiedad Intelectual

e) Queda prohibida la distribución de software malicioso (malware).

f) Queda prohibida la descarga de archivos desde Internet, salvo que esta posibilidad no implique vulnerar o infringir los derechos de terceros titulares de derechos de autor.

g) Queda prohibido acceder a material pornográfico, actividades lúdicas o de entretenimiento, diversión o pasatiempos de similar tenor, páginas que promuevan el odio, el racismo, inciten a la violencia o con contenido contrario a las normas de sentido común y buenas costumbres.

h) Queda prohibido emitir comentarios o dar información en redes sociales sobre incidentes de seguridad acaecidos dentro de la A.N.M.A.T., de corresponder se realizará a través de los canales formales de difusión del organismo.

i) Queda prohibido atentar contra lo infraestructura tecnológica de terceros y/o de la A.N.M.A.T.

j) Queda prohibida cualquier conducta ilegal contraria a la legislación local o a la legislación del país a la cual pertenece el sitio que se accede por Internet.

2.1.7. Monitoreo y Auditoría

Dado que el equipamiento, los sistemas y la información que componen la infraestructura tecnológica son propiedad de la A.N.M.A.T., el uso de los mismos serán monitoreados y/o auditados mediante herramientas de seguridad y auditoria diseñadas para tal fin, comprendiendo dicha actividad el uso de los

equipos informáticos, tráfico de la red de datos, accesos a sistemas y bases de datos, uso de Internet y del correo electrónico, con las limitaciones que las disposiciones legales imponen en cuanto al respeto de la privacidad.

2.2. Usos Inadecuados

2.2.1. Uso Inadecuado de los Recursos

Los recursos informáticos de la A.N.M.A.T. se suministran con el propósito de asistir al agente en la ejecución de sus tareas laborales y de que realice el procesamiento de información que le fuera indicado. Por lo cual toda utilización de estos recursos con propósitos no autorizados o ajenos al destino para el cual fueron provistos será considerada como uso indebido.

Entre los usos indebidos se mencionan los siguientes:

a) Instalar software que no haya sido autorizado por la DIRECCIÓN DE INFORMÁTICA a efectos de evitar la piratería y prevenir la instalación de software que pudiera poner en riesgo la seguridad de la infraestructura tecnológica de la A.N.M.A.T. o generar problemas de índole legal por infracción a la Ley N° 11.723 de Propiedad Intelectual.

b) Iniciar cualquier acción que pueda comprometer la seguridad parcial o total de la infraestructura tecnológica o atentar contra el correcto funcionamiento del mismo.

c) Acceder sin autorización a sistemas o información no pública de la A.N.M.A.T.

d) Facilitar el acceso a la infraestructura tecnológica a personas no autorizadas, cediendo a terceros la credencial de acceso (usuario y contraseña) o tokens físicos o virtuales, permitiendo de este modo el acceso a la infraestructura tecnológica de la A.N.M.A.T..

e) Realizar cambios en la configuración del equipamiento sin la debida intervención de la Dirección Informática, incluyendo la conexión o desconexión de computadoras personales, impresoras, equipamiento de red, etc.

f) Deshabilitar o impedir el funcionamiento de soluciones antimalware instalada en el equipo.

g) Copiar o ejecutar software malicioso o cualquier otro software dentro de los sistemas de la A.N.M.A.T. que produzcan la disminución en la performance de la mismas

h) Violar los derechos de privacidad de terceras personas.

i) Copiar de manera no autorizada el software perteneciente a la A.N.M.A.T..

j) Descargar de archivos que no se cuentan con la licencia de uso respectiva y aún aquellos con licencia de software libre, software de fuente abierta, software de dominio público, trial, shareware o freeware sin la debida autorización de la DIRECCIÓN DE INFORMÁTICA.

k) Utilizar los recursos de tecnología de la información de la A.N.M.A.T. para el desarrollo de cualquier actividad comercial personal, ya sea la compra, venta u oferta de bienes o servicios o bien utilizar la red para la transmisión de publicidad comercial relacionada con dicha actividad, sea cual fuere la razón o la

magnitud de la misma.

l) Realizar la publicidad y/o promoción de cualquier actividad de recreación personal, tales como creencias religiosas, hobbies, etc.

m) Transmitir amenazas, material obsceno o de hostigamiento.

n) Utilizar la red para juegos recreativos.

o) Distribuir de material que cause daños como copias ilegales, accesos no autorizados, malware, sabotajes, etc.

p) Instalar y/o utilizar de software de navegación que no sean las aprobadas por la Dirección de Informática.

q) Emitir comentarios peyorativos acerca de la A.N.M.A.T. o su personal en foros públicos u otros medios de publicación electrónica.

r) Participar de foros, redes sociales, sistemas de chat o listas de discusión en línea que no se encuentren relacionados con sus actividades en la A.N.M.A.T., excepto los institucionales.

s) Utilizar programas especialmente diseñados para el intercambio de archivos (software “peer to peer”).

Los usuarios toman conocimiento de las siguientes normativas vigentes indicadas en la Política de Cumplimiento - Identificación de la Legislación Aplicable. Como también de las sanciones que pudieran generarse como consecuencia del uso indebido de los recursos tecnológico de información conforme la normativa vigente aplicable a cada caso concreto.

2.3. Uso del Correo Electrónico

2.3.1. Correo Electrónico

El usuario se compromete a cumplir con toda la normativa estatal, nacional e internacional aplicable y es único responsable de todos los actos u omisiones que sucedan en relación con su cuenta de correo y/o contraseña, incluido el contenido de sus mensajes realizados a través del mismo. El uso del servicio de correo electrónico implica la aceptación total de los términos y condiciones que rigen su uso en la presente política.

Las cuentas de correo del personal de la A.N.M.A.T., no son compartidas, por lo cual el usuario debe preservar la confidencialidad de su contraseña, debiendo cambiar la misma de acuerdo a lo especificado en el Procedimiento de Administración de Contraseñas cuando sospechara que la misma fue vulnerada. El usuario debe notificar de manera inmediata a la Dirección de Informática cualquier uso no autorizado de su cuenta de correo o cualquier otra vulneración de seguridad que detecte en la misma.

El servicio de correo electrónico habilitado al personal de la A.N.M.A.T. es para uso laboral, debiendo ser usado únicamente para el desempeño de sus funciones, por lo cual el usuario se compromete a enviar y recibir correos electrónicos solo para este propósito.

Los usuarios toman conocimiento que la cuenta de correo electrónico constituye un bien intangible de la

A.N.M.A.T., por lo que toda utilización del mismo podría ser considerada por los terceros como realizada en representación de la A.N.M.A.T.

Por lo tanto, al emitir opiniones personales, se debe aclarar que estas “no constituyen declaraciones oficiales de la A.N.M.A.T.”, en razón de que los recursos con los cuales se realiza la comunicación pertenecen a la A.N.M.A.T.

Se prohíbe cualquier uso personal, comercial o para fines ilícitos o prohibidos, de acuerdo a las normas vigentes en la presenta política. Excepto el relacionado con capacitaciones personales de la administración pública que pudieran ser comunicados por la Dirección de Recursos Humanos.

Los correos electrónicos enviados y recibidos por los usuarios serán controlados por los sistemas de seguridad antimalware y antispam, para minimizar el riesgo de recibir y enviar por este medio, correos y/o adjuntos maliciosos que pudieran vulnerar la seguridad de la infraestructura tecnológica de la A.N.M.A.T.

El espacio de almacenamiento de mensajes en el servicio de correo electrónico es finito, esto significa que el servicio cumple la función de recepción y envío mientras tenga espacio suficiente para tal operación, por lo cual el usuario debe gestionar a los mismos de manera adecuada.

Con el objeto de mejorar su gestión y seguridad se requiere el cumplimiento de las siguientes directivas:

a) No enviar o recibir adjuntos en los correos electrónicos de archivos binarios (programas ejecutables y librerías), scripts y macros, archivos cifrados con contraseñas (ya que evita su análisis de seguridad), archivos multimedia de audio y/o video.

b) No adjuntar archivos de más de 10 Mb, cuando se requiera adjuntar archivos de gran tamaño, se deberá utilizar herramientas de compresión para minimizar el tamaño del adjunto o utilizar los servicios de repositorio de la A.N.M.A.T. para compartir los mismos.

c) Periódicamente mover los mensajes enviados y recibidos a Carpeta Locales. Ya que se debe mantener la casilla de correo con el espacio usado por debajo de su límite para evitar inconvenientes de denegación del servicio por falta de espacio.

d) Evitar escribir el texto del “Asunto” todo en mayúsculas, ya que es posible que los sistemas antispam de los destinos cataloguen el correo como spam.

e) Comunicar a Mesa de Ayuda, aquellos correos que considere como correos “maliciosos” o catalogados como “spam” para contribuir a mejorar los sistemas antimalware y antispam.

f) Eliminar aquellos correos que considere correos “spam” o hayan sido etiquetados en la carpeta “cuarentena”.

g) Ante la duda, eliminar los correos de origen desconocido que contengan adjuntos, no abrirlos ni guardarlos localmente

h) Evitar acceder a los enlaces embebidos en los cuerpos de los correos recibidos, para no caer en correos maliciosos de ataques de phishing, en su lugar copiar el enlace y pegarlo en el navegador web para validar el dominio web al que se accede e ingresa sus credenciales.

i) Utilizar técnicas de firma digital en los casos en que se necesite garantizar autenticación, integridad y confidencialidad de la información incluida en el mensaje.

2.3.2. Firma de Correo Electrónico

Se propone a modo de ejemplo, el siguiente modelo de firma de correo electrónico, en el cual se identifica adecuadamente el emisor, ya que se indica su nombre, función, correo electrónico, domicilio, teléfono y dependencia a la cual pertenece.

Santiago Pedro Geraghty
Dirección de Informática
A.N.M.A.T.
Av. de Mayo 869 - Piso 2 - CABA
Te. 4340-0800 int. 1227
santiago.geraghty@anmat.gob.ar

2.3.3. Envío de Correos Electrónicos Masivos

Se define como el envío de correo electrónico masivo a todo mensaje que es enviado simultáneamente a más de treinta (30) casillas de correos electrónico, superado dicho umbral los correos serán bloqueados, estando tal actividad prohibida, salvo expresa autorización.

Las áreas que por razones inherentes a sus funciones necesiten realizar una comunicación masiva a todo el personal de la A.N.M.A.T. mediante el envío de un correo electrónico masivo, deberán solicitarlo a través de un pedido formal a Comunicación Interna (COMIN) de la Dirección de Asuntos Institucionales.

2.4. Uso del Almacenamiento de Información por el Usuario

2.4.1. Almacenamiento Local

Los discos locales de los equipos informáticos se destinarán al almacenamiento y procesamiento de archivos relacionados con sus actividades laborales. Siendo cada usuario responsable de administrar el espacio y resguardo seguro de la información que el equipo informático contenga.

Por lo cual se indica que para el mantenimiento de una copia de resguardo es necesario almacenar los mismos, en el servicio de almacenamiento que ofrece la A.N.M.A.T. para asegurar la existencia de una copia de resguardo en el caso que se lo requiera.

2.4.2. Almacenamiento en Repositorios de la A.N.M.A.T.

Los archivos electrónicos relacionados con las actividades laborales deberán almacenarse en los servicios de almacenamiento de los servidores de la A.N.M.A.T.. Esta información será asegurada a través de los procesos de copias de resguardo establecidos por la Dirección de Informática.

Toda información existente en los servicios de almacenamiento de los servidores de la A.N.M.A.T. que

no guarde relación laboral (por ejemplo, programas, archivos fotográficos y archivos de audio o videos personales), será auditada y podrá ser considerada información no deseada y ser pasible a ser borrada sin aviso previo con el objeto de mantener la disponibilidad del espacio.

En caso de requerir la restauración de una copia de resguardo, el usuario deberá comunicarse con Soporte tecnico para iniciar el proceso de restauración de copias de resguardo.

2.4.3. Almacenamiento en Servicios Externos a la A.N.M.A.T. de Internet

Está prohibido almacenar archivos laborales o documentos electrónicos de la A.N.M.A.T. en los servicios de almacenamiento de Internet, ya que se expone al riesgo de pérdida de la confidencialidad de los mismos.

Cuando se requiera utilizar un servicio de almacenamiento accesible desde Internet para compartir o almacenar archivos se debe utilizar el servicio de la A.N.M.A.T., el cual fue creado para tal necesidad y posee los requerimientos de seguridad necesarios, como ser múltiple factores de autenticación para asegurar su acceso y procesos de copias de seguridad periódicamente.

ANEXO 3

POLÍTICA DE RECURSOS HUMANOS

OBJETIVOS

Difundir el acuerdo de confidencialidad y de la Política de Seguridad.

Concientizar al personal de la existencia de sanciones disciplinarias o administrativas a quien incumpla la presente política de seguridad de la información.

Promocionar actividades concientización y capacitación en materia de seguridad de la información.

Establecer explícitamente los permisos de acceso a los sistemas y recursos, autorizados por los responsables de las unidades organizativas de la A.N.M.A.T.

RESPONSABILIDADES

Dirección de Recursos Humanos

• Informar a todo el personal que ingresa sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.

• Gestionar la firma del Compromiso de Confidencialidad con el personal.

• Redactar y gestionar la firma del documento de aceptación del compromiso de cumplimiento de la Política de Seguridad por el personal de la A.N.M.A.T.

• Coordinar con la DIRECCIÓN DE INFORMÁTICA las actividades de concientización y capacitación de seguridad informática.

• Intervenir, en el ámbito de su competencia, en los procesos disciplinarios que se inicien consecuencia de

incumplimientos de la presente Política de Seguridad de la Información.

• Informar a la DIRECCIÓN DE INFORMÁTICA toda contratación, desvinculación o cambio de función de los agentes de la A.N.M.A.T.

Dirección de Asuntos Jurídicos

• Colaborar en la redacción y mantenimiento del documento Compromiso de Confidencialidad a firmar por los empleados, proveedores, contratistas y/o terceros.

• Intervenir, en el ámbito de su competencia, en los procesos disciplinarios que se inicien como consecuencia de incumplimientos de la presente Política de Seguridad de la Información. Asesorar en el tratamiento de incidentes de seguridad que requieran de su intervención.

Coordinación de Sumarios

• Intervenir, en el ámbito de su competencia, en los procesos disciplinarios que se inicien como consecuencia de incumplimientos de la presente Política de Seguridad de la Información.

Unidades Organizativas de la A.N.M.A.T.

• Establecer explícitamente los niveles, perfiles o permisos para acceder a la información y sistemas para todo el personal a su cargo en el ámbito de su incumbencia respecto de los sistemas utilizados para sus labores diarias, de manera actualizada.

