MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROPIEDAD DEL INSTITUTO NACIONAL PARA SORDOS INSOR

La información aquí contenida es propiedad del INSTITUTO NACIONAL PARA SORDOS INSOR, por lo tanto, no debe reproducirse, exponerse o discutirse más allá del grupo a quien va dirigida. Al recibir este documento, el destinatario acuerda no reproducir o hacer esta información disponible en ninguna forma a personas que no estén directamente relacionadas y sean responsables de la evaluación de su contenido.

TABLA DE CONTENIDO

1. OBJETIVO. 4
2. ALCANCE. 4
3. INTRODUCCION 4
4. NORMATIVIDAD 5
5. TERMINOS Y DEFINICIONES 8
6. RESPONSABILIDADES. 10
7. ASPECTOS GENERALES. 12
7.1 Organización de la Seguridad y Privacidad de la Información. 13
8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 15
8.1 Política de infraestructura de la seguridad y privacidad de la información. 15
8.2 Política de seguridad y privacidad frente al acceso por parte de Terceros. 16
8.3 Política de gestión de activos de información. 18
8.4 Política de seguridad del personal. 20
8.5 Política de Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos. 21
8.6 Política de gestión de incidentes de seguridad y privacidad. 22
8.7 Política de seguridad física y ambiental. 25
8.8 Políticas de Escritorios y Pantallas despejados, ubicación y protección de equipos de computo 34
8.9 Política de gestión de comunicaciones y operaciones 35
8.10 Política de planificación y aprobación de sistemas. 39
8.11 Política protección contra software malicioso. 40
8.12 Política administración y seguridad de los medios de almacenamiento. 43
8.13 Política de Manejo de la Información. 43
8.14 Política de intercambios de información y software 44
8.15 Política uso de correo electrónico. 45
8.16 Seguridad para el uso de elementos, servicios de red y comunicaciones. 48
8.17 Política de control de accesos. 59
8.18 Política de administración de contraseñas de usuario. 65
8.19 Política de control de acceso a la red. 67
8.20 Política de dispositivos móviles y trabajo remoto. 67

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

8.21 Política de uso de redes inalámbricas. 69

8.22 Política de desarrollo y mantenimiento de sistemas. 71

8.23 Política Controles Criptográficos. 75

8.24 Política de seguridad de los archivos del sistema. 78

8.25 Política de procesos de desarrollo y software. 80

8.26 Política de administración de la continuidad de operaciones. 84

9. PROCESO DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DEL INSTITUTO NACIONAL PARA SORDOS INSOR. 85

10. CONTINUIDAD DE LAS ACTIVIDADES Y ANÁLISIS DE LOS IMPACTOS. 86

11. PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS 89

12. CUMPLIMIENTO 90

13. REVISIONES DE LA POLÍTICA DE SEGURIDAD PRIVACIDAD Y LA COMPATIBILIDAD TÉCNICA. 93

14. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN 100

15. CONSECUENCIAS DEL INCUMPLIMIENTO 102

16. AUDITORIAS 103

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

1. OBJETIVO.

Definir las políticas de seguridad y privacidad de la información estableciendo las medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra una amplia gama de amenazas como acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental, con el fin de minimizar el daño y, cumplir con la misión y objetivos estratégicos de la Entidad.

Las políticas de seguridad de la información definidas en este documento deben ser aprobadas por el Comité de Gestión y Desempeño Institucional, serán publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas, se revisarán de forma anual y cuando ocurran cambios significativos en el Instituto.

os objetivos de seguridad de la información deben ser supervisados y estar disponibles como información documentada indiferente de su soporte, en concordancia con la cláusula 6.2 – Objetivos de la información y planificación para alcanzarlos de acuerdo con la norma ISO 27001:2022.

2. ALCANCE.

Las políticas de seguridad y privacidad de la información contenidas en este manual aplican para los sistemas de información, infraestructura e información documentada que soportan los procesos del INSTITUTO NACIONAL PARA SORDOS (“INSOR”), y es de estricto cumplimiento a todo nivel funcional y organizacional, a todos los funcionarios, contratistas, proveedores, operadores, personal temporal, practicantes, así como otras personas o terceros que en razón del cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que las Entidades de Control y demás Entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

Hace parte del alcance del presente Manual la información creada, procesada y/o utilizada por el INSOR independientemente del medio de almacenamiento (digital, manuscrita, fonética, impresa) y/o lugar en el cual se encuentre ubicada. Las políticas de seguridad y privacidad de la información aplican a toda la información creada, procesada o que, utilizada por el INSTITUTO NACIONAL PARA SORDOS, sin importar el medio, formato, presentación o lugar en el que se encuentre.

La falta de cumplimiento de las políticas de seguridad y privacidad de la información del INSOR, serán motivo para acciones disciplinarias incluyendo la terminación del contrato de trabajo, acción civil y penal. El INSTITUTO

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

NACIONAL PARA SORDOS, también llevará a cabo acciones judiciales donde lo considere apropiado a algún no-empleado que acceda o utilice algún computador, sistema de cómputo, aplicación, sistema de comunicaciones o redes del INSOR, sin autorización.

La Entidad aplica la Guía Declaración Aplicabilidad y el Modelo de Seguridad de Privacidad de la Información MSPI, para dar cumplimiento a lo concerniente a lo documentado y normado por el Ministerio de Tecnologías de la Información MINTIC.

3. INTRODUCCION.

El presente manual establece las políticas que integran el subsistema de seguridad y privacidad de la información como herramienta fundamental para garantizar la protección de los activos de información de la Entidad y el cumplimiento de su objeto de promover, desde el sector educativo, el desarrollo e implementación de política pública para la inclusión social de la población sorda.

En este documento se detallan los procedimientos, normas y controles que deben seguirse para proteger la información de la organización, tanto en formato físico como digital. Además, se establecen las responsabilidades y roles de los diferentes actores involucrados en la gestión de la seguridad de la información, en cumplimiento con el compromiso de desarrollar su gestión con un enfoque de mejoramiento continuo, garantizando la satisfacción de sus grupos de valor y la eficacia de su sistema integrado de gestión, acorde con la política operacional.

Las políticas de seguridad de la información deben ser adoptadas por los funcionarios, contratistas, practicantes, visitantes, terceros, proveedores y ciudadanía en general, que tengan alguna relación con el INSOR; estas se encuentran enfocadas al cumplimiento de la normatividad y las buenas prácticas de seguridad de la información, en búsqueda de la disminución del impacto sobre la identificación de los riesgos generados en la operación de sus activos de información, con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la misma, para propender en la continuidad de las operaciones críticas de la Entidad.

En virtud de ello, se compromete igualmente, a fortalecer el desarrollo de su capital humano, a lograr relaciones asertivas con sus partes interesadas, a optimizar y promover el uso y apropiación de sus recursos físicos, tecnológicos y financieros con el fin de afianzar la seguridad de sus activos de información.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

4. NORMATIVIDAD

La Constitución Política de Colombia: En su artículo 15 consagra que todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

Ley 1266 DE 2008 Habeas Data, la presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política.

Ley 1712 de 2014: Sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015.

Ley 1273 DE 2009, que trata sobre el delito Informático, de la protección de la información y de los datos. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado o denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

https://www.suin- juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699

Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales. https://www.sic.gov.co/preguntas-frecuentes-pdp

Decreto 1078 de 2015: En el artículo 2.2.9.1.1.3 y 2.2.17.1.6 que determinan los principios de la Política de Gobierno Digital en Seguridad de la Información.

Decreto 1083 de 2015: El artículo 2.2.22.2.1 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en línea" y "12 Seguridad Digital".

Decreto 1499 de 2017: Modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión del Desempeño Institucional.

Decreto 2106 de 2019: Por el cual se dictan normas para simplificar, suprimir o reformar trámites innecesarios. Establece que las autoridades que realicen

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

trámites por medios digitales deben implementar estrategias de seguridad digital conforme a lineamientos MinTIC.

Decreto 620 de 2020. Reglamenta servicios ciudadanos digitales, lo cual es clave en el marco del gobierno digital.

Decreto 1263 de 2022. Adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, sobre Transformación Digital Pública.

Decreto 338 de 2022, establece los lineamientos generales para la gobernanza de seguridad digital, con el cual busca aunar y dinamizar el desarrollo legal, los avances técnicos, así como los conocimientos estatales y privados para fortalecer la ciberseguridad del país.

https://www.leyex.info/documents/leyes/601be1dc32bb1a2ee789f230cc6048df.htm

Resolución 1519 del 2020, "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos**".**

https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Resolucion/30044657.

Resolución 500 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

Directiva Presidencial 02 Del 24 De febrero De 2022, "Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)"

https://www.asocapitales.co/nueva/2022/02/25/directiva-presidencial-02-del-24-de-febrerode-2022/

CONPES 3854: establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CONPES 3995: formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital.

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

ISO 27001: La cual está elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

https://www.icontec.org/eval-conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/**ISO 27002**: Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información de una organización (Objetivos de control).

ISO 27003: Esta norma es una guía de implementación del sistema de gestión de la seguridad de la información (SGSI) e información acerca del uso del PDCA y de los requerimientos de sus diferentes fases.

Además, Colombia cuenta con el ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación) cuyo objetivo es fomentar la normalización, certificación, metrología y la gestión de la calidad, también es el representante directo de la ISO en Colombia.

Dentro del gran compendio de normas que posee se tomarán en cuenta las siguientes:

NTC-5411-1: Contiene directrices sobre la gestión de la seguridad de las TIC Tecnologías de la Información y Comunicaciones, presenta los modelos y conceptos fundamentales para la comprensión básica de la seguridad de la TIC.

GTC-169: Proporciona asesoría y guía sobre la gestión de los incidentes de seguridad de la información.

Estas normas son una guía para la elaboración del manual, teniendo en cuenta que existe un número muy amplio; estas son las que se tomarán como marco para lograr una política de seguridad sólida, confiable y eficiente.

Se mencionan aquí algunas de los marcos legales que un sistema de gestión de la seguridad de la información, debidamente implementado, debe cumplir:

Lineamientos de Mintic, Modelo de Seguridad y Privacidad de la Información MSPI 2277-2025

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

DAFP, Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020.

https://www.funcionpublica.gov.co/documents/20119/767360/2025-09-11_Guia_gestion_integral_riesgo_v7.pdf/6bb23c52-643d-eaed-fcd6-b80d27408f41?version=1.0

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.

DOCUMENTO MAESTRO DE LOS LINEAMIENTOS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

Resolución 2277 del 03 de junio de 2025: con la cual se actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), contenido en el Anexo 1 de la Resolución 500 de 2021, y se derogan disposiciones anteriores que resultaban contrarias a los nuevos estándares internacionales en esta materia.

https://mintic.gov.co/portal/715/articles-403045_recurso_2.pdf

5. TERMINOS Y DEFINICIONES

Activos de Información:

Administración del riesgo: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Administrador de Programas Fuente: Funcionario designado por el responsable del Proceso de Gestión de las TIC, con la responsabilidad exclusiva de custodiar, controlar y registrar los programas fuente utilizados por el INSOR.

Autenticación: Provisión de credenciales (usuario y contraseña) para poder acceder a recursos protegidos en equipos de cómputo.

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: garantizar que todos los recursos informáticos estén protegidos contra uso no autorizado o revelaciones accidentales. La información deberá ser considerada como privada y restringida. se garantiza

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Disponibilidad: garantizar que la información crítica y la capacidad de procesamiento puedan ser resguardadas y recuperadas rápida y completamente en caso de que ocurra alguna contingencia que interrumpa la continuación de las operaciones. se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Etiquetado:

Proceso de asignar etiquetas o metadatos a los activos para clasificarlos, identificarlos, rastrearlos y gestionarlos de manera eficiente

Evaluación de riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, también se fundamenta en comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo, la probabilidad de que ocurran y su potencial impacto en la operatoria del Instituto.

Espacio de trabajo: Lugar donde se lleva a cabo actividades diarias que incluye escritorio de trabajo y equipo de cómputo.

Firewalls: son dispositivos de seguridad, que permiten filtrar contenidos y proteger las aplicaciones de accesos no autorizados o ataques de tipo hacker.

Información documentada:

Es cualquier información que la organización debe controlar y mantener, junto con el medio que la contiene, para lograr sus objetivos de gestión y cumplir con requisitos normativos. Puede ser cualquier tipo de información, como políticas, procedimientos, procesos, registros y manuales, en cualquier formato o medio (físico o digital).

Incidente de seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadores, o red de computadores, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Cuando una acción contra una persona u organización, después de un incidente de seguridad de la información, implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas legales vigentes.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

A la hora de la recopilación de las pruebas, se preservará la cadena de custodia y se utilizarán herramientas y procedimientos aceptados de análisis forenses.

Integridad y exactitud: establecer mecanismos para garantizar que toda la información que se maneje se encuentre libre de errores y/o corrupción de cualquier índole. se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Jefe Oficina Asesora de Planeación y Sistemas: Es el responsable de liderar y coordinar los procesos de planeación estratégica, operativa e institucional de la entidad.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Instituto.

Lugar seguro: Sitio físico o electrónico que protege la información de accesos no autorizados, perdida, robo, daño, fuga. Cuya recuperación es inmediata para personas autorizadas.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el Objeto de simular múltiples peticiones del mismo remitente original.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Responsable de Seguridad y privacidad de la información: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Instituto que así lo requieran.

Tecnología de la Información: Se refiere al hardware y software operados por el Instituto o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Instituto, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Tercero: Empresa con contrato temporal que presta servicios directos o indirectos, bien sea en las instalaciones del INSTITUTO NACIONAL PARA SORDOS, o en sus propias instalaciones y que emplea algunos de los recursos informáticos y de comunicaciones del INSTITUTO NACIONAL PARA SORDOS.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Usuario: Funcionarios, contratistas o terceros que hacen uso de los servicios informáticos del Instituto Nacional para Sordos-INSOR.

6. ROLES Y RESPONSABILIDADES

Todos los jefes de oficinas autoridades administrativas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de las políticas de seguridad y privacidad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

Las Políticas de Seguridad y privacidad de la Información son de aplicación obligatoria para todo el personal del INSOR, cualquiera sea su situación, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe las máximas autoridades del INSOR deben aprobar esta Política y son responsables de la autorización de sus modificaciones.

La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.