• Asegurar la continuidad operacional de las tareas que desarrollaba el agente ante la desvinculación o cambio de función en la unidad organizativa.

POLÍTICAS

3.1. Antes del empleo

3.1.1. Selección de recursos humanos

En lo que respecta a la selección de recursos humanos, se regirá conforme a la normativa vigente en la materia.

3.1.2. Aceptación de Términos y Condiciones de Contratación

Los nuevos empleados firmarán los documentos Acuerdo de Confidencialidad y la Política de Seguridad de la Información, por la cual el empleado declara conocer la existencia de la misma, así como aceptar el control y monitoreo del uso de los recursos tecnológicos que utilizará en el desempeño de sus tareas.

El empleado deberá comprometerse a utilizar la información solamente para el uso específico al que se ha destinado y no comunicarla, diseminarla o hacer pública sin autorización de un responsable jerárquico.

3.2. Durante el empleo

3.2.1. Responsabilidad de las titulares de las unidades organizativas

Los titulares de unidades organizativas en todos los niveles impulsarán la aplicación de la Política de Seguridad de la Información, por lo cual informarán su existencia y la obligación de cumplimiento durante el desempeño de sus funciones.

Todas las unidades establecerán para todo el personal a su cargo, de forma explícita, los perfiles o permisos de acceso a la información y sistemas de la A.N.M.A.T. utilizados en sus labores diarias, informando todo ello de forma anual a la DIRECCIÓN DE INFORMÁTICA, a través de una matriz de acceso en la cual se listarán usuarios y sistemas a los cuales se autoriza dicho acceso, o cuando surgieran cambios de los accesos autorizados.

3.2.2. Concientización y Capacitación en Seguridad de la Información

Se promoverán actividades de concientización en materia de seguridad de la información, mediante la implementación de un plan de concientización para el personal de la A.N.M.A.T.

Se impulsará la divulgación de las políticas, directrices, procedimientos de seguridad y el cumplimiento de las mismas desde la Dirección de Recursos Humanos y demás Direcciones o Unidades Organizativas.

3.2.3. Proceso Disciplinario y Sanciones por Incumplimiento

Ante la violación de lo dispuesto en la presente Política de Seguridad, serán de aplicación los procesos disciplinarios que correspondan de conformidad con la normativa vigente y atendiendo en cada caso la situación de revista y forma de contratación de cada agente.

De corresponder, las sanciones se impondrán conforme las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

Las sanciones disciplinarias o administrativas mencionadas precedentemente, serán implementadas sin perjuicio de la eventual responsabilidad civil o patrimonial, y/o en responsabilidad penal, en la que el agente pudiera incurrir producto de su accionar.

3.3. Desvinculación o Cambio de puesto de trabajo

3.3.1. Responsabilidad ante la Desvinculación o Cambio

Se establece que, ante la desvinculación o cambio de función del personal de la A.N.M.A.T., su superior inmediato es responsable que el conocimiento sea transferido apropiadamente, antes de proceder a la desafectación del empleado, como también a la devolución de los activos que le fueron otorgados al empleado para el desempeño de sus funciones en la A.N.M.A.T.

ANEXO 4

POLÍTICA DE GESTIÓN DE ACTIVOS

OBJETIVOS

Designar propietarios responsables de los activos de información. Clasificar los activos de información según su sensibilidad y criticidad. Asegurar el apropiado nivel de protección para los activos.

Gestionar adecuadamente los activos de información, incluida su destrucción segura.

RESPONSABILIDADES

DIRECCIÓN DE INFORMÁTICA

• Designar a los Propietarios de los Activos de Información.

Propietarios de los Activos de Información

•Clasificar los activos de información de acuerdo con su grado de sensibilidad y criticidad.

•Mantener actualizada la clasificación efectuada.

• Permitir o denegar el acceso al activo de información.

• Inventariar los activos de información.

• Mantener un registro sistemático de los activos de información.

• Identificar los activos de información asociados a los procesos de negocio de la Secretara.

• Elaborar procedimiento de asignación y de devolución de activos tecnológicos.

• Controlar y administrar el inventario de los activos de información.

• Asegurar que la protección de los recursos de la tecnología de información involucrados en los procesos de negocio de la A.N.M.A.T.

• Asistir en la identificación de activos de información de redes y seguridad.

• Elaborar procedimiento de clasificación de la información.

• Asistir en la identificación de activos de información involucrados en los procesos de negocio de la A.N.M.A.T.

POLÍTICAS

4.1. Responsabilidad sobre los Activos

4.1.1. Inventario de Activos

Se llevarán inventarios de activos actualizados y se designarán responsables de los mismos, ya sean activos físicos o activos de información. Se declara su constante actualización ante altas y bajas de los activos que integran el inventario y una revisión anual de los mismos.

Se identificarán los activos de información que dan soporte a los negocios de la A.N.M.A.T., registrándose la descripción, propietario, procesos involucrados, área, recursos asociados, responsable técnico y cualquier otra información que sea relevante.

4.1.2. Propietarios de Activos

Se designarán propietarios de los activos inventariados, como también responsables patrimonialmente sobre los mismos.

El propietario del activo en ningún caso es el dueño/a del activo, el dueño del activo es la A.N.M.A.T., no obstante, el propietario designado tiene una serie de responsabilidades sobre él, las cuales son el de asegurar que los activos sean inventariados, asegurar que los activos sean clasificados y protegidos adecuadamente y garantizar el manejo adecuado cuando el activo es eliminado o destruido.

Se establece que la DIRECCIÓN DE INFORMÁTICA podrá efectuar una propuesta tentativa sobre las asignaciones de propiedad de los activos de información, en base a quien crea el activo de información, quien lo procesa, o quien lo gestiona durante su ciclo de vida.

Si bien los propietarios de los activos de información delegan la implementación de los controles de seguridad y administración operativa a personal técnico idóneo, los propietarios conservan la responsabilidad sobre los mismos.

4.1.3. Devolución de Activos

Se contemplará en el procedimiento de baja de usuarios, la devolución de bienes. En dicho contexto, los/las empleados/as, contratistas y usuario/as de terceras partes devolverán los activos (equipamiento tecnológico, documentación, tarjetas de ingreso, etc.) asignados para el cumplimiento de sus actividades, tras la terminación del vínculo laboral, contrato o acuerdo con la A.N.M.A.T., conforme a la constancia de entrega de equipamiento tecnológico que fuera firmada previamente.

4.2. Política de Clasificación de la Información

4.2.1. Directrices de Clasificación de la Información

Los propietarios de los activos de información tendrán la potestad de clasificar a la misma. En aquellos casos excepcionales en que la propiedad se encuentre compartida, se definirá la clasificación entre el conjunto de propietarios, también se usará el mismo criterio para el otorgamiento de los permisos de acceso. La clasificación de la información que se asignará a los activos de información será la siguiente:

• ***Información Pública:*** toda aquella información cuya divulgación al público en general no representa riesgo alguno para la A.N.M.A.T., para el Sector Público Nacional o para terceros.

• ***Información Reservada***: toda información cuyo acceso posee un cierto nivel de restricción, el cual se encuentra determinado por el o los propietarios de la misma. Su divulgación o uso no autorizado podría ocasionar riesgos o pérdidas leves para la A.N.M.A.T., Sector Público Nacional o terceros. Esta Información puede ser conocida y utilizada por los empleados de la A.N.M.A.T. y/o algunas entidades externas debidamente autorizadas. Por ejemplo, información almacenada en la Intranet de la A.N.M.A.T. Como criterio general, se considerará reservada a toda aquella información que no sea no sea pública, confidencial o secreta.

• ***Información Confidencial***: información que sólo puede ser conocida y utilizada por un grupo reducido de empleados, que la necesiten para el cumplimiento de sus tareas y funciones y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas significativas a la A.N.M.A.T., al Sector Público Nacional o a terceros.

- Información Secreta: información de uso exclusivo y personal, por ejemplo, contraseñas.

4.2.2. Etiquetado de la Información

Los activos de información serán etiquetados de acuerdo a las directrices de clasificación indicadas en la presente política. Existiendo excepciones para aquellos activos clasificados como “información pública”.

4.3. Gestión de Soportes de Almacenamiento

4.3.1. Soportes de Almacenamiento Removibles

Se almacenan los soportes de medio extraíbles (cintas magnéticas, discos externos u otros) en un ambiente seguro y protegido, teniendo en cuenta la criticidad de la información contenida y las especificaciones de los fabricantes o proveedores del soporte de almacenamiento.

Se establece el control de los dispositivos de almacenamiento removibles, mediante el monitoreo de los archivos que se copian desde y hacia estos dispositivos.

4.3.2. Eliminación Segura de Soportes de Información

Se implementan procedimientos de borrado seguro de la información al declararse la baja el soporte de almacenamiento que lo contiene o para las operaciones de reciclado de los dispositivos de almacenamiento evitando de este modo acceder a información residual en los soportes de almacenamiento.

La eliminación segura se considera para todo elemento de soporte de información, tales como papeles, cintas magnéticas (datos, audio y video), discos magnéticos o de estado sólido, dispositivos de almacenamientos ópticos, unidades extraíbles y cualquier otra tecnología o soporte de almacenamiento de datos.

Los medios de almacenamiento, que se intentan reutilizar, pero no puedan ser recuperados serán destruidos físicamente de manera apropiada, para que la información contenida no pueda ser recuperada utilizando técnicas forenses.

ANEXO 5

POLÍTICA DE CONTROL DE ACCESOS

OBJETIVOS

Declarar la existencia de pautas y actividades de control en los accesos a la información y los sistemas de la A.N.M.A.T. Asegurar la infraestructura tecnológica de la A.N.M.A.T. en los accesos de redes privadas y públicas.

Establecer procesos para la adecuada gestión de usuarios y permisos de acceso.

Asegurar el acceso a los sistemas de información, bases de datos y servicios de información, con el objeto de impedir el acceso no autorizado.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas.

RESPONSABILIDADES

Propietarios de la Información

• Aprobar y/o solicitar la asignación de privilegios de acceso a los usuarios.

Dirección de Informática

• Establecer procedimientos para la gestión de usuarios y gestión de permisos a los sistemas.

• Controlar periódicamente la asignación de privilegios a usuarios.

• Solicitar procedimientos y/o instructivos a otras unidades organizativas para establecer pautas de cumplimiento de los distintos procesos de A.N.M.A.T.

• Monitorear el uso de las instalaciones de procesamiento de la información, el uso de los dispositivos móviles y trabajo remoto, la revisión de registros de eventos y actividades.

• Establecer controles de seguridad en los todos sistemas que acceden a Internet.

• Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

• Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.

• Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.

• Exigir el cumplimiento de las configuraciones de seguridad a la Dirección de Informática para su implementación en los sistemas de la A.N.M.A.T.

• Determinar los controles de accesos, identificación y autenticación a ser implementados.

• Establecer el control de acceso en las redes a través de la subdivisión de las mismas.

• Implementar el control de puertos, de conexión a la red y de ruteo de red a través de reglas de acceso.

• Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.

• Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

• Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.

• Efectuar un control de los registros generados por los sistemas de seguridad, de redes y comunicaciones periódicamente.

• Implementar procedimientos para la habilitar y deshabilitar los derechos de acceso a los sistemas.

• Apoyar la implementación de los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios por la Dirección de Informática.

• Ajustar todos los relojes de los sistemas de hardware y de software con el objeto de asegurar la concordancia en los registros de eventos y actividades.

• Definir e implementar el registro de eventos y actividades de usuarios, así como la depuración de los mismos.

• Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.

• Efectuar un control de los registros generados por las aplicaciones, servicios y sistemas operativos periódicamente para detectar desvíos, inconsistencias y errores.

Unidades Organizativas de la A.N.M.A.T.

• Establecer y notificar a la DIRECCIÓN DE INFORMÁTICA los niveles, perfiles o permisos de acceso a la información y a los sistemas de todo el personal a su cargo en el ámbito de su incumbencia materializado a través de una matriz de acceso.

• Solicitar nuevas solicitudes de permisos de acceso o bajas de los mismos.

Unidad de Auditoría Interna

Verificar, a través de las auditorías que correspondan:

• Que las Unidades Organizativas hayan definido la matriz de accesos.

• Que la Dirección de Informática tenga actualizado los permisos declarados por las unidades organizativas a los sistemas de la A.N.M.A.T.

• El cumplimiento de la Dirección de Informática en lo que respecta a la gestión de contraseñas.

POLÍTICA

5.1. Requerimientos para el Control de Accesos

5.1.1. Política de Control de Accesos

Se controlará el acceso a la información y a los recursos tecnológicos de la A.N.M.A.T., por lo cual se declara la:

a) Existencia de una definición explícita de perfiles de acceso o permisos individuales concedidos a los usuarios para acceder a los activos de información, formalizado a través de la matriz de accesos elaborada por cada una de las unidades organizativas.

b) Revocación de los derechos de acceso ante cambios de función o desvinculación laboral.

c) Identificación del propietario de la información o aplicación a la cual se desea acceder, identificación del usuario que solicita el acceso, identificación del usuario que autoriza e identificación del usuario que

lo concede operativamente.

d) Segregación de las funciones referidas a quien solicita, quien autoriza y quien concede operativamente el acceso.

e) Revisión periódica de los permisos de acceso concedidos.

5.2. Gestión de Acceso de Usuarios

5.2.1. Creación y Eliminación de Cuentas de usuario

Se redactarán procedimientos que permitan crear, modificar y eliminar cuentas de usuarios de los sistemas, bases de datos y servicios de información, asociados a un identificador univoco (ID de usuario) para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad a los fines de garantizar la trazabilidad de sus acciones.

Se utilizará una cuenta de usuario única asociada a una sola persona para poder determinar inequívocamente las actividades realizadas por este. Salvo excepciones por cuestiones de seguridad, según se indica en la Política de Gestión de Asignación de Permisos de Acceso con Privilegios Especiales o si la cuenta fuera una “cuenta de servicio”, la cual sí puede estar asociada y configurada en más de un sistema. La creación y uso de cuentas de usuario genéricas usada por varios individuos, será excepcional por razones exclusivamente operativas; debiéndose requerir un análisis previo y autorización por parte de la Dirección de Informática antes de su creación. Una vez finalizada la tarea que requirió su creación y uso, será eliminada.

Se eliminarán los permisos de acceso de los usuarios una vez que la DIRECCIÓN DE INFORMÁTICA haya recibido la notificación de baja o cambio de funciones, de áreas de pertenencia o desvinculación laboral o contractual con la A.N.M.A.T.

Se establecerá una revisión mensual con el objeto de:

• Inhabilitar cuentas de usuarios de los sistemas principales de gestión de usuarios (controladores de dominio) inactivas por más de treinta cinco (35) días corridos o cuentas de usuarios desvinculados de la A.N.M.A.T.

• Eliminar cuentas de usuarios inactivas treinta cinco (35) días corridos de los sistemas, base de datos y aplicaciones y servicios, cuando la eliminación de las mismas no provoque inconvenientes operativos.

• Eliminar las cuentas de usuarios redundantes o no identificables previo análisis de sus actividades.

• Las excepciones para evitar inhabilitar o eliminar cuentas de usuario, estas deberán ser formalmente comunicadas, justificadas y aprobadas por la DIRECCIÓN DE INFORMÁTICA.

El acceso a los sistemas de la A.N.M.A.T. por parte de los proveedores, contratistas y terceros estará vedado hasta tanto no hayan firmado el compromiso de confidencialidad.

5.2.2. Gestión de Roles y Permisos de Accesos

Se controlará la asignación de roles y permisos de acceso a los activos de información.

Se priorizarán la asignación de roles de usuarios a la asignación de permisos individuales.

Los propietarios de los activos de información tendrán el derecho de solicitar la asignación de roles y/o permisos de acceso para otros usuarios a la Dirección de Informática.

Se identificarán niveles de acceso de lectura, escritura o una combinación de ambos para los sistemas, bases de datos y aplicaciones.

Se priorizará el principio de asignación de mínimos privilegios, suficientes para realizar las tareas solicitadas.

5.2.3. Gestión de Permisos de Acceso con Privilegios Especiales

La asignación de permisos de acceso con privilegios especiales (administrador) se concederá solo al personal de sistemas. Los usuarios con permisos de accesos con privilegios especiales podrán poseer dos cuentas de usuario, una para sus tareas habituales y otra para realizar estrictamente actividades que requieren estos permisos con privilegios especiales.

No se deberán utilizar las cuentas de usuarios con permisos con privilegios para realizar actividades habituales como ser navegación en Internet o lectura del correo electrónico, sino que estas, sólo se utilizarán ante la necesidad de realizar tareas específicas que lo requieran, como ser tareas de instalación, reconfiguración, contingencia y/o recupero.

5.2.4. Gestión Central de Contraseñas

Se establecerán mecanismos automáticos que permitan a los usuarios cambiar las contraseñas asignadas inicialmente, la primera vez que ingresan al sistema.

Se establecerá como mínimo las siguientes características básicas de complejidad: longitud mínima de ocho (8) caracteres, compuesta por mayúsculas, minúsculas y caracteres numéricos en su conformación.

Se configurarán los sistemas principales de gestión de usuarios (controladores de dominio) de forma tal, que soliciten el recambio de la contraseña cada doce (12) meses impidiendo la reutilización de las últimas diez (10) contraseñas.

Se cambiarán las contraseñas por defecto (de usuario administrador, root o similar) de los sistemas y dispositivos luego que hubieran finalizado su instalación y configuración inicial.

Se cambiarán las contraseñas de las cuentas utilizadas por los servicios de soporte externos de la A.N.M.A.T. luego que la tarea de los mismos hubiera finalizado.

Se almacenarán en los sistemas de gestión de contraseñas las credenciales de los usuarios, se almacenarán en sobre cerrado y caja fuerte las contraseñas críticas (administrador, root o similares) según el procedimiento establecido.

Se incluirá en el compromiso de confidencialidad el mantenimiento del secreto de las contraseñas o de la información de autenticación.

5.2.5. Revisión de Permisos de Acceso

Se llevarán revisiones periódicas de accesos de los usuarios a fin de mantener un control eficiente del acceso a los datos y servicios de información.

Se solicitará regularmente la actualización de los permisos de accesos concedidos a los usuarios por las unidades organizativas (Matriz de Acceso), con el objeto de contrastar el nivel de cumplimiento de los procesos de gestión de permisos de acceso.

5.2.6. Revocación y Cambios de Permisos de Acceso

Se implementarán procedimientos formales para la de revocación y cambios de derechos de acceso de los usuarios en todos los sistemas y servicios.

Tras la desvinculación del usuario, se deshabilitarán los derechos de acceso a todos los sistemas y servicios de información utilizados por el individuo, verificando previamente que se puede seguir accediendo con otras credenciales activas al sistema o servicio referido.

Ante un cambio de función se removerán los derechos de acceso que no fueron aprobados para la nueva función, comprendiendo todos los derechos de accesos lógicos y físicos, como ser llaves, tarjetas de identificación y accesos a instalaciones de procesamiento de la información.

Se cambiarán las contraseñas de acceso privilegiadas que pudieran conocer el empleado, contratista o usuario de tercera parte, tras la finalización de su contrato o ante un cambio de función.

5.3. Responsabilidades del Usuario en el uso de las Contraseñas

5.3.1. Directivas en el Uso de las Contraseñas

Los usuarios se comprometen a mantener las contraseñas en secreto, ya que la contraseña es considerada información secreta y personal, no debiendo ser compartida, ni aún con su personal jerárquico. Cuando existiera indicio que la confidencialidad de la contraseña hubiera sido comprometida, se informará y solicitará el cambio de la misma, inmediatamente.

La composición de la contraseña no estará basada en datos que se pudiera adivinar u obtener fácilmente, mediante información relacionada con la persona, como ser nombres, números de teléfono, número de oficina, fechas de cumpleaños, etc.

El usuario no reutilizará o reciclará viejas contraseñas, como tampoco almacenará contraseñas en papel, archivos de texto, planillas de cálculo o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.

El usuario contempla para su almacenamiento el uso de gestores de contraseñas, software instalado en las estaciones de trabajo (PCs y notebooks).

5.4. Control de Acceso a Sistemas y Aplicaciones

5.4.1. Política de Restricción del Ingreso a los Sistemas e Información

Al igual que la política de control de accesos a las redes y servicios asociados se restringirá el acceso a la red interna, a los sistemas, base de datos y otros activos de información en base a la premisa “Todo

acceso a la información y recursos tecnológicos está prohibido, a menos que se permita explícitamente". Los usuarios tendrán acceso solo a los sistemas y activos de información que hubieran sido específicamente autorizados mediante la comunicación de la Matriz de Accesos la cual describirá detallada y explícitamente la asignación de roles y permisos concedidos a los usuarios para acceder a los sistemas y activos de información.

La Dirección de Informática autorizará el acceso a los sistemas, bases de datos y activos de información, mediante el pedido formal del titular de la dirección propietaria de la información a la cual se pretende acceder.

5.4.2. Directivas para Asegurar los Inicios de Sesión

El acceso a los servicios de información se realizará a través de inicios seguros de sesión. Por lo cual, el proceso de inicio seguro contempla:

a) Desplegar un aviso informativo, advirtiendo que sólo los usuarios autorizados pueden iniciar sesión en el equipo informático.

b) Evitar mostrar mensajes de ayuda que pudieran asistir al usuario durante el procedimiento de conexión, que diera indicio del dato erróneo (usuario o contraseña) ante una autenticación incorrecta. Es decir, no divulgar ningún indicio que provea asistencia a usuarios aún no autenticados.

c) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no indicará que parte de los datos fue correcta o incorrecta.

d) Firmar la "Política de Uso Aceptable de los Recursos de Tecnología de la Información" antes de acceder a los recursos tecnológicos de la A.N.M.A.T., consintiendo mediante esta firma su conocimiento y aceptación.

e) Evitar configurar el equipo informático con credenciales almacenadas que provoquen el inicio de sesión de forma automática.

f) Registrar todas las conexiones exitosas y los intentos de conexión fallidas.

g) Evitar implementaciones que transmitan las contraseñas en texto plano sobre la red de datos.

h) Implementar medidas para la protección ante ataques de fuerza bruta, como ser:

- Bloqueo de la cuenta del usuario, inmediatamente luego de cinco (5) reintentos fallidos.
- Desbloqueo automático de la cuenta luego de diez (10) minutos de haberse bloqueado.

5.4.3. Gestión de las Contraseñas

Se implementarán en las estaciones de trabajo el uso de sistemas gestores de contraseñas que garantizan la confidencialidad y eficiencia en la administración de las mismas para los usuarios finales.

En los sistemas que no fuerzan el cambio automático de la contraseña luego del primer inicio de sesión, el usuario deberá cambiar la misma de forma manual.

Se prohíbe compartir o almacenar las contraseñas en texto plano.

Las contraseñas de cuentas administrativas genéricas (administrador, root, etc.) con privilegios especiales para efectuar actividades críticas son resguardadas de manera especial y solo deben ser utilizadas ante necesidades específicas para realizar tareas de contingencia, recupero o reconfiguración que lo requieran.

Se definen las directivas para la administración de contraseñas críticas, requiriendo las mismas las siguientes características:

a) Las contraseñas críticas poseerán un nivel alto de complejidad (letras, números, mayúsculas, minúsculas y caracteres especiales) en su conformación.

b) La definición de la contraseña será efectuada como mínimo por dos personas, de tal manera que ninguna de ellas conozca la contraseña completa, siendo responsables por una parte de la misma.

c) Las partes de las contraseñas serán resguardadas físicamente en sobres cerrados por duplicado.

d) La utilización de las contraseñas críticas será formalmente registrada, documentando las causas que determinaron su uso, el usuario que hizo uso de la misma y las actividades que se realizaron con ella.

e) Las contraseñas críticas se renovarán una vez utilizadas, procediendo luego a su resguardo nuevamente.

5.4.4. Uso de programas utilitarios privilegiados

Se prohíbe el uso de programas con capacidades de evasión de los sistemas de control y seguridad. Se prohíbe la búsqueda o de evaluación de vulnerabilidades de seguridad sin el debido control y la autorización de la Dirección de Informática.

5.4.5. Control de Acceso al Código Fuente

Se restringirá y controlará el acceso al código fuente de las aplicaciones de software desarrolladas en la A.N.M.A.T. solo al personal autorizado por la DIRECCIÓN DE INFORMÁTICA, con el fin de evitar que sean introducidos cambios sin la debida autorización y control de las áreas involucradas, copias y descargas no autorizada del código fuente.

Todo programa objeto o ejecutable en producción tendrá un único programa fuente asociado que garantice su origen, es decir que existirá trazabilidad de versión entre el programa objeto y el código fuente.

Se establecerá la existencia de un implementador del sistema y/o aplicaciones, el cual será responsable de su pase a producción.

Se prohíbe el resguardo de programas fuentes en los ambientes de producción.

Se realizarán copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la A.N.M.A.T. teniendo para ello presente, la política de Copia de Resguardo y

Restauración.

ANEXO 6

POLÍTICA EN LA GESTIÓN DE LA CRIPTOGRAFÍA

OBJETIVOS

Implementar de manera adecuada y eficiente la criptografía para proteger la confidencialidad, no repudio, autenticidad e integridad de la información.

RESPONSABILIDADES

Dirección de Informática

• Implementar protocolos criptográficos actualizados.

• Instalar los certificados digitales en los sistemas de la A.N.M.A.T.

• Mantener la infraestructura tecnológica que da soporte a las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC en inglés) firmadas digitalmente durante su ciclo de vida.

• Verificar el cumplimiento en el uso de los controles criptográficos de los sistemas expuestos a internet, en los desarrollos de software, en las copias de resguardo y en otros usos de la criptografía.

• Redactar procedimientos de reguardo seguro de contraseñas administrativas

• Gestionar el ciclo de vida de claves públicas y privadas internas mediante la implementación de infraestructura de claves públicas (PKI en inglés)

POLÍTICAS

6.1. Cumplimiento de Requisitos

6.1.1. Política de Uso de Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para el resguardo de la información, con el fin de asegurar la confidencialidad. Por lo cual, se asegura la información y las comunicaciones mediante la utilización de controles criptográficos, en los siguientes casos:

• Almacenamiento de Datos, cuando el nivel de protección sea requerido.

• Cifrado de dispositivos móviles.

• Transmisión de información, dentro y fuera del ámbito de la A.N.M.A.T.

• Copias de Resguardo de la Información.

• Sitios de internet de la A.N.M.A.T., a través de certificados digitales.

Se utilizarán algoritmos de cifrado robustos, que serán validados periódicamente por la Dirección de

Informática, con el objeto de evitar el uso de algoritmos de cifrado obsoletos y deprecados o producto del avance de técnicas de descifrado.

Se gestionará el ciclo de vida de los certificados digitales de los sitios de internet de la A.N.M.A.T.

6.1.2. Firma Digital

Cuando el nivel de seguridad lo requiera se deberá asegurar la autenticidad e integridad de los documentos electrónicos, mediante firma digital.

Se promoverá la implementación de una infraestructura de clave pública (“Public Key Infrastructure” en inglés) para su uso interno.

Se protegerá la confidencialidad de las claves privadas, las cuales deberán ser resguardadas bajo el control exclusivo de su propietario.

6.1.3. Gestión de Claves Criptográficas

Se implementarán procesos seguros de administración de claves criptográficas utilizadas por parte de la A.N.M.A.T. respecto a las claves secretas (en criptografía simétrica) y las claves privadas (en criptografía asimétrica), para protegerlas contra modificación, destrucción, copia y divulgación no autorizada.

Se implementarán mecanismos y tomarán los recaudos necesarios para proteger la confidencialidad de las claves privadas.

Se redactarán procedimientos para las operaciones de almacenamiento de claves secretas y privadas, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados referidas a cuentas administrativas, renovación y actualización, reglas sobre cuándo y cómo deben cambiarse las claves. Como también generación e implementación de claves en operaciones de Copias de Resguardo y Restauración.

ANEXO 7

POLÍTICA FÍSICO AMBIENTAL

OBJETIVOS

Prevenir el acceso físico no autorizados, daños e interferencia dentro de las distintas dependencias de la A.N.M.A.T. Proteger el equipamiento de procesamiento de información de la A.N.M.A.T. mediante la ubicación 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 pudieran perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la A.N.M.A.T.

Proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

RESPONSABILIDADES

Dirección General de Administración

• Elaborar los protocolos de actuación ante incendio, ante corte de suministro eléctrico y actuación ante situaciones de robo, hurto o hechos vandálicos dentro de las instalaciones de la A.N.M.A.T.

• Elaborar procedimiento de ingreso y egreso de personas.

• Elaborar procedimiento de ingreso y egreso de equipamiento tecnológico.

• Controlar el funcionamiento de los sistemas de protección anti-incendio.

• Controlar el funcionamiento de los sistemas de climatización

• Controlar las operaciones de seguridad física y ambiental para el resguardo de los activos.

• Establecer procedimientos para la gestión de registros de huellas dactilares.

• Establecer procedimientos para la gestión de altas, modificaciones y bajas de personal externo a la A.N.M.A.T. que presta servicios en las dependencias (por ejemplo, personal de vigilancia, personal de limpieza, etc.).