El Comité de Gestión y Desempeño Institucional de la Entidad

El Comité Institucional de Gestión y Desempeño debe tratar los temas de seguridad y privacidad de la información asegurando la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información y tomará las medidas necesarias para planear, implementar y hacer seguimiento a las actividades necesarias para adoptar el Modelo de Seguridad de la Información al interior de su entidad y las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

El Responsable de Seguridad y privacidad de la información

El responsable de seguridad y privacidad de la información u oficial de seguridad de la información tendrá a su cargo liderar y gestionar la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad.

Oficina Asesora Jurídica

Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información y al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Gestión del Talento Humano

Controlar y salvaguardar la información personal de los funcionarios de planta de la entidad, asegurando su tratamiento conforme a la normatividad vigente.

Control Interno

En el marco de su Plan Anual de Auditoría, la Oficina de Control Interno o quien haga sus veces debe incluir auditorías técnicas y de gestión de seguridad de la información.

Proceso Gestión TIC:

Identificar los activos de información, gestionar los riesgos de seguridad de la información de los activos a su cargo y asesorar a las otras dependencias en los procesos de identificación e implementación de controles de seguridad de la información de la infraestructura a su cargo.

Funcionarios y contratistas

Los funcionarios y contratistas de la entidad deben aplicar las políticas y procedimientos de seguridad de la información, actuando como propietarios o custodios de la información, garantizando la protección de los activos de información. Y Participar activamente en los programas de capacitación y sensibilización sobre seguridad de la información.

7. ASPECTOS GENERALES.

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad y privacidad de la Información, que incluyen los siguientes tópicos:

Organización de la Seguridad y privacidad de la información

Orientado a administrar la seguridad y privacidad de la información indiferente de su soporte, dentro del INSOR y establecer un marco gerencial para controlar su implementación.

Clasificación y Control de Activos

Destinado a mantener una adecuada protección de los activos del Instituto. El objetivo es asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

Seguridad del Personal

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Instituto o uso inadecuado de instalaciones.

Seguridad Física y Ambiental

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

e información del Instituto.

Gestión de las Comunicaciones y las Operaciones

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Control de Acceso

Orientado a controlar el acceso lógico a la información.

Desarrollo y Mantenimiento de los Sistemas

Orientado a garantizar la incorporación de medidas de seguridad y privacidad de la información en los Sistemas de información desde su desarrollo y/o implementación y durante su Mantenimiento.

Administración de la Continuidad de Operaciones

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad y privacidad de la información.

A fin de asegurar la implementación de las medidas de seguridad y privacidad comprendidas en esta Política, el INSOR identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política. Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales.

El Comité de Gestión y Desempeño junto al Responsable de Seguridad y Privacidad de la Información, revisará como mínimo cada año la presente Política, a efectos de mantenerla actualizada. Así mismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

7.1 ORGANIZACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El presente Manual Política de Seguridad Y privacidad de la información establece la administración de la Seguridad y privacidad de la información, como parte fundamental de los objetivos y actividades del INSOR.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad y privacidad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades del INSOR pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad y la privacidad de la Información, por lo que se establecerán las medidas adecuadas para la protección de la información y control de acceso.

Objetivo

Administrar la seguridad y privacidad de la información dentro del INSOR y Establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Institutos especializados para la obtención de asesoría en materia de seguridad y privacidad de la información.

Garantizar la aplicación de medidas de seguridad y privacidad adecuadas por parte de todos los funcionarios, contratistas, proveedores, operadores, personal temporal, practicantes, así como otras personas o terceros hacia la información del INSOR.

Alcance

Esta Política se aplica a todos los recursos del INSOR y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

El Profesional especializado de la Oficina de Planeación y Sistemas información será el responsable de impulsar la implementación de la presente Política.

El Comité de Gestión y Desempeño junto al Responsable de Seguridad y privacidad de la información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad del INSOR. El seguimiento de acuerdo con las clases de competencias propias de cada área de las actividades relativas a la seguridad y privacidad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad de operaciones, impulso de procesos de concientización,

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad y privacidad de la Información asistirá al personal del INSOR en materia de seguridad y privacidad de la información y coordinará la interacción con entidades especializadas. Así mismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información del INSOR y verificará la aplicación de las medidas de seguridad y privacidad necesarias para la protección de la misma.

El área de Control Interno será responsable de realizar revisiones Independientes sobre la vigencia y el cumplimiento de la presente Política.

El responsable de la Secretaria General cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información e información documentada, la obligatoriedad del cumplimiento de la Política de Seguridad y Privacidad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

El responsable del Oficina asesora jurídica participará en dicha tarea. A sí mismo, Notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad y Privacidad de la Información de la Entidad.

8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

POLITICA GENERAL: El INSTITUTO NACIONA PARA SORDOS, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables y atendiendo la normativa y guías establecidas para tal fin por el Ministerio de Tecnologías de la Información MINTIC.

8.1 Política de infraestructura de la seguridad y privacidad de la información.

La seguridad y privacidad de la información es una responsabilidad del INSOR y por lo tanto afecta al Ministerio de la Igualdad y la Equidad, por tal razón el comité Institucional de Desarrollo Administrativo y Control, integrado por representantes designados por el despacho de la Dirección General, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad y privacidad.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Asignación de Responsabilidades en Materia de Seguridad y privacidad de la Información.

El Comité de Gestión y Desempeño asigna las funciones relativas a la Seguridad y privacidad Informática del INSOR al Jefe del Área de Informática (en su defecto a quien él proponga y tenga las capacidades para tal tarea), en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad y privacidad de los sistemas de información de la entidad, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad y privacidad informática tratados en la presente Política.

A continuación, se detallan los procesos de seguridad y privacidad de la información, indicándose en cada caso el/los responsables/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsible
Seguridad del Personal	Proceso Gestion Talento Humano
Seguridad Física y Ambiental	Proceso Gestion Ambiental
Seguridad en las comunicaciones	Proceso Comunicación estratégica
Control de Acceso a la información (físico y digital)	Proceso Gestión de Bienes y Servicios
Seguridad en el desarrollo y mantenimiento de sistemas	Proceso Gestión TIC
Planificación de la continuidad de operaciones	Proceso Direccionamiento Estratégico

Cabe aclarar que, si bien los propietarios de la información pueden delegar la administración de sus funciones a personal designado a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad y privacidad Informática.

En cumplimiento de lo anterior la Entidad generó la guía de estratificación nivel de responsabilidad frente a la seguridad y privacidad de la información código GUGT01.

Proceso de Autorización para Instalaciones de Procesamiento de Información.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Los nuevos recursos de procesamiento de información serán autorizados por los responsables de las áreas involucradas, el Jefe de la Oficina Asesora de de Planeación y sistemas, el profesional especializado del proceso Gestión TIC, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad y privacidad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del INSOR.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad y privacidad Informática y deberá ser autorizado por el responsable del Proceso de Gestión de las TIC y por el responsable del área al que se destinen los recursos.

Asesoramiento Especializado en Materia de Seguridad y privacidad de la Información.

El Responsable de Seguridad y privacidad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en la entidad a fin de brindar ayuda en la toma de decisiones en materia de seguridad y privacidad. Éste podrá obtener asesoramiento de otras Entidades. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad y privacidad Informática el contacto con todas las Áreas del INSOR.

Cooperación entre Institutos.

En los intercambios de información de seguridad y privacidad, no se divulgará información confidencial perteneciente al INSOR a personas no autorizadas.

El intercambio de información confidencial, sólo se permite cuando se haya firmado un Acuerdo de confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad y privacidad informática cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

8.2 Política de seguridad y privacidad frente al acceso por parte de Terceros.

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de cumplir la Política de seguridad y privacidad de la información del INSOR y proteger los activos del INSOR, con el fin de que los Colaboradores cumplan con las disposiciones de este Manual frente a la información compartida por el INSOR. Esto incluye:

- Procedimientos para proteger los bienes del INSOR, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.
- Descripción de los servicios disponibles.
- Permiso para la transferencia de personal cuando sea necesario.
- Obligaciones de las partes emanadas del acuerdo y Responsabilidades legales.
- Existencia de Derechos de Propiedad Intelectual.
- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:
  - Métodos de acceso permitidos, y el control y uso de identificadores Únicos Como identificadores de usuario y contraseñas de usuarios.
  - Proceso de autorización de accesos y privilegios de usuarios.
  - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
- Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de Contingencia.
- Responsabilidades relativas a la instalación y al mantenimiento de Hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad y privacidad de la información.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad y a la privacidad.
- Relación entre proveedores y subcontratistas.

Relación con proveedores

En caso de que la Entidad o personal externo a la organización tengan acceso a los sistemas de información o a los recursos que manejan activos de información deberemos establecer de modo formal las condiciones para el uso de dichos activos y supervisar el cumplimiento de dichas condiciones, acorde con lo normado en ISO 27001:2022.

8.3 Política de Clasificación de Activos de Información

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Generalidades

La información es uno de los activos más valiosos del INSOR, por lo tanto, su adecuada identificación, clasificación y protección es esencial para garantizar la continuidad del servicio, el cumplimiento de la normativa vigente y la confianza de los ciudadanos. Este lineamiento se fundamenta en los principios del Modelo de Seguridad y Privacidad de la Información y en los estándares internacionales de gestión de seguridad, como la norma ISO/IEC 27001:2022.

La clasificación de activos permite valorar la información según su nivel de sensibilidad, criticidad y uso, facilitando la implementación de controles proporcionales que protejan su confidencialidad, integridad y disponibilidad (CID).

Objetivo

Establecer los lineamientos para la identificación, clasificación, protección y gestión de los activos de información del INSOR, permitiendo aplicar medidas de seguridad adecuadas que mitiguen riesgos asociados a la pérdida, alteración o divulgación no autorizada de la información.

Alcance

Esta política aplica a todos los activos de información creados, almacenados, procesados o transmitidos por el INSOR, independientemente del formato (físico o digital), del medio (local o en la nube), o del área responsable. Incluye información operativa, técnica, estratégica y administrativa, así como los sistemas, infraestructuras y personas involucradas en su gestión.

Responsabilidades

Oficial de Seguridad de la Información: Liderar la implementación, actualización y seguimiento de esta política. Verificar el cumplimiento de los lineamientos y validar las clasificaciones realizadas.

Propietarios de la información (dependencias responsables): Identificar y clasificar los activos bajo su control, con base en los criterios definidos. Mantener actualizada la información en el inventario de activos.

Funcionarios y contratistas: Conocer y respetar la clasificación de los activos con los que interactúan, así como las restricciones de acceso y uso asociadas, como custodios de la información aplicando y manteniendo los controles de seguridad según el nivel de clasificación del activo.

Criterios de clasificación

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Cada activo de información debe ser clasificado considerando tres propiedades fundamentales:

a) Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Se refiere a la protección frente a accesos no autorizados. Niveles:

- **Alta** (Información Pública Reservada): su divulgación puede afectar intereses públicos.
- **Media** (Información Pública Clasificada): su revelación vulnera derechos de personas o entidades.
- **Baja** (Información Pública): puede divulgarse sin restricción.
- .

b) Integridad: Propiedad de la información que busca preservar su exactitud y completitud.

Garantiza que la información sea exacta y completa. Niveles:

- **Alta**: su alteración puede generar impactos legales, económicos o reputacionales severos.
- **Media**: puede tener impacto moderado en la operación.
- **Baja**: impacto mínimo o nulo en caso de modificación.

c) Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

Refiere a la accesibilidad oportuna de la información cuando sea requerida. Niveles:

- **Alta**: su no disponibilidad genera consecuencias críticas.
- **Media**: ocasiona retrasos o impactos moderados.
- **Baja**: no afecta significativamente los procesos institucionales.

Clasificación Final del Activo

Con base en los niveles asignados a las tres propiedades anteriores, se determinará una clasificación final del activo como:

- **Alta criticidad:** al menos dos propiedades con nivel alto.
- **Media criticidad:** una propiedad con nivel alto o dos con nivel medio.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- **Baja criticidad:** todas las propiedades en nivel bajo.

Inventario y Actualización

Todos los activos deben estar registrados en la plantilla establecida para el registro generado por MINTIC, indicando su tipología, propietario, custodia, clasificación, soporte, formato, idioma, y demás atributos definidos por MINTIC.

La actualización del inventario debe realizarse cuando:

- Se incorporen nuevos activos.
- Se modifiquen procesos o responsabilidades.
- Se migren o eliminen sistemas o documentos.
- Se identifiquen errores o inconsistencias.

Etiquetado de los Activos

Todos los activos clasificados deberán estar debidamente etiquetados de acuerdo con los niveles asignados (ej. IPR-A-1), especialmente aquellos en formato físico. Si no se encuentran etiquetados, se deben tratar con el nivel de confidencialidad más alto por defecto.

Disposición Final de Activos MARIBEL

Dentro del proceso de actualización del inventario de activos de información, es necesario identificar la disposición final de los activos de la entidad, ya sea su selección, conservación o eliminación. Esta disposición se encuentra articulada con el instrumento archivístico Tablas de Retención Documental (TRD), cuya implementación es de cumplimiento obligatorio para las entidades públicas del orden nacional en Colombia, de acuerdo con lo establecido en la Ley General de Archivos (Ley 594 de 2000).

En cuanto a la disposición final, los activos que deban conservarse por su valor histórico deberán **mantenerse en su formato original** y **agruparse según las series y subseries documentales** definidas en la TRD correspondiente a cada dependencia. La **preservación a largo plazo** aplica a los documentos en cualquiera de su soporte a los cuales se debe garantizar sus características de autenticidad, integridad, inalterabilidad, fiabilidad y disponibilidad.

La eliminación de activos debe garantizar que la información no sea recuperable.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Los métodos deberán adecuarse al tipo de activo (digital o físico) y su nivel de clasificación, incluyendo:

- Borrado seguro.
- Desmagnetización.
- Destrucción física.
- Eliminación certificada.

Toda eliminación debe estar registrada y ser verificable acorde con lo establecido en el acuerdo 001 de 2024 sobre eliminación documental.

Reclasificación de los activos

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

~~Frecuentemente,~~ La información se clasificará como confidencial o critica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta acorde con los Lineamientos para el Inventario y Clasificación de Activos de Información de MINTIC.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

8.4 Política de seguridad del personal.

Generalidades

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

La seguridad y privacidad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde el proceso de **Selección, disponiendo de los Términos y condiciones de Empleo, generando Conciencia de seguridad de la información, educación y formación, informando el proceso disciplinario, las responsabilidades después de la terminación o cambio de empleo, la aplicación de acuerdos de confidencialidad o no divulgación, las responsabilidades en el trabajo remoto y generando informes de eventos de seguridad de la información**

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo. Éstas incluirán las responsabilidades generales y especificas relacionadas con la implementación y el mantenimiento de la Política de Seguridad y privacidad de la información.