• Gestionar los sistemas de seguridad electrónica (controles de accesos físicos, cámaras y sistemas de alarmas) con asistencia de la Dirección de Informática.

• Coordinar al personal de vigilancia física.

Dirección de Informática

• Controlar los sistemas de seguridad electrónica (controles de accesos físicos, cámaras y sistemas de alarmas).

• Elaborar procedimiento de aviso de dispositivos tecnológico extraviado o robado.

• Realizar tareas periódicas de mantenimiento preventivo del equipamiento de procesamiento de datos y comunicaciones para asegurar su disponibilidad e integridad permanentes.

• Implementar los sistemas de control de acceso.

• Implementar borrado seguro de la información en todo equipamiento informático dado de baja o que necesite ser reutilizado.

• Establecer las configuraciones necesarias para implementar la política de pantallas limpias en equipos desatendidos.

• Elaborar procedimiento de actuación ante incendio dentro del/los Centro/s de Cómputos.

Unidades Organizativas

• Solicitar los permisos de accesos físicos al responsable de la gestión de los sistemas de seguridad electrónica de la A.N.M.A.T. para todo el personal a su cargo.

Unidad de Auditoría Interna

• Auditar los accesos físicos otorgados.

Dirección de Recursos Humanos

• Cumplir con la política de pantallas y escritorios limpios, para la protección de la información.

POLÍTICAS

7.1. Áreas Seguras

7.1.1. Perímetro de Seguridad Física

El perímetro externo se encuentra delimitado por las entradas de Av de Mayo 869 y Rivadavia 870.

El perímetro interno está delimitado por las guardias policiales de ingreso al edificio.

7.1.2. Controles físicos de la Entrada

Cada entrada de todas las dependencias cuentan con personal policial y personal de seguridad privada que recibe gente externa al edificio y genera un ingreso que debe ser firmado por el personal interno que recibe la visita. Este ticket firmado tiene que ser entregado a la seguridad al retirarse del edificio.

7.1.3. Protección contra amenazas de origen ambiental, internas y externas

En sede central existirá seguridad física mediante tarjeta magnética en las entradas de las instalaciones y además cámara de seguridad en el piso en el cual se encontrase la sala de comunicaciones, el centro de procesamiento de datos y centro de operaciones de seguridad (SOC), con el objeto de contrarrestar cualquier amenaza interna o externo que pusiera en peligro los activos y operaciones de la A.N.M.A.T.

Se establecerán protocolos de actuación ante amenazas internas, externas (vándalos, accesos forzados, etc.) y procedimiento de actuación ante incendios.

7.1.4. Directivas de Seguridad para Áreas Críticas

Se establecerán controles adicionales para las áreas críticas, controles de acceso biométricos por niveles de acceso y control a través de seguridad física; permitiendo solo el acceso autorizado, seguimiento y control mediante cámaras de seguridad, prohibición de grabaciones de video y fotografías sin la debida autorización. Se establecerá el acompañamiento presencial por el personal de la A.N.M.A.T. durante la ejecución de trabajos por parte de terceros.

7.2. Seguridad de los equipos

7.2.1. Ubicación y Protección de Equipos

El centro de cómputos se deberá ubicar de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales y accesos no autorizados. Se deberá ubicar en un sitio con acceso restringido y dicha ubicación deberá permitir la supervisión constante a los fines de minimizar el riesgo de amenazas potenciales por robo, hurto, incendio, polvo, calor y radiaciones electromagnéticas.

Se establece que está prohibido comer, beber y fumar dentro del centro de cómputos, la sala de comunicaciones y centro de operaciones de seguridad, como también está prohibido tomar fotografías o realizar grabaciones sin la debida autorización.

7.2.2. Seguridad en el Suministro Eléctrico

Los centros de procesamientos de datos y las salas de comunicaciones estarán protegidos ante posibles fallas en el suministro de energía u otras anomalías eléctricas.

Se asegurará la continuidad del suministro de energía por medio de la existencia de equipamiento de Suministro de

Energía Interrumpible (UPS) y el uso de Generadores de Energía Eléctrica de respaldo.

Se deberá asegurarla iluminación de emergencia en caso de falla en el suministro principal de energía.

7.2.3. Seguridad en el Cableado Eléctrico y de Datos

Se protegerán las instalaciones contra descargas eléctricas dentro del edificio de acuerdo a las normativas vigentes, adoptando filtros de protección contra rayos a todas las líneas de ingreso de energía eléctrica y telecomunicaciones.

El cableado de comunicaciones que transporta datos y brinda apoyo a los servicios de información deberá estar protegido contra intercepción o daño. El cableado eléctrico y de transmisión de datos y telecomunicaciones deberá cumplir con los requisitos técnicos vigentes de la República Argentina.

Deberá existir separación de los cables de energía de los cables de comunicaciones de datos para evitar interferencias.

Se protegerá el tendido del cableado de red troncal entre los pisos, mediante la utilización de ductos y redes redundantes. Se utilizarán bandejas dedicadas, piso técnico y/o ductos embutidos en las paredes, siempre que sea posible.

7.2.4. Mantenimiento del Equipamiento Informático

Se deberán realizar tareas periódicas de mantenimiento preventivo del equipamiento de procesamiento de datos y comunicaciones para asegurar su disponibilidad e integridad permanentes, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.

7.2.5. Ingreso y Egreso de Bienes

Se registrará el ingreso y egreso de equipamiento tecnológico.

El retiro de bienes deberá efectuarse solamente mediante autorización del responsable patrimonial, director o jefe de unidad, debiéndose crear, al efecto, un registro del movimiento de egreso. El director o jefe de unidad que autoriza el movimiento del bien informará inmediatamente al responsable patrimonial dicho movimiento

Se deberán establecer procedimientos para el apropiado registro de la entrada y salida de bienes.

Se deberá establecer un documento modelo de retiro o traslado de equipamiento tecnológico conforme modelo del anexo 16.

7.2.6. Seguridad de los Equipos fuera de las Instalaciones

El uso de equipamiento informático fuera del ámbito de las dependencias de la A.N.M.A.T. deberá contar con controles de seguridad preventivos ante pérdida, robo, daño o intercepción. Los usuarios deberán respetar el cuidado de los activos siguiendo las pautas de las Políticas de Uso Aceptable de los Recursos de Tecnología de la Información.

Se deberá establecer un procedimiento que permita al poseedor del dispositivo tecnológico reportar rápidamente cualquier incidente de robo o extravío y de esta manera mitigar los riesgos a los que eventualmente estuviera expuesta la A.N.M.A.T. ante la ocurrencia de dicho incidente, mediante la revocación de las credenciales asociadas y notificación a los grupos de trabajo a los cuales potencialmente podría comprometer la información almacenada en el dispositivo móvil.

7.2.7. Reutilización o Baja de Equipamiento Informático

Se deberán aplicar operaciones de borrado seguro a todo equipamiento informático, siguiendo las directivas mencionadas en la Política de Eliminación Segura de Soportes de Información, antes de que el mismo sea normalizado para su reutilización o fuera dado de baja, previo resguardo de la información útil o licencias alojadas en dicho equipamiento.

7.2.8. Equipos Desatendidos y Pantallas Limpias

Los usuarios deberán cerrar las sesiones de las aplicaciones, sistemas y servicios de red, cuando no estén siendo utilizados y son desatendidos.

Los usuarios al ausentarse momentáneamente de su puesto de trabajo deberán cerrar las sesiones activas o en su defecto, bloquean el equipo informático para evitar el acceso indebido al mismo en su ausencia. Este cierre o bloqueo deberá realizarse aun cuando se establece el bloqueo automático de las pantallas de las estaciones de trabajo y servidores en todo equipo que se encuentre desatendido por más de cinco (5) minutos, con el objeto de evitar accesos no autorizados a los mismos.

Los usuarios deberán apagar los equipos informáticos cuando finalizan su jornada laboral, excepto cuando sea solicitado por la DIRECCIÓN DE INFORMÁTICA ante tareas de mantenimiento o instalación de actualizaciones fuera del horario laboral, para lo cual bloquean sus equipos informáticos.

7.2.9. Escritorios Limpios

Los usuarios deben proteger la información no pública que utilizan en sus tareas diarias, no exponiendo documentación en papel u otro medio de almacenamiento (pendrives, unidades removibles, cd, etc.) sobre su puesto de trabajo de manera desatendida.

Toda documentación en papel y soportes de almacenamiento con información reservada, confidencial o crítica deberá mantenerse bajo llave en los gabinetes o cajas fuertes cuando la misma no es utilizada.

Los usuarios deberán inmediatamente retirar la información sensible o confidencial, una vez que la misma es impresa.

ANEXO 8.

POLÍTICA DE SEGURIDAD EN LAS OPERACIONES

OBJETIVOS

Asegurar los procesos operacionales para el procesamiento de la información.

Proteger contra software malicioso, para asegurar que la información y las instalaciones de procesamiento de información se encuentren protegidos ante esta amenaza.

Establecer responsabilidades y procedimientos para la gestión y operación, incluyendo instrucciones operativas, procedimientos para el respaldo de información e instalación de software en producción.

Asegurar el adecuado registro de eventos referidos a la actividad de usuarios y de los sistemas. Gestionar las vulnerabilidades técnicas de manera apropiada y establecer controles de auditoría.

RESPONSABILIDADES

Dirección de Informática

• Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

• Analizar los riesgos de seguridad que pudieran afectar los procesos de negocio de la A.N.M.A.T.

• Elaborar documentación de gestión de cambios referidos a cambios en sistemas de seguridad y redes que pudieran afectar los procesos de la A.N.M.A.T., para asegurar una correcta implementación y acciones de reversión de cambios de ser necesario.

• Elaborar procedimientos para el manejo de incidentes de seguridad.

• Administrar los sistemas de seguridad de software antimalware, software de análisis de eventos de seguridad, software de evaluación de vulnerabilidades, sistemas de seguridad de borde, sistema de análisis de tráfico y otros.

• Requerir a las distintas unidades organizativas la documentación referida a procedimientos y documentación establecida en la presente política de seguridad.

• Elaborar de procedimientos operativos referidos a la gestión de altas y bajas de servidores físicos y virtuales, gestión de copias de seguridad, restauración y pruebas, procedimiento de traspaso de ambientes, de atención de proveedores, soporte técnico, normalización de dispositivos informáticos (PCs y notebooks) y otras actividades operativas.

• Elaborar documentación de gestión de cambios técnicos en los sistemas y equipamiento tecnológico que pudieran afectar los procesos de la A.N.M.A.T., para asegurar una correcta implementación y acciones de reversión de cambios de ser necesario.

• Administrar los medios técnicos necesarios para permitir la existencia de ambientes independientes con el objeto de asegurar la segregación de los distintos ambientes para los sistemas y procesos de negocio.

• Monitorear y documentar las necesidades de capacidad de los sistemas en operación y proyectar las demandas futuras, a fin de evitar que la falta de recursos ponga en riesgo la continuidad operativa a futuro.

• Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos e informes impresos y para la eliminación segura de los mismos.

• Controlar la realización de las copias de resguardo de información, así como las pruebas periódicas de restauración.

• Gestionar la correcta instalación de actualizaciones en los sistemas operativos y en el software instalado, priorizando las instalaciones de seguridad.

• Ajustar todos los relojes de los sistemas de hardware y de software con el objeto de asegurar la correcta concordancia en los registros de eventos y actividades.

• Asegurar el adecuado registro de las actividades realizadas por el personal operativo, para su posterior revisión.

• Analizar los riesgos operacionales de los procesos de negocio de la A.N.M.A.T.

• Documentar los incidentes operacionales para aprender de ellos y evitar su posible ocurrencia futura.

• Asistir en la implementación de controles de seguridad, por ejemplo, software antimalware, software de análisis de eventos de seguridad, software de evaluación de vulnerabilidades y otros.

• Colaborar con el tratamiento de los incidentes de seguridad, de acuerdo a lo requerido por la Dirección de Informática.

• Actualizar periódicamente los permisos de acceso asignados a los usuarios a los distintos sistemas en producción a través de la matriz de acceso.

• Elaborar documentación de gestión de cambios funcionales en los procesos que pudieran afectar los procesos de la A.N.M.A.T., para asegurar una correcta implementación y acciones de reversión de cambios de ser necesario.

• Efectuar validaciones desde el punto de vista funcional posterior a cambios técnicos y/o de configuración en los sistemas y procesos de la A.N.M.A.T.

Unidad de Auditoría Interna

• Definir y planificar actividades de auditoría sobre la infraestructura tecnológica de la A.N.M.A.T.

• Controlar la correcta asignación de permisos concedidos a través de la matriz de acceso a los sistemas en producción.

• Controlar la existencia de documentación actualizada relacionada con los procedimientos operacionales.

POLÍTICAS

8.1. Procedimientos y Responsabilidades Operativas

8.1.1. Procedimientos e Instructivos Operativos

Los procedimientos e instructivos operativos (por ejemplo, Instalación y Configuración de los Sistemas

virtuales y físicos, Gestión de Incidentes, Respaldo con Copias de Seguridad y Restauración, Traspaso de Ambientes, Atención de Soporte Técnico, etc.) deberán ser identificados, documentados, actualizados y puestos a disposición de todos los usuarios involucrados en dichas tareas. Se deberán establecer responsabilidades referidas a tales procesos operativos, que especifican:

a) Objetivo, Alcance y Responsabilidades de cada actividad

b) Procedimiento enumerando las actividades

c) Diagrama de Flujo

d) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.

e) Contacto de soporte a quien contactar en caso de dificultades operativas o técnicas imprevistas.

8.1.2. Gestión de Cambios

Previo a los cambios de los sistemas de la A.N.M.A.T., se deberá redactar documentación de control de cambios de los mismos, incluyendo en la misma, operaciones de reversión si fuera necesario, siendo todo cambio evaluado previamente en aspectos funcionales, técnicos y de seguridad.

Se deberá controlar que los cambios a implementar no afecten la seguridad de los procesos asociados ni de la información que administra.

Se deberá controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. Razón por la cual se deberá evaluar el posible impacto operativo de los cambios previstos y se deberá verificar su correcta implementación.

Los documentos de control de cambios deberán contemplar los siguientes puntos:

a) Identificación del proceso afectado, objetivo, alcance y responsables.

b) Trazabilidad de los cambios efectuados

c) Evaluación del posible impacto de dichos cambios.

d) Aprobación formal de los cambios propuestos por las áreas intervinientes. e) Planificación del proceso de cambio.

f) Pruebas funcionales, técnicas y de seguridad del nuevo escenario.

g) Comunicación de detalles de cambios a todas las áreas pertinentes.