La implementación de la Política de Seguridad y privacidad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por esto que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Selección

Términos y condiciones de Empleo

Conciencia de seguridad de la información, educación y formación

Proceso disciplinario

Responsabilidades después de la terminación o cambio de empleo

Acuerdos de confidencialidad o no divulgación

Trabajo remoto

Informes de eventos de seguridad de la información

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Explicitar las responsabilidades en materia de seguridad y privacidad de la información en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad y privacidad de la información, y se encuentren capacitados para respaldar la Política de Seguridad y privacidad del INSOR en el transcurso de sus tareas normales.

Establecer compromisos de confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia

Alcance

Esta Política se aplica a todo el personal de cualquiera área sea cual sea su situación o vínculo, y al personal externo que efectúe tareas dentro del ámbito del INSOR.

Responsabilidad

El Jefe de la Oficina Asesora Jurídica Oficina asesora jurídicajunto al Coordinador del Grupo Interno de Trabajo de Talento Humano incluirá las funciones relativas a la seguridad y privacidad de la información en las descripciones de responsabilidades de los funcionarios, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad y privacidad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable de Seguridad y privacidad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad y privacidad reportados.

Las máximas autoridades del INSOR serán responsables de implementar los medios y canales necesarios para que se maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, tomarán conocimiento, efectuarán el seguimiento de la investigación, controlarán la evolución e impulsarán la resolución de los incidentes relativos a la seguridad y privacidad.

El responsable de la Oficina jurídica participará en la elaboración del Acuerdo de confidencialidad a firmar por los funcionarios, contratistas y terceros que desarrollen funciones en el INSOR, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del INSOR es responsable del reporte de debilidades e incidentes de seguridad y vulnerabilidad de la privacidad que oportunamente se detecten.

Se deben establecer los controles establecidos por la norma ISO 27001:2022 para gestionar los incidentes en la seguridad de la información y aplicar los principios para gestionar incidentes en la seguridad de la información.

Acuerdo de confidencialidad.

Como parte de sus términos y condiciones iniciales de empleo, los funcionarios, cualquiera sea su situación, firmarán un Acuerdo de confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del INSOR (el "Acuerdo de confidencialidad"). La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Así mismo, mediante el Acuerdo de Acuerdo de confidencialidad el funcionario declarará Conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo.

Se desarrollará un procedimiento para la suscripción del Acuerdo de confidencialidad donde se incluirán aspectos sobre:

- Suscripción inicial del Compromiso por parte de la totalidad del personal.
- Revisión del contenido del Compromiso cada año.
- Método de resuscripción en caso de modificación del texto del Compromiso.

Capacitación del Usuario.

Formación y Capacitación en Materia de Seguridad y privacidad de la Información.

Todos los funcionarios del INSOR y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el INSOR, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del INSOR.

El responsable del Grupo interno de trabajo de Talento Humano será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Cada seis meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

El personal que ingrese al Instituto recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad y privacidad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad y privacidad de la información, que deban ser tratadas con un orden preferencial.

8.5 Política de gestión de incidentes de seguridad y privacidad.

Comunicación de Incidentes Relativos a la Seguridad o a la privacidad.

Los incidentes relativos a la seguridad o privacidad de la información serán comunicados a través de canales de gestión apropiados tan pronto como sea posible. Para estos eventos el INSOR debe contar con herramientas de gestión de Incidentes, por medio del cual se atenderá el evento al que se dará el tratamiento pertinente.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad o de la privacidad, el Responsable de Seguridad y Privacidad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Todos los funcionarios y contratistas deben conocer el procedimiento de Mesa de Ayuda GLPI código y Procedimiento Gestión PRGT01 e Incidentes seguridad de la Información código PRGT03. y deben informar de los incidentes tan pronto hayan tomado conocimiento de su ocurrencia.

Comunicación de Debilidades en Materia de Seguridad.

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad o de la privacidad de la información, son responsables de registrar y comunicar las mismas al Responsable de Seguridad y

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

privacidad Informática.

Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

- Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- Alertar inmediatamente al Responsable de Seguridad y privacidad Informática del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

Aprendiendo de los Incidentes

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad y privacidad del INSTITUTO NACIONAL PARA SORDOS INSOR y se aplicarán sanciones de acuerdo con el Código Único Disciplinario

El proceso de Gestión TIC será el encargado de recopilar y entregar a la Oficina de Control Disciplinario, las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

- Contemplar y definir todos los tipos probables de incidentes relativos seguridad, incluyendo:
- Fallas operativas
- Código malicioso.
- Intrusiones.
- Fraude informático.
- Error humano
- Catástrofes naturales.

- Comunicar los incidentes a través de canales gerenciales apropiados tan pronto como sea posible.

8.6 Política de control acceso lógico

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del INSOR. Así mismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad y privacidad.

En alineación con las medidas tecnológicas ISO 27001:2022, se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información de la Entidad para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas y se refiere a controles en:

- AREAS SEGURAS
  EQUIPAMIENTO
-

A su vez se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

El establecimiento de perímetros de seguridad, privacidad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del INSOR, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del INSOR como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del INSOR. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al INSOR, pero situado físicamente fuera del mismo, así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al INSTITUTO NACIONAL PARA SORDOS INSOR.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en almacenamientos físicos como carpetas, cajas y el mobiliario de archivol, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a instalaciones e información del INSOR.

Proteger el equipamiento de procesamiento de información crítica Del INSOR ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del INSOR.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Implementar medidas para proteger la información y la privacidad de la misma manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información INSOR: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

Responsabilidad

El Responsable de Seguridad y privacidad Informática definirá junto con el responsable del Proceso de Gestión de las TIC y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente capítulo.

El responsable del Proceso de Gestión de las TIC asistirá al Responsable de Seguridad y privacidad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones del INSOR.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal Del INSOR a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los funcionarios del INSTITUTO NACIONAL PARA SORDOS INSOR cuando lo crean conveniente.

Todo el personal Del INSOR es responsable del cumplimiento de la política de pantallas y escritorios despejados, para la protección de la información relativa al trabajo diario en las oficinas.

Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las instalaciones de procesamiento de información.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

El INSOR utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el responsable del Proceso de Gestión de las TIC con el asesoramiento del Responsable de Seguridad y privacidad Informática, de acuerdo con la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda y se aplicará el numeral 9.1.1 Política de control de acceso de la norma ISO27001:2022, así:

- Definir y documentar claramente el perímetro de seguridad.
- Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, alarmas, cerraduras, etc.
- Verificar la existencia de un área de recepción atendida por personal. El acceso a dichas áreas estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
- Extender las barreras físicas necesarias desde el piso hasta el techo, a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.
- Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

El Responsable de Seguridad y privacidad Informática llevará un registro actualizado de Los sitios protegidos, indicando:

- Identificación del Edificio y Área.
- Principales elementos a proteger.
- Medidas de protección física.

Controles de acceso físico.

Las áreas protegidas se resguardarán mediante el empleo de controles de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

acceso físico, los que serán determinados por el Responsable de Seguridad y privacidad Informática junto con el responsable del Proceso de Gestión de las TIC, a fin de permitir el acceso sólo al personal autorizado, para lo cual se aplica el PROTOCOLO CONTROL DE ACCESO PCGT01 y controles de acceso físico que tendrán, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad y privacidad del área y los procedimientos de emergencia.

- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se mantendrá un registro protegido para permitir auditar todos los accesos.

- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

- Revisar y actualizar cada 6 meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el responsable de la Unidad Organizativa de la que dependa.

- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará el área de control Interno o en su defecto quien sea propuesto por el Ccomité de Gestión y Desempeño de la Información.

Protección de oficinas, recintos, información documentada e instalaciones.

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad, seguridad y privacidad. Asimismo, se considerarán las amenazas a la seguridad y a la privacidad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegida del INSOR:

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

AREAS PROTEGIDAS
Centro de cómputo
Encerramiento de planta eléctrica y UPS
Racks de Comunicaciones (switches)
Archivo Central

Se establecen las siguientes medidas de protección para áreas protegidas:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- Establecer que los sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
- Separar las instalaciones de procesamiento de información administradas por INSOR de aquellas administradas por terceros.
- Almacenar los materiales peligrosos o combustibles en lugares seguros a una distancia prudencial de las áreas protegidas del INSOR.
- Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

Desarrollo de tareas en áreas protegidas.

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
- Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado.
- Se mantendrá un registro de todos los accesos de personas ajenas.
- Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el responsable de dicha área o el responsable del Proceso de Gestión de las TIC y el Responsable de Seguridad y privacidad Informática.
- Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

Aislamiento de las Áreas de Recepción y Distribución.

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

- Limitar el acceso a las áreas de depósito, desde el exterior de la sede del INSTITUTO NACIONAL PARA SORDOS INSOR, sólo al personal previamente identificado y autorizado.
- Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
- Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
- Registrar el material entrante al ingresar al sitio pertinente.

Ubicación y Protección del Equipamiento y Copias de Seguridad.

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
- Adoptar controles adecuados para minimizar el riesgo de amenazas

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

potenciales, por:

- Revisar

AMENAZAS POTENCIALES
Robo o hurto
Incendio
Explosivos Humo
Inundación o filtración de agua
Polvo
Vibraciones
Efectos Químicos
Interferencia en el suministro de Energía
Radiación Electromagnética
Inundación
Condiciones ambientales (humedad, temperatura)

regularmente las condiciones físicas y ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información digital y documentada . Esta revisión se realizará cada seis meses.
- Considerar así mismo el impacto de las amenazas citadas que tengan lugar en zonas próximas a la sede del INSOR.
- Gestionar respaldo externo del 100% de la información sistemas y datos.

Suministros de Energía.

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas contar una planta eléctrica de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. **Seguridad del Cableado**

El cableado estructurado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción, las interferencias o los daños.

Mantenimiento de Equipos

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Se realizará el mantenimiento de los equipos o para asegurar su disponibilidad e integridad permanente de la información. acorde con el plan de mantenimiento, procedimiento y formato establecido por la Entidad formato Plan mantenimiento servicios tecnológicos código FOGT06.

Seguridad de los equipos fuera de las instalaciones.

El uso de equipos de cómputo destinados al procesamiento de información, fuera del +ámbito del INSOR, será autorizado por el Jefe ó coordinador del mismoe. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del INSOR para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma y debe estar cubierto por la respectiva póliza de seguros.

Eliminación o reutilización segura de los equipos.

Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.

8.7 Políticas de Escritorios y Pantallas despejadas, ubicación y protección de equipos de computo

Se adopta una política de escritorios despejados para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Objetivo: Reducir los riesgos de acceso no autorizado, perdida, daño o fuga de información que pudieran originarse desde los puestos de trabajo.

Alcance: Aplica a todos los espacios de trabajo de los funcionarios, contratistas y terceros que de manera eventual o permanente presten sus servicios en el INSOR.

Se aplicarán los siguientes lineamientos:

- No deberán dejarse documentos con información clasificada o sensible en el "Escritorio" tanto físico como el Escritorio virtual (se

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

denomina "Escritorio" al espacio digital en los equipos de cómputo). Cada vez que los funcionarios se retiren del lugar de trabajo, es importante que bloqueen los equipos de cómputo para garantizar la seguridad de la información. Una forma común de hacerlo es utilizando la combinación de teclas Win + L. Esta acción activa la función de bloqueo de pantalla y requiere una contraseña para desbloquear el equipo, evitando el acceso no autorizado.

- Es recomendable utilizar cajoneras o archivadores para almacenar de forma segura la información sensible o crítica Y almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos
- Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
- Retirar inmediatamente la información sensible o confidencial, una vez impresa.
- Los puestos de trabajo deben preferiblemente ubicarse en lugares que no queden expuestos al fácil acceso de cualquier persona.
- Los equipos que queden ubicados cerca de las zonas de atención o tránsito de público, deben situarse de forma que las pantallas de trabajo no queden expuestas y puedan ser visualizadas por personas no autorizadas.
- Si los equipos de trabajo son móviles, deben necesariamente contar con medidas de protección física para evitar su robo.
- No se debe ingerir alimentos ni bebidas cerca de los equipos de cómputo, quien realice esta acción asume el riesgo y su responsabilidad de daño o perdida de información.
- Cuando aplique en los sitios donde se almacene información física o electrónica (activos de información), se debe implementar condiciones ambientales que controlen o alerten temperatura y humedad adecuadas. La supervisión de estos activos de información son los responsables de los respectivos activos de información identificados en cada área del INSOR.

Control: Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.

Política de salas y tableros limpios

En caso que se utilice un equipo de trabajo para presentaciones, si este es de uso común debe eliminarse la información presentada, sobre todo si su tratamiento debería ser de uso interno o confidencial.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Al finalizar las presentaciones que precisen de equipos de proyección, audio o computación, quienes hayan hecho uso de los mismos deben asegurarse de apagarlos por completo.

8.8. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES - Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de otros sistemas de información del INSOR, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre sí, tanto dentro del INSOR como con terceros fuera de él. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Alineados con la norma ISO 27001:2022 se requiere establecer controles de carácter técnico que deberán estar orientados a procedimientos documentados de operación, gestión de cambios, gestión de la capacidad y separación de ambientes de desarrollo.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información del INSTITUTO NACIONAL PARA SORDOS INSOR.

Responsabilidad

El Responsable de Seguridad y privacidad Informática tendrá a su cargo, entre otros:

- Identificación de los riesgos a partir de la clasificación de los activos de información, incluyendo la documentada para definir

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

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 y privacidad de la información.

- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para las aplicaciones de Gobierno Electrónico.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- Controlar los mecanismos de distribución y difusión de información dentro del Instituto.

-
- El responsable del Proceso de Gestión de las TIC tendrá a su cargo lo siguiente:

El responsable de Seguridad y privacidad Informática junto con el responsable del Proceso de Gestión de las TIC y el responsable del Oficina asesora jurídicaOficina asesora jurídicadel INSOR evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad y privacidad de la información involucrada en la gestión de los productos o servicios prestados.