8.1.3. Gestión de las Capacidades

Se monitoreará y evaluarán las necesidades de capacidad operacional actuales en los sistemas y la proyección a futuras demandas, con el objeto de garantizar que el crecimiento del consumo no ponga en riesgo las actividades operativas ante la falta de recursos.

Se establecerá la revisión, monitoreo y ajuste de los requerimientos de capacidad desde la perspectiva de la seguridad de la información mediante marcos normativos de seguridad.

8.1.4. Separación de Entornos

Se definirán mínimamente cuatro ambientes diferenciados: desarrollo, pruebas funcionales, pruebas de seguridad y producción, los cuales deberán estar separados y ser independientes, excepcionalmente podrán existir menos entornos debido a consideraciones de arquitectura o la reutilización de componentes.

Se definirán procedimientos formales para el traspaso entre estos ambientes, con el fin de reducir el riesgo de cambios no autorizados en los mismos y garantizar la producción de sistemas seguros.

Se deberá dar cumplimiento a las siguientes directivas:

a) El personal de desarrollo no tendrá acceso al ambiente productivo, oficiando solo como asesor del personal de producción cuando este lo requiera.

b) Ante extrema necesidad se deberá establecer el registro del acceso y el cambio efectuado en el servidor de producción por el personal de desarrollo en caso de urgencia.

c) Se deberá aislar el ambiente (sistema y datos) de seguridad para realizar pruebas de evaluación de vulnerabilidades o pruebas de penetración, para que en caso de comprometer o dañar el ambiente, no afecte a los restantes entornos.

d) El ambiente de producción deberá contar solamente con el software necesario para el funcionamiento del sistema al que sirve, no deberán existir en él compiladores u otros utilitarios del sistema que pudieran alterar el correcto funcionamiento del sistema productivo.

8.2. Protección contra Código Malicioso

8.2.1. Controles contra Código Malicioso

Se protegerán los sistemas tecnológicos mediante la implementación de controles para prevenir, detectar, eliminar y recuperar los sistemas afectados por código malicioso. Los sistemas de detección de código malicioso deberán estar instalados y actualizados en todas las estaciones de trabajo y servidores que conforman la infraestructura tecnológica de la A.N.M.A.T.

Se controlará toda actividad de lectura y grabación de archivos, en estaciones de trabajo y servidores, todo tráfico de carga y descarga de archivos en los servidores de conexión a Internet y el control en los correos electrónicos con archivos adjuntos o accesos sitios de Internet, con el objeto de evitar la ejecución de código que pudiera dañar o alterar el normal funcionamiento de la infraestructura tecnológica de la A.N.M.A.T.

Se ejecutarán periódicamente análisis preventivos para la detección y eliminación de código malicioso en los servidores y estaciones de trabajo.

8.3. Copias de Seguridad

8.3.1. Copia de Resguardo y Restauración

Se establecerán procedimientos para las actividades de Copia de Resguardo y Restauración, debiendo ser los mismos revisados y actualizados cuando se requiera.

Se definirá un esquema de rotulado de las copias de resguardo, que permita contar con toda la información necesaria para identificar y administrar cada una de ellas debidamente.

Se establecerá un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor y asegurando la destrucción segura de los medios desechados.

Se almacenará en una ubicación remota del origen, las copias de resguardo junto con registros exactos y completos de las mismas y procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio origen de la copia.

Se asignará a la información de resguardo, un nivel de protección física y ambiental según los requisitos del proveedor del medio de almacenamiento y las normas aplicadas en el sitio principal.

Se verificarán periódicamente la efectividad de los procedimientos de copias y restauración, asegurándose que cumplan con los requerimientos de los planes de continuidad de las actividades de la A.N.M.A.T., a los efectos de minimizar las posibles interrupciones de las actividades normales de la A.N.M.A.T. (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Se establecerá el cifrado de las Copias de Resguardo, de acuerdo a la Política de Uso de Controles Criptográficos. Se establece la siguiente periodicidad para la realización de copias de resguardo:

a) Una copia diaria incremental de toda la información almacenada desde la última copia completa en medio magnético almacenado en disco.

b) Una copia semanal completa resguarda en medio magnético almacenado en disco. c) Una copia completa mensual bajada a medio extraíble, es decir a cinta magnética.

Se establecerá período de retención en cintas magnéticas por cuatro (4) años antes de reusar el medio de almacenamiento, a partir de la fecha de entrada en vigencia de la presente política de seguridad.

Se establecerá el siguiente alcance como mínimo, para realizar copias de seguridad de los activos de información de los entornos en Producción de:

a) Las máquinas virtuales completas en ejecución dentro de los servidores físicos. b) Los servidores de base de datos.

c) Los servidores de repositorios y recursos compartidos que almacenas archivos de los usuarios.

d) Los servidores de correo electrónico.

e) Los archivos del Boletín Oficial en PDF firmados digitalmente.

8.4. Registro de Actividad y Monitoreo

8.4.1. Registro de Eventos

Se registrarán los eventos referidos a la actividad de usuarios y del sistema, eventos asociados a errores y la seguridad en los servidores accedidos.

Se almacenarán ajenos a su origen, los eventos de las estaciones de trabajo y servidores críticos, con el objeto de garantizar su integridad y disponibilidad para la detección e investigación de incidentes de seguridad. Los registros de eventos podrán almacenarse localmente en las estaciones de trabajo y servidores que sean consideradas no críticas.

8.4.2. Protección de los Registros de Información de Auditoría

Se implementarán controles para la protección de los registros de auditoría almacenados contra alteración de los mismos o su eliminación.

Se implementarán controles para evitar fallas por falta de espacio en los dispositivos de almacenamiento de los registros de auditoría.

8.4.3. Actividad de los Administradores y Operadores

Se registrará la actividad de los usuarios administradores y operadores de sistemas que administren información confidencial, reservada o secreta.

Implementarán alertas automáticas que informen actividades catalogadas sospechosas, ya sea debido a accesos u operaciones indebidas o fallos de los sistemas.

8.4.4. Sincronización de Relojes de los Sistemas

Se sincronizarán los relojes de todos los sistemas y equipos informáticos en relación a una o varias fuentes de sincronización únicas de referencia, a fin de garantizar la exactitud de los registros de auditoría.

8.5. Control en la Instalación de Software

8.5.1. Instalación de Software en Producción

Se controlará la instalación de software en sistemas operacionales en producción estableciéndose previamente autorizaciones, conformidades y pruebas.

Toda aplicación, desarrollada por la A.N.M.A.T. o por un tercero, tendrá un propietario y responsable técnico.

Se establecerá la gestión de cambios ante actualizaciones de software en producción antes que el nuevo sistema sea puesto en el ambiente productivo. Se conservará la versión previa del sistema a poner en producción, como medida de contingencia y posibilitar acciones de reversión de los cambios si fuera necesario.

Se establece la separación de roles, por lo cual el implementador de los sistemas en producción, no será el

programador o analista del desarrollo del software a implementar. Por lo cual, los desarrolladores o analistas no podrán acceder a los ambientes de producción para realizar implementaciones o modificaciones, salvo excepcionalmente, cuando fueran autorizados por la Dirección de Informática para la resolución de temas puntuales.

8.6. Gestión de Vulnerabilidades

8.6.1. Vulnerabilidades Técnicas y Remediación

Se efectuarán pruebas de evaluación de vulnerabilidades de seguridad de los sistemas, con el objeto de conocer el grado de exposición, antes de desplegarlo en producción y se adoptarán las medidas necesarias para remediar las vulnerabilidades detectadas, para todo sistema de software desarrollado en la A.N.M.A.T.

Se instalarán las actualizaciones de seguridad de forma automática de los sistemas operativos, se implementarán directrices de configuraciones seguras.

Se establecerán escaneos periódicos en busca de vulnerabilidades de seguridad sobre la infraestructura de la A.N.M.A.T.

Se elaborarán informes de evaluación de vulnerabilidades detectadas y acciones de remediación para corregir las fallas de seguridad detectadas.

8.6.2. Restricciones en la Instalación de Software

Se prohíbe la instalación de software que no sea autorizada por la Dirección de Informática, ya que la instalación no controlada de software en sistemas informáticos puede dar inicio a la introducción de vulnerabilidades, fuga de información, falta de integridad u otros incidentes de seguridad o bien a la transgresión de derechos de propiedad intelectual.

Se prohíbe la instalación y uso de cualquier tipo de aplicación y utilidades que activen licencias de manera indebida.

Se implementarán revisiones y controles para detectar y restringir el uso de aplicaciones y utilidades de software que pudieran anular o evitar los controles de seguridad o que pudieran usarse para evaluar la seguridad de la infraestructura tecnológica de la A.N.M.A.T. sin haber sido debidamente autorizadas.

8.7. Auditoría de los Sistemas en Producción

8.7.1. Controles de Auditoría de los Sistemas de Información

Se planificarán y definirán actividades de auditoría sobre los sistemas en producción para determinar los privilegios asignados formalmente mediante la Matriz de Accesos y Matriz de Responsabilidades, con el objeto de auditar permisos asignados y responsabilidades en su mantenimiento.

Se auditarán los incidentes operacionales para detectar si las soluciones aplicadas son permanentes o temporales, con el objeto de eliminar su ocurrencia.

Se auditará la efectividad de las actividades de Infraestructura referidas al mantenimiento, monitoreo y

gestión de accesos y gestión de actualizaciones.

ANEXO 9

POLÍTICA EN LA GESTIÓN DE LAS COMUNICACIONES

OBJETIVOS

Asegurar las redes de datos y telecomunicaciones, tanto internas como externas, con el objeto de garantizar su funcionamiento correcto y seguro.

Mantener un inventario detallado las redes de datos y telecomunicaciones.

Proteger la información que es intercambiada con otros organismos, entidades, proveedores y terceros

RESPONSABILIDADES

Dirección de Informática

• Mantener documentación con información actualizada relacionada a las redes de datos internas y externas.

• Implementar mecanismos de autenticación de múltiples factores.

• Implementar el uso adecuado de protocolos de cifrado en las redes de datos y telecomunicaciones

• Definir e implementar la adecuada segregación de las redes, en las redes internas de usuarios, redes virtuales de los centros de cómputos y redes de interconexión entre las dependencias, de forma tal que si una red es vulnerada no se propague indiscriminadamente.

• Asegurar que todo intercambio de información con partes externas se realice a través conexiones cifradas de extremo a extremo.

• Implementar controles para asegurar los sistemas de correos electrónico

• Inhabilitar la conexión a la infraestructura tecnológica de la A.N.M.A.T., cuando se detecte que dicha conexión represente una amenaza que pudiera vulnerar la confidencialidad, integridad y/o disponibilidad de la información o de los sistemas y recursos de la A.N.M.A.T.

• Implementar el uso adecuados de protocolos de cifrado en los servidores.

• Asistir en la implementación de segregación de redes en los centros de cómputo.

• Cumplir con los requerimientos de seguridad a aplicar en los sistemas de correo electrónico.

• Mantener el adecuado funcionamiento de los servicios secundarios de apoyo de los sistemas en producción.

• Asegurar el registro de las actividades realizadas por el personal operativo para su posterior revisión.

Dirección de Asuntos Jurídicos

• Incluir requerimientos de seguridad en los acuerdos de intercambio de información con otros organismos,

entidades, proveedores y terceros como compromisos de confidencialidad, responsabilidad de las partes para el uso, protección y custodia de la información y cumplimiento de las normativas legales entre otros.

Unidad de Auditoría Interna

• Auditar el cumplimiento de los requisitos de seguridad en el intercambio de Información con partes externas de la A.N.M.A.T.

• Auditar la documentación referida a topología de redes.

POLÍTICAS

9.1. Gestión en la Seguridad en las Redes de Datos

9.1.1. Seguridad en las Redes

Se documentará la información referida a topologías de redes internas, externas, redes de interconexión con otros organismos y enlaces de proveedores de servicios de Internet.

Se establecen las reglas de acceso sobre la premisa “Todo acceso a la información y recursos tecnológicos está prohibido, a menos que se permita explícitamente”.

Los usuarios deberán tener acceso solo a las redes respecto las cuales hubieran sido específicamente autorizados mediante la comunicación de la Matriz de Accesos, la cual deberá describir detallada y explícitamente la asignación de roles y permisos concedidos a los usuarios para acceder a determinados sistemas y activos de información.

Se monitoreará y registrarán las actividades en la red de manera preventiva, para lo cual se definirán controles que inspeccionen los paquetes de datos que circulan en la red con el objeto de detectar tráfico indebido que pueda vulnerar la seguridad de los sistemas informáticos.

Se restringirán las conexiones físicas de los puertos de los dispositivos de red, permitiéndoles conectarse únicamente a los dispositivos con direcciones físicas autorizadas.

Se limitará la navegación de Internet para evitar comprometer el rendimiento y/o estabilidad del acceso a la misma.

Se controlará que los equipos informáticos que se conecten hacia y desde Internet, sea efectuada a través de dispositivos de seguridad que inspeccionan el tráfico saliente y entrante, con el objeto de evitar que la navegación transgreda las normas establecidas en la Política de Uso Aceptable de los Recursos de Tecnología de la Información.

Se controlará el tráfico de datos interno y externo de la red informática mediante dispositivos de seguridad que controlen activamente las comunicaciones con origen y destino autorizados.

Se implementarán controles para mantener la alta disponibilidad de los servicios de red y equipamiento informático interconectado.

Las conexiones externas hacia equipos internos estarán restringidas y sujetas al cumplimiento de procesos

de aprobación, que requieren de la expresa autorización del director del área de pertenencia y de la DIRECCIÓN DE INFORMÁTICA.

Se implementarán mecanismos de múltiples factores de autenticación a las conexiones que accedan mediante redes privadas virtuales (VPN) a la infraestructura interna de la A.N.M.A.T.

Se promoverá el uso de certificados digitales para validar los extremos de la conexión. Las conexiones externas estarán cifradas por medio de algoritmos actualizados.

9.1.2. Nivel de Acuerdo de Servicios en Redes y Telecomunicaciones

Se establecerá el acuerdo de Nivel de Servicio para las redes internas con las siguientes características: disponibilidad del 99%, velocidad 100Mbps como mínimo, segregación de redes y seguridad de puertos, existencia de procedimiento para verificar conectividad y escalamiento hasta nivel 3 (especialista en redes y comunicaciones) para resolución de problemas.

9.1.3. Segregación de Redes

Se segregarán las redes de las distintas unidades organizativas para aislarlas entre sí. Se restringirá el tráfico de acuerdo a los perfiles y permisos de acceso solicitados para los usuarios declarados por los responsables de las distintas unidades organizativas de la A.N.M.A.T. a través de la matriz de accesos.

9.2. Intercambio de Información con Partes Externas

9.2.1. Controles en el Intercambio de la Información

Todo intercambio de información con entidades externas se deberá realizar a través conexiones cifradas de extremo a extremo. Se promoverá la implementación de certificados para la validación de cada uno de los dos extremos antes del intercambio de la información y de este modo asegurar la confidencialidad, integridad y la autenticidad de la información que se transmite y envía hacia redes externas; evitando la intercepción, copia no autorizada, modificación o direccionamiento incorrecto.

Todo intercambio de información de gran tamaño se deberá realizar mediante los servicios locales de almacenamiento provisto para tal fin y disponibles para todos los usuarios de la A.N.M.A.T.. Por lo cual se prohíbe el intercambio mediante el uso de cuentas particulares en repositorios de almacenamiento públicos.

9.2.2. Acuerdos para el Intercambio de Información con Partes Externas

Los intercambios de información con entidades externas, deberán realizarse mediante acuerdos entre el A.N.M.A.T. y dichas entidades, los cuales deberán definir puntos tales como responsabilidad de las partes en el uso, protección y custodia de la información, trazabilidad de los datos, cumplimiento de las normas técnicas y legales y requisitos de cifrado entre otros.

9.2.3. Seguridad del Correo Electrónico

El uso del servicio de correo electrónico laboral deberá estar sujeto a la Política de Uso Aceptable de los Recursos de Tecnología de la Información, por lo cual todo el personal de la A.N.M.A.T. deberá aceptar las pautas de uso declaradas en la utilización del mismo.

Se protegerá el sistema de correos electrónicos para evitar el acceso no autorizado, denegación de servicio, correos publicitarios no deseados, suplantación de identidad del remitente y demás amenazas existentes, mediante la implementación de sistemas antimalware y antispam, con el objeto de detectar archivos adjuntos maliciosos que pusieran en peligro a la infraestructura tecnológica de la A.N.M.A.T. a través de correos fraudulentos que intentan robar de información a través de técnicas de phishing.

Se prohíbe la recepción y envío de correos adjuntos con binarios (programas ejecutables y librerías), scripts y macros, como también “archivos comprimidos con contraseña”; ya que evita que los sistemas antimalware y antispam evalúen la sanidad de los archivos comprimido que fuera recibido o enviado.

Se incorporará la siguiente leyenda al pie del mensaje en el uso del correo electrónico laboral:

"El mensaje precedente es privado y en consecuencia confidencial y solamente para él o los destinatarios al cual está dirigido. Si ha recibido este correo electrónico por error no debe revelar, copiar, distribuir o usar su contenido. La transmisión errónea del mensaje no implica la renuncia a la confidencialidad ni a ningún otro derecho del emisor.”

9.2.4. Compromiso de Confidencialidad en el Intercambio de Información

Se deberán establecer acuerdos de confidencialidad, para la protección de la información de la A.N.M.A.T. que sea transferida a entidades externas. Dichos acuerdos deberán responder a los requerimientos de confidencialidad o no divulgación de la A.N.M.A.T., existiendo en los anexos un modelo de los mismos.

ANEXO 10

POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

OBJETIVOS

Incluir requerimientos de seguridad en todo desarrollo propio o de terceros. Controlar los cambios en la actualización de los sistemas.

Establecer un marco de desarrollo seguro a través de la implementación de ambientes independientes dentro del ciclo de desarrollo de sistemas.

Asegurar las transacciones que formen parte de los procesos de la A.N.M.A.T. Desarrollar aplicaciones seguras.

Usar responsablemente los datos de pruebas.

RESPONSABILIDADES

Dirección de Informática

- Definir los controles a ser implementados en los sistemas desarrollados internamente o por terceros.
- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.

- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para el control de cambios a los sistemas
- Evaluar la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas
- Implementar el control de código malicioso.
- Asistir en la documentación de gestión de cambios
- Definir y asignar las funciones de implementador.
- Implementar las definiciones establecidas respecto a los controles y las medidas de seguridad.
- Documentar la gestión de cambios
- Efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple requerimientos de desarrollo seguro en todas sus fases.
- Elaborar documentación de gestión de cambios.
- Elaborar procedimientos de solicitud de software de aplicación.

POLÍTICAS

10.1. Requerimientos de Seguridad de los Sistemas

10.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

La Dirección de Informática participará en las fases tempranas del ciclo de vida de desarrollo de los sistemas informáticos.

Se establecerán directivas de seguridad para el desarrollo de aplicaciones, las cuales deberán describir requerimientos básicos de seguridad.

10.1.2. Seguridad en los Servicios accedidos desde Redes Públicas

Se implementarán controles de seguridad para todos los sistemas de la A.N.M.A.T. expuestos en Internet, con el objeto de evitar errores de enrutamiento, mensajes no autorizados, alteración de los datos, divulgación de la información, duplicación de mensajes o reproducción no autorizada entre otras amenazas.

Se usarán túneles de comunicaciones cifrados con protocolos seguros, se incorporarán múltiples factores de autenticación (si el servicio lo permite) y se promoverá el uso de firma digital y de certificados digitales en los dos extremos (origen y el destino) desde todo acceso a la red interna desde redes públicas.

10.1.3. Protección de las Transacciones en los Servicios de Aplicación

Redes

Se deberán utilizar transacciones para los servicios de aplicación, con el objeto de proteger y evitar la transmisión incompleta, alteración, pérdida, divulgación y/o duplicación no autorizada de mensajes o su reproducción.

Se deberá promover el uso de certificados y/o firma digital para garantizar las comunicaciones de extremo a extremo, la validación y verificación de autenticación en toda la cadena de transmisión, el uso de canal de comunicación es cifrado para garantizar la confidencialidad de las transmisiones y la utilización de protocolos seguros.

10.2. Seguridad en Procesos de Desarrollo

10.2.1. Política de Desarrollo Seguro de Software

Se declara el compromiso de involucrar a la Dirección de Informática en el ciclo de vida de desarrollo de los sistemas de información desde el inicio del mismo con el objeto de validar la seguridad en su arquitectura.

Se deberán incorporar en el diseño y desarrollo de los nuevos sistemas de información y en todas las mejoras o actualizaciones, las directivas de seguridad para el desarrollo de aplicaciones, la que será aplicable a todo desarrollo de sistemas de información, dentro de la A.N.M.A.T., como también el realizado por terceros.

10.2.2. Control de Cambios en el Proceso de Desarrollo

Durante el ciclo de vida de desarrollo de software se deberán evaluar, validar y documentar los cambios realizados, mediante un versionado detallado con el objeto de minimizar los riesgos de modificaciones indebidas que pudieran comprometer las operaciones del entorno productivo, respetando las instancias de desarrollo, pruebas y producción.

10.2.3. Revisión luego de Cambios en Sistemas Operativos de las Plataformas

Luego de la instalación de actualizaciones de las plataformas operativas y sistemas operativos se deberán realizar revisiones funcionales para asegurarse de que no se ha generado un impacto adverso en las aplicaciones operativas y por ende en las operaciones de negocio.

10.2.4. Restricciones a los Cambios de Paquetes de Software

Se limitará la instalación de las actualizaciones de los paquetes de software, bases de datos y sistemas operativos a aquellos absolutamente necesarios, siendo prioritarias las actualizaciones de seguridad. Luego de la instalación de actualizaciones se deberán realizar revisiones funcionales para asegurarse de que no se ha generado un impacto adverso en las aplicaciones operativas y por ende en las operaciones de negocio.

10.2.5. Seguridad en la Ingeniería de Software

Se contemplarán requisitos de seguridad de identificación, autenticación, autorización, auditabilidad y trazabilidad en los diseños de software.

Se utilizarán algoritmos y funciones de criptografía actualizados y reconocidos por su fortaleza en el

desarrollo de software.

Se documentará detalladamente el código fuente.

Se establecerá una metodología para una clara codificación.

Se documentarán los procesos y componentes del sistema.

10.2.6. Seguridad en los Entornos de Desarrollo

Se establecerán entornos de desarrollo seguros, por lo cual se deberá restringir el acceso al código fuente solo al personal necesario, se realizarán copias de resguardo periódicamente del código fuente, se utilizarán entornos independientes de desarrollo y se establecerán procedimientos de pasaje de entornos.

10.2.7. Tercerización del Desarrollo de Software

Se establecerán requerimientos contractuales de calidad y seguridad según lo mencionado en la Política de Desarrollo Seguro de Software, los que deberán plasmarse en acuerdos firmados y consensuados con el proveedor del desarrollo de software.

10.2.8. Pruebas de Seguridad del Sistema

Se realizarán evaluaciones de seguridad en busca de vulnerabilidades sobre desarrollos de software nuevos y sobre las modificaciones, sobre desarrollos propios o de terceros.

Se realizarán evaluaciones de seguridad sobre la plataforma en la que está implementada el desarrollo de software. Las pruebas de seguridad se deberán realizar en un entorno independiente denominado entorno de seguridad.

10.2.9. Pruebas de Aceptación del Sistema

Se realizarán pruebas funcionales de aceptación para evaluar los requisitos funcionales y la aceptación de los mismos en los sistemas desarrollados antes de pasarlo al entorno productivo. Estas pruebas funcionales se deberán realizar en un entorno independiente denominado preproductivo.

10.2.10. Propiedad Intelectual del Desarrollo de Software

Todo algoritmo o código fuente desarrollado por la A.N.M.A.T. o por terceros es de propiedad exclusiva de la A.N.M.A.T., estando prohibida su copia parcial, total y distribución de la misma a terceros sin la debida autorización.

10.3. Datos de Prueba y Operativos

10.3.1. Protección de los Datos de Prueba

Las pruebas de los sistemas desarrollados se deberán realizar con datos “no reales”, excepcionalmente podrán realizarse con datos extraídos del ambiente productivo, mediante autorización previa de un superior jerárquico, debiendo los mismos ser despersonalizados y enmascarados antes de su uso, evitando de este modo exponer información que pueda no ser pública.

10.3.2. Cambios de Datos de Sistemas en Producción

La modificación, actualización o eliminación de los datos operativos en producción serán realizadas, solo a través de los sistemas que procesan dichos datos. Ya que una modificación por fuera de los sistemas de un dato almacenado ya sea en un archivo o base de datos podría poner en riesgo la integridad de la información.

Excepcionalmente, cuando no fuera posible la aplicación de la directiva precedente, se documentará e informará a las partes interesadas (propietario de la información responsable de la gestión técnica y responsable de los procesos a los cuales afecte la modificación manual), registrando el usuario, fecha y hora, operación, motivo de la modificación, cuentas utilizadas, solución implementada, etc.

ANEXO 11.

POLÍTICA EN RELACIÓN A LOS PROVEEDORES

OBJETIVOS

Establecer un nivel de seguridad en la prestación de servicios conforme a los requerimientos de seguridad de la A.N.M.A.T.

RESPONSABILIDADES

Coordinación de Compras, Patrimonio y Suministros y la Dirección de Asuntos Jurídicos

• Controlar la inclusión en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios, lo indicado en la Política en Relación a los Proveedores y de todas otras las normas, procedimientos y prácticas relacionadas.

Dirección de Informática

• Controlar el vencimiento de los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios de la A.N.M.A.T.

• Gestionar los requerimientos y necesidades de las contrataciones de bienes y servicios de tecnología de la A.N.M.A.T.

• Redactar documentación referida a la justificación y solicitudes de requerimientos de sistema de hardware y software a contratar.

POLÍTICAS

11.1. Seguridad en las Relación con los Proveedores

11.1.1. Política de Seguridad en la Relación con los Proveedores

Todos los proveedores deberán suscribir el acuerdo de compromiso de confidencialidad de terceros según modelo del ANEXO 15.

Los proveedores que brindan soporte remotamente no deberán acceder directamente a los dispositivos que

dan soporte, sino a través del personal técnico de la A.N.M.A.T. a los cuales guiarán operativamente, siendo éstos los que aplicarán los cambios operativamente.

Todo cambio a realizar por el proveedor sobre los servicios, sistemas e infraestructura deberá ser planificado e informado previamente al personal técnico del área de competencia, para la evaluación, cálculo del riesgo que implica dicho cambio y confirmación de ejecución por parte del personal técnico de la A.N.M.A.T.

Los proveedores que acceden físicamente a las instalaciones para dar soporte se deberán identificar, registrar sus ingresos y estar siempre acompañados por personal técnico de la A.N.M.A.T. dentro de las instalaciones de la A.N.M.A.T.

11.1.2. Seguridad en los Acuerdos con los Proveedores

Se deberán identificar e incluir los acuerdos los niveles de servicio (SLA) y acuerdo de Compromisos de Confidencialidad en todo contrato o convenio con los proveedores.

Se deberán incluir en las contrataciones, en caso de corresponder, requisitos de documentación que lo certifique como socio o distribuidor de la marca que se contrata si no fuera una contratación directa a la marca.

Se solicita en las contrataciones, en caso de corresponder, el detalle de los contactos (teléfonos, correos electrónicos y página web) de asistencia de soporte técnico y el nivel de escalamiento correspondiente.

En las contrataciones con los proveedores que proporcionen personal, se deberá consignar el compromiso de informar cualquier cambio de los mismos, con el objeto de gestionar adecuadamente los permisos de alta del personal y de revocar los permisos del personal dado de baja. Se podrá poner a disposición de los proveedores la presente Política en Relación a los Proveedores.

11.2. Administración de la Prestación de Servicios de Proveedores

11.2.1. Supervisión y Revisión de los Servicios

Dentro de cada área de competencia en la A.N.M.A.T., se deberán controlar los servicios prestados por terceras partes, comprobando que la entrega y calidad se encuentra dentro de los términos y condiciones definidas en los acuerdos. Por lo cual se deberá elaborar la pertinente acta de recepción una vez comprobada la calidad y entrega del bien o servicio.

ANEXO 12

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD

OBJETIVOS

Gestionar de manera adecuada los eventos e incidentes de seguridad de la información, de forma tal que se apliquen las acciones correctivas oportunamente.

Comunicar rápidamente las debilidades detectadas para su inmediata corrección.

RESPONSABILIDADES

Dirección de Informática

• Notificar a la máxima Autoridad de la A.N.M.A.T. o en quien esta delegue tal competencia y a la Dirección Nacional de Ciberseguridad la ocurrencia de aquellos incidentes de seguridad, que dada su relevancia se considere necesario.

• Redactar el Plan de Respuesta a Incidentes de Seguridad de la Información.

• Redactar los Procedimientos de Respuesta a Incidentes de Seguridad de la Información.

• Analizar los incidentes de seguridad reportados.

• Comunicar a la DIRECCIÓN DE INFORMÁTICA los incidentes de seguridad detectados.