PROCEDIMIENTOS POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El responsable de Seguridad y privacidad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El responsable del Proceso de Gestión de las TIC evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Los procedimientos de control de cambios contemplarán siguientes puntos:

- Identificación y registro de cambios significativos.
- Evaluación del posible impacto de dichos cambios.
- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambio.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Prueba del nuevo escenario.
- Comunicación de detalles de cambios a todas las personas pertinentes.
- Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Separación entre Instalaciones de Desarrollo e instalaciones.

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se tendrán en cuenta los siguientes controles:

- Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
- Separar las actividades de desarrollo y prueba, en entornos diferentes.
- Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
- Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
- Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
- Definir propietarios de la información para cada uno de los ambientes de Procesamiento existente.
  El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles indicados en el punto "Separación de Funciones".

Gestión de Instalaciones Externas.

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas:

- Identificar las aplicaciones sensibles o críticas que convenga retener en el INSOR.
- Obtener la aprobación de los propietarios de aplicaciones específicas.
- Identificar las implicaciones para la continuidad de operaciones del INSOR.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deberán ser acordadas entre el responsable de Seguridad y privacidad Informática, el responsable del Área de Informática y el responsable del Oficina asesora jurídica y oficina asesora jurídica del INSOR.

8.8 Política de planificación y aprobación de sistemas.

Planificación de la Capacidad.

El responsable del Proceso de Gestión de las TIC, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información del Instituto para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad y privacidad o a la continuidad de operaciones y del procesamiento, y puedan planificar una adecuada acción correctiva.

Se debe cumplir con lo descrito en el Procedimiento gestión de la Capacidad, con el objetivo de: establecer las actividades que permitan asegurar que la capacidad de los servicios de TIC y la infraestructura de TIC, que cumplen con los requisitos acordados de capacidad y rendimiento en términos de costo-beneficio y que satisfacen tanto la capacidad actual y futura y las necesidades del INSOR.

Aprobación del sistema.

El responsable del Proceso de Gestión de las TIC y el Responsable de Seguridad y privacidad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

- Verificar el impacto en el desempeño y los requerimientos de capacidad de los computadores, diligenciando el formato Hoja de Vida Equipo Computo.
- Garantizar la recuperación ante errores.
- Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Garantizar la implementación de un conjunto acordado de controles de seguridad.
- Desarrollar disposiciones relativas a la continuidad de operaciones del INSOR.
- Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
- Considerar el efecto que tiene el nuevo sistema en la seguridad global.
- Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

8.9 Política protección contra software malicioso.

Controles Contra Software Malicioso.

El Responsable de Seguridad y privacidad Informática definirá controles de detección y prevención para la protección contra software malicioso. El responsable del Proceso de Gestión de las TIC, o el personal designado por éste, implementará dichos controles.

El Responsable de Seguridad y privacidad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado por el Instituto.
- Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
- Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadores y medios informáticos, como medida de precaución y rutinaria.
- Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (Probar dichas actualizaciones en un entorno de prueba Previamente si es que constituyen cambios críticos a los sistemas).
- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del INSOR, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Concientizar al personal acerca del problema de los falsos virus (hoax) de cómo proceder frente a los mismos.

Mantenimiento. Backup y Resguardo de la Información.

El responsable del Proceso de Gestión de las TIC y el de Seguridad y privacidad Informática determinarán los requerimientos para resguardar cada software o datos en función de su criticidad. Con base a esto, se definirá y documentará un esquema de resguardo y respaldo de la información.

El responsable del Proceso de Gestión de las TIC dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Instituto.

Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de operaciones Del INSOR.

Se definirán procedimientos para el respaldo y resguardo de la información, que deberán considerar los siguientes puntos:

- Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo con lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
- Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el INSOR. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.
- Asignar a la información de resguardo (Backups) un nivel de protección física y ambiental según las normas. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

resguardo.
- Probar periódicamente los medios de resguardo.
- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Registro de Actividades del Personal Operativo.

El responsable del Proceso de Gestión de las TIC asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
- Ejecución de operaciones críticas.
- Cambios a información crítica.

Registro de Fallas.

El responsable del Proceso de Gestión de las TIC desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

- Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
- Revisión de medidas correctivas para garantizar que los controles no Fueron comprometidos, y que las medidas tomadas fueron autorizadas.
- Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

Administración de la Red: control de redes.

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Instituto, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración de los equipos servidores, incluyendo los equipos en las áreas usuarias.
- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de internet, y para proteger los sistemas, conectados, implementar

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

controles esp.

- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
- El responsable del Proceso de Gestión de las TIC implementara dichos controles.

8.10 Política administración y seguridad de los medios de almacenamiento.

Administración de Medios Informáticos Removibles.

El responsable del Proceso de Gestión de las TIC, con la asistencia del Responsable de Seguridad y privacidad Informática, implementará procedimientos para la administración de medios informáticos removibles (USB, discos externos, cintas etc.).

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el INSOR.
- Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Eliminación de Medios de Información.

El responsable del Proceso de Gestión de las TIC, junto con el Responsable de Seguridad y privacidad Informática definirán procedimientos para la eliminación segura de los medios de información.

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

- Documentos bs magnéticas.
- Memorias USB, Discos externos y fijos.
- Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
- Datos de prueba.
- Documentación del sistema.

8.11 Política de Manejo de la Información.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo con la clasificación establecida en la Clasificación y Control de Activos.

En los procedimientos se contemplarán las siguientes acciones:

- Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, comunicaciones de voz en general, multimedia y cualquier otro ítem potencialmente sensible.
- Restringir el acceso solo al personal debidamente autorizado.
- Mantener un registro formal de los receptores autorizados de datos.
- Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.
- Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

Seguridad de la documentación del sistema.

La documentación del sistema puede contener información sensible, por lo que se consideran los siguientes puntos para su protección:

- Almacenar la documentación del sistema en forma segura.
- Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

8.12 Política de intercambios de información y software

Acuerdos de intercambio de información y software

Cuando se realicen acuerdos entre entidades para el intercambio de información y software, se especificarán el grado de sensibilidad y privacidad de la información de la entidad involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

- Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- Procedimientos de notificación de emisión, transmisión, envío y recepción.
- Normas técnicas para el empaquetado y la transmisión.
- Pautas para la identificación del prestador del servicio intercambio.
- Responsabilidades y obligaciones en caso de pérdida de datos.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

adecuadamente protegida.

- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- Controles especiales que puedan requerirse para proteger ítems sensibles, (claves o información encriptada, etc.).

8.13 Política uso de correo electrónico.

El Responsable de Seguridad y privacidad Informática verificará que los procedimientos de aprobación de Software recibido (Aprobación del Sistema) incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y la entidad.

Autorización: Niveles de Autorización adecuados para establecer disposiciones y emitir datos y/o documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.

Procesos de oferta y contratación pública: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.

Trámites en línea: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.

Verificación: Grado de verificación apropiado para constatar la información suministrada por los usuarios.

Cierre de la transacción: Forma de interacción más adecuada para evitar Fraudes.

Protección a la duplicación: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

No repudio: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envío o recibió.

Responsabilidad: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Seguridad del Correo Electrónico: Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

- La vulnerabilidad de los mensajes al acceso o modificación no

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

autorizados o a la negación de servicio.
- La posible intercepción y el consecuente acceso a los mensajes en los Medios de transferencia que intervienen en la distribución de los mismos.
- Las posibles vulnerabilidades a errores, por ejemplo, digitación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
- La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad del equipo receptor o de la red a la que se encuentra conectada.
- El impacto de un cambio en el medio de comunicación en los procesos del Instituto.
- Las consideraciones legales, como la necesidad potencial de contar con Prueba de origen, envió, entrega y aceptación.
- El acceso de usuarios remotos a las cuentas de correo electrónico.
- El uso inadecuado por parte del personal.