• Permitir en tiempo (inmediata) y forma (con privilegios administrativos) el acceso a todos los sistemas involucrados en el incidente de seguridad.

Dirección de Recursos Humanos

• Comunicar fehacientemente los procedimientos referidos a la Gestión de Incidentes a todo el personal actual y al personal nuevo al inicio de la relación laboral.

Dirección de Asuntos Jurídicos

• Colaborar en el tratamiento de incidentes de seguridad cuando la Dirección de Informática requiera de su intervención.

Dirección de Recursos Humanos

• Reportar debilidades e incidentes de seguridad que oportunamente se detecten.

POLÍTICAS

12.1. Gestión de Incidentes de Seguridad y Mejoras

12.1.1. Procedimientos y Responsabilidades

Se establecerá un plan general de respuesta a incidentes que contemple la preparación, detección, comunicación evaluación, análisis, contención, recuperación de los sistemas afectados y aprendizaje del mismo.

Se establecerán procedimientos de respuesta a incidentes de seguridad de la información para la correcta gestión de los mismos, con el fin de garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad

Se establece que la Dirección de Informática tiene la autoridad para acceder a todo sistema, dispositivo o equipamiento tecnológico involucrado en alertas de seguridad que considere apropiado, para analizar el incidente, evitar que escale y pudiera afectar la disponibilidad, confidencialidad e integridad de la

información o de los sistemas de la A.N.M.A.T. como también para realizar actividades forenses luego que hubiera ocurrido el incidente.

12.1.2. Comunicación de Alertas o Incidentes de Seguridad

Se establece la obligatoriedad de comunicar cualquier alerta o incidente de seguridad, siguiendo el Procedimiento de Comunicación de Incidentes de Seguridad, tan pronto como estos sean detectados por el personal y/o contratistas de la A.N.M.A.T.

12.1.3. Comunicación de Debilidades de Seguridad de la Información

Todo el personal y/o contratistas deberán informar cualquier debilidad de seguridad sospechada o detectada por ellos mismos, en los sistemas o servicios de la A.N.M.A.T.

Se prohíbe que el personal y/o contratistas intenten buscar o probar dichas debilidades de seguridad detectadas o sospechadas, por medio de cualquier software de evaluación de vulnerabilidades o pruebas de penetración, tal actitud se podrá interpretar como un intento de violación a la seguridad de los sistemas de la A.N.M.A.T. y generar las sanciones correspondientes

12.1.4. Evaluación de los Eventos y Análisis de los Incidentes Seguridad de Información

Se deberá proceder a la evaluación inicial de los eventos de seguridad catalogados como incidentes y analizar su impacto y urgencia de resolución. Por lo cual se deberán establecer criterios de priorización de incidentes dependiendo del sistema, servicio, información o usuario afectado.

En el procedimiento de respuestas de incidentes de seguridad se deberán definir parámetros que permiten decidir si el evento clasifica como incidente de seguridad de la información.

12.1.5. Respuesta a los Incidentes de Seguridad

Se deberán establecer procesos de respuesta a incidentes de seguridad que incluyan actividades tales como recopilación y registro evidencias para su evaluación inicial, análisis del incidente y acciones de remediación, comunicación del estado de situación del proceso de resolución a todas las personas y áreas con un incumbencia y necesidad de saber, aprendizaje del incidente y análisis forense para profundizar su estudio y confirmar la causa.

12.1.6. Aprendizaje de los Incidentes de la Seguridad

Se documentará la resolución del incidente, con el objeto de identificar y evaluar aquellos incidentes que sean recurrentes o de alto impacto. A efectos de mejorar y agregar controles para limitar la frecuencia, daño y costo de futuros incidentes similares.

Se documentarán todas las fallas encontradas en los procedimientos descriptos u operaciones desarrolladas y los inconvenientes detectados para su resolución, como ser convocatoria de la parte técnica, obtención de credenciales, accesos a los sistemas, ausencia de registros, etc.

12.1.7. Recopilación de Evidencias

Se procederá a la adquisición de imágenes forense y preservación de la información que pudiera servir

como evidencia, ya sea para conocer la causa del incidente, implementar una medida disciplinaria interna o iniciar una acción legal, cuando el incidente lo requiera. Para lo cual se documentará como se detectó el incidente, se resguardarán los registros de los eventos asociados al incidente, como también los equipos informáticos involucrados en el mismo.

En este aspecto se deberá tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, y normativa complementaria.

ANEXO 13

POLÍTICA DE GESTIÓN DE LA CONTINUIDAD

OBJETIVOS

Responder rápidamente las posibles interrupciones de las actividades normales de la A.N.M.A.T. Proteger los procesos críticos mediante acciones de recuperación.

Establecer planes de contingencia para asegurar la efectividad de las operaciones de contingencia de la A.N.M.A.T.

Coordinar eficientemente las áreas de la A.N.M.A.T. ante situaciones que requieran acciones de recuperación de los sistemas.

RESPONSABILIDADES

DIRECCIÓN DE INFORMÁTICA

La DIRECCIÓN DE INFORMÁTICA participarán activamente en la arquitectura, definición, documentación, pruebas y actualización de los planes de contingencia, siendo responsable de:

• Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la A.N.M.A.T.

• Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la A.N.M.A.T.

• Establecer la arquitectura y requerimientos necesarios y la elaboración del Plan de Recuperación de Desastres (DRP)

• Redactar los procedimientos para llevar a cabo el plan de contingencia

• Definir de los procesos de la A.N.M.A.T. a incluir en el plan de contingencia.

• Documentar el flujo de trabajo y arquitectura de los procesos de la A.N.M.A.T. involucrados en el plan de contingencia.

• Acompañar en la redacción de los procedimientos involucrados en el plan de contingencia

• Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la A.N.M.A.T.

• Verificar la arquitectura definida en el plan de contingencia.

• Verificar la existencia de los procedimientos a implementar que incluyan las acciones contempladas en cada etapa del plan de continuidad.

• Coordinar el proceso de administración de la continuidad de las operaciones.

• Acompañar en la redacción de los procedimientos involucrados en el plan de contingencia y el plan de respuestas de desastres.

POLÍTICAS

13.1. Gestión de Continuidad de las Operaciones

13.1.1. Planificación de la Continuidad de las Operaciones

Se deberá establecer un plan de contingencia para actuar ante incidentes que produzcan la interrupción de la continuidad de las operaciones en la A.N.M.A.T., con el objeto de garantizar que los planes operativos de restauración de las operaciones sean ordenados y consistentes entre sí.

El proceso de administración de la continuidad deberá tener en cuenta:

a) Priorización de los procesos críticos de la A.N.M.A.T.

b) Identificación de las amenazas que pudieran ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, interrupción del suministro de energía eléctrica, caídas de enlaces, incendio, desastres naturales, atentados, etc.

c) Asignación de responsabilidades.

d) Establecimiento de una estructura de gestión.

e) Documentación de la estrategia de continuidad de las actividades consecuente con los objetivos y prioridades acordados.

f) Comunicación y capacitación del personal, en materia de procedimientos y procesos de emergencia acordados a través de procedimientos de recuperación.

13.1.2. Procedimientos para la Continuidad en situaciones de emergencia

Se deberán mantener los requisitos de seguridad de la información en los planes de continuidad de las operaciones que dan respuesta a situaciones de emergencia.

Se deberán establecer Procedimientos de Recuperación de Desastres para diferentes escenarios de contingencia.

Se deberá nominar al personal de respuesta ante incidentes con la responsabilidad, autoridad y la competencia en los distintos niveles, técnicos, comunicacionales y jerárquicos para ejecutar el procedimiento de recuperación de desastres.

Se deberá establecer una estructura de administración adecuada para prepararse a mitigar y responder ante un evento disruptivo, con personal técnico y la competencia necesaria.

Se deberá desarrollar un plan documentado, procedimientos de respuesta y recuperación, detallando cómo la A.N.M.A.T. administrará un evento disruptivo y mantendrá la seguridad de su información a un nivel predeterminado.

13.1.3. Verificación de los Planes de Continuidad de las Operaciones

Se deberán realizar revisiones periódicas de los planes de continuidad de las operaciones, implementado a través de la planificación anual de pruebas para evaluar la efectividad de la misma. Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate, los responsables de las áreas de Infraestructura, Procesos y de Seguridad Informática.

13.2. Redundancia

13.2.1. Redundancia en las Instalaciones de Procesamiento y Transmisión de la Información

Se deberán implementar componentes y/o arquitecturas redundantes en las instalaciones de procesamiento y transmisión de la información, a efectos de cumplir con los requisitos de disponibilidad operativa.

ANEXO 14.

POLÍTICA DE CUMPLIMIENTO NORMATIVO Y TÉCNICO

OBJETIVOS

Cumplir con las disposiciones legales, normativas y contractuales vigentes a fin de evitar sanciones administrativas por incumplimiento de responsabilidades.

Proteger los registros de la A.N.M.A.T.

Garantizar que las revisiones de cumplimiento sean realizadas correctamente de acuerdo con las políticas y procedimientos organizacionales.

RESPONSABILIDADES

Dirección de Informática

• Realizar revisiones periódicas a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

• Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

• Redactar el Compromiso de Confidencialidad para el personal y terceros.

• Proponer e implementar las medidas para la adecuada protección de todo dato, información y/o registro de la A.N.M.A.T. en los medios de almacenamiento físicos y lógicos por medio de copias de seguridad.

• Cumplir con los requerimientos de seguridad solicitados por la Dirección de Informática.

Dirección de Asuntos Jurídicos

• Intervenir, en los casos que así corresponda y en el ámbito de su competencia, en la documentación redactada por la DIRECCIÓN DE INFORMÁTICA respecto a las contrataciones pertinentes a los sistemas de información.

• Intervenir, en el ámbito de su competencia, respecto los modelos de Compromisos de Confidencialidad.

• Intervenir, en el ámbito de su competencia, en la aprobación de la presente política de seguridad de la información.

Unidad de Auditoría Interna

• Intervenir, en el ámbito de su competencia, en la presente política de seguridad de la información.

• Verificar, a través de las auditorías que correspondan, el cumplimiento de la presente política de seguridad de la información dentro de las distintas unidades organizativas.

Unidades Organizativas de la A.N.M.A.T.

• Velar por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

POLÍTICAS

14.1. Cumplimiento de Requisitos Legales

14.1.1. Identificación de la Legislación Aplicable

Todos los empleados, con la aceptación del compromiso de cumplimiento de la Política de Seguridad, aceptan conocer lo dispuesto por:

• ***Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164:*** Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal.

• ***Ética en el Ejercicio de la Función Pública. Ley 25.188:*** Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.

• ***Código de Ética de la Función Pública:*** Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.

• ***Código Penal Art. 255:*** Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario sufrirá además inhabilitación especial por doble tiempo.

• ***Ley N° 24.624. Artículo 30***: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de

la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.

• ***Ley 11.723 de Propiedad Intelectual***: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.

• ***Ley N° 25.506 de Firma Digital***: Establece que la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

• ***Ley 26.388 de Delitos Informáticos***: Reglamente que se castiga penalmente ciertas conductas cometidas a través de medios informáticos, las cuales comprenden:

- Delitos informáticos en general
- Delitos contra la integridad sexual. Pornografía infantil
- Violación de secretos y de la privacidad
- Acceso a sistema informático
- Acceso a banco de datos
- Publicación de una comunicación electrónica
- Fraude informático
- Daño informático

• **Ley 26.904 de Grooming**: Ley que incorpora al código penal el Grooming, la cual castiga penalmente, el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

• **Ley 26.326 de Protección de Datos Personales**: Principios generales relativos a la protección de datos, derechos de los titulares de datos, usuarios y responsables de archivos, registros y bancos de datos. Control y Sanciones

14.1.2. Derechos de Propiedad Intelectual

Se deberá dar cumplimiento de los requisitos legales y contractuales relacionados con la instalación y uso de software protegido por la legislación relativa a la propiedad intelectual.

La instalación de software deberá respetar la Ley de Propiedad Intelectual N° 11.723 y sus decretos asociados, como así también el tipo de licenciamiento designado por el autor del mismo.

14.1.3. Protección de los Registros de la A.N.M.A.T.

Los registros de datos se deberán proteger contra pérdida, destrucción, acceso no autorizado, publicación no autorizada, degradación del medio de almacenamiento, obsolescencia del formato o medio de almacenamiento.

Los registros de datos, correspondientes a las cuentas de correos electrónicos no se eliminarán cuando el

propietario de dicha cuenta fuera desvinculado de la A.N.M.A.T., sino que serán almacenados por el período establecido por la Política de Copia de Resguardo.

14.1.4. Protección de Datos y Privacidad de la Información Personal

A través de la presente Política de Seguridad de la Información se establece que las actividades serán objeto de control y monitoreo, respetando la protección de los datos y privacidad de la información personal, a fin de no violar el derecho a la privacidad del empleado.

Todos los empleados deberán suscribir el documento “Acuerdo de Confidencialidad” mediante el que declaran conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento, con motivo del ejercicio de sus funciones.

14.2. Revisiones de Cumplimiento de Seguridad

14.2.1. Revisión Independiente de la Seguridad de la Información

Se establece la posibilidad de revisiones independiente de Seguridad de la Información, con el objeto de evaluar de forma independiente la eficacia de la implementación de seguridad existente. Esta revisión será independiente a la Dirección de Informática y permitirá incluir oportunidades de mejora en los objetivos de control y/o cambios en el enfoque de la estrategia de seguridad existente.

Dicha revisión podrá ser realizada independientemente por la Unidad de Auditoría Interna a través de especialistas de seguridad externos a la A.N.M.A.T.

14.2.2. Cumplimiento de la Política y Procedimientos de Seguridad

Los responsables de cada unidad organizativa deberán velar por el correcto cumplimiento de las normas y procedimientos de seguridad establecidos y deberán brindar apoyo a las revisiones de cumplimiento, efectuadas por la Dirección de Informática.

La Unidad de Auditoría Interna, en el ámbito de su competencia, al igual que la Dirección de Informática, tiene la incumbencia de realizar revisiones periódicas en todas las áreas de la A.N.M.A.T. a efectos de garantizar el cumplimiento de las políticas, normas y existencia de procedimientos o instructivos de operaciones dentro del área de su incumbencia.

14.2.3. Cumplimiento Técnico

Se deberá verificar periódicamente que los sistemas de información cumplan técnicamente con lo establecido por la política, normas y procedimientos de seguridad, por lo cual se incluirá la revisión de los sistemas en producción a fin de identificar vulnerabilidades producto de configuraciones deficientes en el hardware y software hayan sido implementados. En caso de ser necesario, estas revisiones podrán contemplar la asistencia técnica especializada. El resultado de dichas evaluaciones deberá formalizarse en un informe técnico para su ulterior interpretación por parte de los especialistas de la DIRECCIÓN DE INFORMÁTICA.

La verificación del cumplimiento comprende pruebas de evaluación de vulnerabilidades y/o pruebas de penetración, cuyo objetivo es la detección de vulnerabilidades en los sistemas y la infraestructura. Las verificaciones de cumplimiento sólo serán realizadas por personas de la Dirección de Informática,

autorizadas y bajo supervisión.

DOCUMENTOS MODELOS Y GLOSARIO DE TÉRMINOS

ANEXO 15

DOCUMENTOS MODELOS

OBJETIVOS

Confidencialidad de la información, con el objeto de prevenir la divulgación no autorizada de información por parte del personal de la A.N.M.A.T., adjudicatarios, oferentes, proveedores y terceros.

Registro de la salida de equipamiento tecnológico desde las sedes edilicias de la A.N.M.A.T.

RESPONSABILIDADES

Dirección de Recursos Humanos

• Gestionar los medios necesarios para que todo el personal de la A.N.M.A.T. firme el compromiso de confidencialidad.

Agentes

• Firmar el compromiso de confidencialidad. Todos los empleados de la A.N.M.A.T., tanto se trate de funcionarios jerárquicos, administrativos, operativos y técnicos; sea cual fuere su nivel escalafonario, forma de contratación y su situación de revista en todo el ámbito de la A.N.M.A.T. tienen la responsabilidad de firmar el compromiso de confidencialidad.

Proveedores, Oferentes o Adjudicatarios y Terceros

• Firmar el compromiso de confidencialidad, a todos aquellos que accedan a información no pública o hagan uso de los recursos tecnológicos de la A.N.M.A.T.

15.1. Acuerdos de Confidencialidad

Se establece el uso de los siguientes modelos de acuerdo de compromiso de confidencialidad:

15.1.1. Modelo del Compromiso de Confidencialidad para los Empleados

Compromiso de Confidencialidad para la Seguridad de la Información del Personal de la A.N.M.A.T.

Me comprometo a guardar absoluta reserva frente a terceros respecto de toda información institucional, gubernamental o personal a la que acceda durante mi labor, que no haya sido catalogada expresamente como "información pública", así como a utilizarla exclusivamente para el ejercicio de mis funciones, evitando comunicar, diseminar o hacer pública la misma a ninguna persona o entidad, salvo autorización previa y escrita de la A.N.M.A.T.

Acepto que este compromiso subsistirá aún después de finalizada la relación laboral, hasta la publicación oficial de la información respectiva.

Asimismo, me comprometo a no revelar ni compartir, y hacer uso responsable de las contraseñas, dispositivos físicos, virtuales o cualquier otra información o modalidad de acceso (por ejemplo, tokens por software y hardware, certificados electrónicos y certificados digitales, etc.) que me fueran otorgados, comprometiéndome a mantener la confidencialidad de los mismos y a utilizarlos solo para los fines para los cuales se me ha autorizado. Acepto que toda acción que se tome con mis credenciales de acceso a los sistemas informáticos está bajo mi responsabilidad, por lo cual me comprometo a informar inmediatamente si mis credenciales de acceso fueran comprometidas.

Declaro haber sido notificado que las actividades que impliquen manejo, intercambio o procesamiento de información de la A.N.M.A.T. pueden ser objeto de control y monitoreo conforme las pautas establecidas en la Decisión Administrativa N° 641/21.

De la misma forma me comprometo a dar cumplimiento estricto a toda la normativa relacionada con el presente, en el marco de las políticas de seguridad de la información que notifique la A.N.M.A.T. y de la Decisión Administrativa N° 641/21, en particular la Ley de Ética de la Función Pública N° 25.188, el Código de Ética de la Función Pública aprobado por el Decreto N° 41/99, la Ley de Protección de los Datos Personales N° 25.326, la Ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos N° 24.766 , la Ley Marco de Regulación de Empleo Público Nacional N° 25.164 y el Convenio Colectivo de Trabajo General para la Administración Pública Nacional, homologado por el Decreto N° 214/06.

Firma: .....

Nombre y Apellido: ..... DNI: .....

Legajo/CUIL: ..... Fecha: .....

15.1.2. Modelo del Compromiso de Confidencialidad para Terceros

Compromiso de Confidencialidad para la Seguridad de la Información para OFERENTES / PROVEEDORES / ADJUDICATARIOS de la A.N.M.A.T.

Me comprometo a guardar absoluta reserva frente a terceros respecto de toda información institucional, gubernamental o personal a la que acceda como consecuencia directa o indirecta de mi calidad de OFERENTE / PROVEEDOR / ADJUDICATARIO, que no haya sido catalogada expresamente como "información pública", así como a utilizarla exclusivamente para los fines expresamente autorizados, evitando comunicar, diseminar o hacer pública la misma aninguna persona o entidad, salvo autorización previa y escrita de la A.N.M.A.T..

Acepto que este compromiso subsistirá aún después de finalizada mi calidad de OFERENTE / PROVEEDOR / ADJUDICATARIO, salvo expresa dispensa.

Asimismo, me comprometo a no revelar ni compartir, y hacer uso responsable de las contraseñas, dispositivos físicos, virtuales o cualquier otra información o modalidad de acceso (por ejemplo, tokens por software y hardware, certificados electrónicos y certificados digitales, etc.) que me fueran otorgados, comprometiéndome a mantener la confidencialidad de los mismos y a utilizarlos solo para los fines para los cuales se me ha autorizado. Acepto que toda acción que se tome con mis credenciales de acceso a los

sistemas informáticos está bajo mi responsabilidad, por lo cual me comprometo a informar inmediatamente si mis credenciales de acceso fueran comprometidas.

Declaro haber sido notificado que las actividades que impliquen manejo, intercambio o procesamiento de información de la A.N.M.A.T. pueden ser objeto de control y monitoreo conforme las pautas establecidas en la Decisión Administrativa N° 641/21.

De la misma forma me comprometo a dar cumplimiento estricto a toda la normativa relacionada con el presente, en el marco de las políticas de seguridad de la información que notifique la A.N.M.A.T. y la Decisión Administrativa N° 641/21, la Ley de Protección de los Datos Personales N° 25.326, y la Ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos N° 24.766.

Firma: .....

Nombre y Apellido: ..... DNI: ....

Empresa/Entidad: ..... Fecha: .....

15.2. Modelo de Retiro o Traslado de Equipamiento Tecnológico

Se establece el siguiente documento como modelo para el retiro o traslado de equipamiento tecnológico.

AUTORIZACIÓN PARA LA SALIDA DE EQUIPAMIENTO TECNOLÓGICO

Ciudad Autónoma de Buenos Aires, {FECHA} El que suscribe, autoriza la salida de la sede de {DIRECCION SEDE} del siguiente equipamiento tecnológico perteneciente a la A.N.M.A.T. que se detalla a continuación.

15.3. Modelo de Constancia de Entrega de Equipamiento Tecnológico

CONSTANCIA DE ENTREGA DE EQUIPAMIENTO INFORMÁTICO Estimado usuario/a:

Se deja constancia de la entrega de una notebook perteneciente al patrimonio de la A.N.M.A.T. La misma fue entregada oportunamente para ser usada estrictamente para tareas laborales, razón por la cual deberá devolverse a la DIRECCIÓN DE INFORMÁTICA una vez finalizada la relación laboral con la A.N.M.A.T.

Se recuerdan ciertas consideraciones de seguridad a contemplar, dada la información de la A.N.M.A.T. que se accesa, elabora y gestiona por medio de la notebook entregada, como ser:

- *No usar la notebook para fines lúdicos o de entretenimiento.*
- *No instalar aplicaciones o utilidades sin la autorización de la Dirección Informática.*
- *No almacenar documentación laboral solamente en la notebook, sino en los repositorios existentes dentro de nuestra infraestructura, ya que en ellos se realizan periódicamente copias de respaldo (previa conexión por VPN).*
- *Ante el robo o hurto de la notebook, se debe informar inmediatamente a Soporte Técnico y formalizarlo*

luego a través del envío de un correo electrónico a la Dirección de Informática con el objeto de cambiar las credenciales de acceso del usuario afectado.

Atentamente.

DIRECCIÓN DE INFORMÁTICA

Notificado:

Fecha:

Nombre y Apellido:

D.N.I.:

N° de Serie:

ANEXO 16

GLOSARIO DE TÉRMINOS

En la presente política de seguridad de la información se mencionan los siguientes términos:

• **Activo de 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. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

• **Amenaza**: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

• **Ataque informático**: Ciberataque.

• **Ataque de fuerza bruta**: Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta. Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, tardan mucho tiempo en encontrar la combinación correcta (hablamos en ocasiones de miles años), por esta razón, la fuerza bruta suele combinarse con un ataque de diccionario.

• **Auditabilidad**: Permite registrar y monitorizarla utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados y autorizados.

• **Backdoor**: Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores, pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos. Por otro lado, también se consideran puertas traseras a los programas que, una vez

instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante. Por lo tanto, aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat.

• **Base de datos**: una gran cantidad de información que ha sido sistematizada para su correcto almacenamiento, de forma tal que los datos que allí están contenidos puedan ser utilizados cuando se considere necesario, pudiendo ser posteriormente reordenados u organizados.

• **Ciberdelincuente**: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

• **Ciberataque**: Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

• **Código Malicioso**: Malware.

• **Confidencialidad**: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

• **Contramedida**: Control.

• **Control**: Los medios para gestionar el riesgo, incluidos políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, de gestión o jurídica. También se utiliza como sinónimo de salvaguarda o contramedida.

• **Disponibilidad**: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

• **Evaluación del riesgo**: proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o magnitud son aceptables o tolerables. Ayuda a la toma de decisiones sobre el tratamiento del riesgo.

• **Evento**: Ocurrencia o cambio detectado 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.

• **Factores de Autenticación**: son métodos aplicables al control de acceso que permiten confirmar la identidad del usuario antes de conceder el acceso solicitado. Se pueden clasificar según los tipos de atributos que puede tener una identidad, siendo estos:

- 1FA, incluye cualquier conocimiento asociado al usuario, “lo que se conoce”, las contraseñas en sí, entran en esta categoría o por ejemplo aquellas respuestas al desafío pregunta-respuesta para accesar ante el

olvido de la contraseña.
- 2FA, refiere a algo que se posee físicamente, “lo que se tiene”, por ejemplo, tarjetas coordenadas, código recibido por SMS, token físico o por software u otro mecanismo que se encuentre registrado y asociado al usuario.
- 3FA, refiere a la biometría (reconocimiento facial, reconocimiento de voz, lectura del iris, etc.), es decir, algo “que se es”. Adicionalmente se agregan los siguientes factores:
- 4FA, localización del origen del intento de acceso a través de la dirección IP, “donde esta”, para validar como un factor más la autenticidad de la conexión, por ejemplo, no debiera concederse el acceso a conexiones fuera del país si el usuario no hubiera declarado el viaje.
- 5FA, refiere a matices del comportamiento “lo que hace habitualmente” a través del aprendizaje automático (Machine Learning), aprendiendo sobre las características de comportamiento casi únicas en tiempo real que permiten verificar continuamente la identidad una vez que se haya accedido al sistema.

• **Firma electrónica**: Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

• **Incidente de Seguridad**: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

• **Integridad**: La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que, de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

• **Infraestructura crítica**: Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

• **Infraestructura de clave pública**: Una serie de procesos y tecnologías para la asociación de claves criptográficas (públicas y privadas) con la entidad a quien esas claves se emitieron.

• **Infraestructura Tecnológica**: es el conjunto de sistemas de hardware que comprende el equipamiento informático de procesamiento (computadoras personales y servidores), almacenamiento, redes y comunicaciones, seguridad y demás elementos físicos, como también los sistemas de software que permiten la gestión de los mismos y la gestión de las operaciones de negocio.

• **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, 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.

• **Información sensible**: Nombre que recibe la información privada y que debe protegerse del acceso de personas no autorizadas sin importar el soporte en el que se encuentre o transmita.

• **Malware**: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

• **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

• **Plan de Contingencia**: Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.

• **Peer to Peer (P2P):** Los sistemas P2P no se requiere una infraestructura dedicada. Los servidores dedicados y clientes no existen, ya que cada peer puede tomar el papel tanto de servidor como de cliente al mismo tiempo. Una ventaja importante de los sistemas peer-to-peer es que todos los recursos disponibles son proporcionados por los peers. Durante la distribución de un contenido, los peers aportan sus recursos para transmitir el contenido a los demás peers. Por lo tanto, cuando un nuevo peer se agrega al sistema al sistema P2P, la demanda se incrementa, pero la capacidad general del sistema también. Es un tipo de red que permite compartir archivos de forma colaborativa, sin intermediarios, entre quienes posean programas P2P, sin necesidad de servidores centralizados.

• **Phishing:** Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

• **PKI**: Ver Infraestructura de clave pública.

• **Propietarios de activos de Información**: Son los responsables de la clasificación conforme a los procedimientos establecidos, el mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias.

• **Red Privada Virtual**: Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

• **Remediación**: acto de mitigar una vulnerabilidad o una amenaza.

• **Riesgo**: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

• **Streaming**: El streaming es un tipo de tecnología multimedia que envía contenidos de vídeo y audio a su dispositivo conectado a Internet. Esto le permite acceder a contenidos (TV, películas, música, pódcast) en cualquier momento que lo desee, en un PC o un móvil.

• **Token**: Dispositivo físico (hardware) o digital (software) que permite el acceso a un recurso restringido en lugar de usar una contraseña, firma digital o dato biométrico; es decir, actúa como una llave con la que acceder a un recurso.

• **Virus**: Malware que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento.

• **VPN**: Red Privada Virtual.

• **Vulnerabilidad**: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

FUENTES DE REFERENCIA

[REF1] Glosario de términos de ciberseguridad, INCIBE (2021)

[REF2] Principios de la seguridad informática, Mila Leal Asir (2012)

[REF3] Glosario de Términos de Ciberseguridad, Anexo II, Resolución 1523/2019 Jefatura de Gabinete de Ministros de Gobierno de Modernización

[REF4] Glosario de Términos Inglés-Español, ISACA (2015) [REF5] Ley N 25.506 de Firma Digital

[REF6] Sistemas distribuidos, Francisco de Asís López Fuentes (2015)

[REF7] Guía Metodológica - Implantación de un SGSI, AGESIC (2012)

[REF8] Sitio web Glossary - National Institute of Standards and Technology (NIST) https://csrc.nist.gov/glossary

[REF9] Sitio web AVAST https://www.avast.com/es-es/c-what-is-streaming

Pablo Scagliarini
Jefe I
Dirección General de Administración
Administración Nacional de Medicamentos, Alimentos y Tecnología Médica