Control de Correo Electrónico

El responsable de Seguridad y privacidad de la Información en cumplimiento con el MANUAL ADMINISTRACIÓN Y GESTIÓN DE CUENTAS DE CORREO ELECTRÓNICO DESDE LA CONSOLA ADMINISTRATIVA (GOOGLE WORKSPACE) DEL INSOR MNGT04, documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

- Protección contra ataques al correo electrónico, por ejemplo, virus, interceptación, etc.
- Protección de archivos adjuntos de correo electrónico.
- Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de prueba jurídica.
- Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
- Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, Cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
- Definición de los alcances del uso del correo electrónico por parte del personal Del INSOR.
  Potestad Del INSOR para auditar los mensajes recibidos o emitidos por los servidores de la entidad, lo cual se incluirá en el "Acuerdo de confidencialidad".

Estos dos últimos puntos deben ser tenidos en cuenta bajo las normas vigentes que no sólo prohíben a los empleados a hacer uso indebido o con fines particulares del patrimonio estatal, sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

Entender el correo electrónico como una herramienta más de trabajo que

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

se entrega al funcionario con el fin de ser utilizada conforme al uso al cual está destinada, y que faculta al INSOR a implementar sistemas de control destinados a velar por la protección y el buen uso de sus recursos.

Adicionalmente deben tenerse en cuenta las siguientes normas para el buen uso del correo electrónico dentro Del INSOR:

- El servicio de correo electrónico del INSOR, debe usarse única y exclusivamente para actividades relacionadas directamente con las actividades de la entidad y está restringido únicamente para el uso de las personas que determine el Despacho de la Dirección General.
- Los funcionarios del INSOR, no están autorizados para enviar archivos de más de 25 Mb a través del servicio de correo electrónico, salvo que exista una autorización directa la oficina del Despacho del INSOR o que existan unos requerimientos de la entidad.
- Los usuarios de correo electrónico, no están autorizados a enviar información en forma masiva a múltiples direcciones de correo electrónico, ya que dicho comportamiento podría ser interpretado como correo "spam" y acarrear que bloqueen el servicio de correo electrónico del INSOR.
- Cuando un empleado requiera el uso de correo electrónico debe solicitarlo formalmente a la Oficina de Planeación mediante un requerimiento de solicitud de acceso debidamente diligenciado y autorizado por el jefe inmediato del usuario, especificando las necesidades del uso de este servicio.
- Los funcionarios deben abstenerse de abrir enlaces o archivos adjuntos sospechosos recibidos por correo electrónico, y deben reportar inmediatamente cualquier intento de phishing, malware u otros riesgos informáticos al área encargada de seguridad de la información.
- Cualquier usuario que haga uso de la infraestructura de correo electrónico implícitamente autoriza al INSTITUTO NACIONAL PARA SORDOS a evaluar en cualquier momento el contenido de la información que intercambie.
- Ningún usuario de correo electrónico, debe modificar, falsificar o eliminar cualquier información que aparezca en cualquier lugar de un mensaje de correo electrónico, incluyendo el cuerpo del mensaje o encabezado.
- Salvo con aprobación previa de la Oficina de Planeación y/o el Despacho ningún empleado puede usar cuentas gratuitas de correo electrónico en Internet para el envío de mensajes corporativos de la entidad. Todos los mensajes de carácter corporativo deberán ser

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

enviados a través del sistema de correo electrónico corporativo y designado por el INSOR.

- Salvo que exista una autorización expresa de la Oficina de planeación y/o el Despacho ningún empleado está autorizado para interceptar, revelar o contribuir en la intercepción de mensajes de correo electrónico a través de herramientas de escaneo.
- El SPAM o correo "basura" es una modalidad de envío indiscriminado de mensajes de correo electrónico no solicitados y que por lo general es masivo. Los usuarios del servicio del correo electrónico del INSOR, no deben contestar mensajes SPAM, ya que al hacerlo confirmarán su dirección de correo y si le llegan mensajes de un mismo remitente, notifique a la Oficina de planeación y sistemas.
- Ningún usuario del servicio de correo electrónico del INSOR debe prestar atención a mensajes con falsos contenidos de virus (Hoaxes), ofertas de premios, dinero, solicitudes de ayuda caritativa, venta de bienes (hardware o software) o financiamiento a muy bajo costo, productos medicinales, acceso gratuito a portales, advertencia de virus de fuentes desconocidas, etc.
- Para todos los funcionarios o usuarios del servicio de correo electrónico del INSOR, está prohibido brindar servicios que, de manera directa o indirecta, faciliten la proliferación de spam, en esto se incluye casillas de correo, software para realizar spam, hosting de sitios de Web para realizar SPAM o que realicen SPAM, o bien que realicen Hoaxes o bromas de mal gusto y/o fraudes, éstos últimos definidos como un correo electrónico que atrae el interés del usuario y que esconde una maniobra deshonesta. Y brindar servicios que, de manera directa o indirecta, faciliten la proliferación de Software malicioso o Malware, Software espía o Spyware o Phishing, vishing smishing.

Declaración de rectificación

A cada correo saliente de e-mail por Internet se le debe asociar un "aviso" como se detalla a continuación:

El Instituto Nacional para Sordos – INSOR no garantiza, de manera expresa ni implícita, la disponibilidad, integridad o confidencialidad de los mensajes enviados por correo electrónico. No se hace responsable por daños derivados de demoras, pérdidas de datos, entregas erróneas o interrupciones del servicio ocasionadas por fallas del sistema, errores u omisiones del usuario. El uso de la información contenida en este correo electrónico es bajo su

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

responsabilidad. Asimismo, el INSOR no asume responsabilidad alguna por la veracidad o exactitud de la información obtenida a través de medios electrónicos. Las opiniones del contenido son de su autor y no necesariamente representan la opinión oficial del Instituto Nacional para Sordos – INSOR.

8.14 Seguridad para el uso de elementos, servicios de red y comunicaciones.

Las redes de comunicación de datos proveen múltiples puntos de entrada al Ambiente de cómputo del INSOR, y a la Información almacenada directamente y periféricamente en este ambiente. En consecuencia, las comunicaciones entre equipos de cómputo y usuarios son críticas para la operación del INSOR, también incrementa las amenazas de conexiones no autorizadas para acceder a los datos e información de la entidad, acorde con el numeral 9.1.2 Acceso a las redes y a los servicios de red de la norma ISO27001:2002 se debe cumplir con lo siguiente:

Acceso de red

Las conexiones no seguras a los servicios de red pueden afectar a todo el INSOR, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El responsable del Proceso de Gestión de las TIC tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal de alguna máxima autoridad del INSOR que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad del INSOR.

Para esto, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Caminos de acceso no estándar.

- Para proteger el ambiente de cómputo del INSOR, de accesos por Ambiente, deben de estar de acuerdo con las conexiones autorizadas, aprobadas y establecidas.
- Todos los caminos de acceso deben ser planeados, diseñados e instalados para no evadir la seguridad.
- Ningún empleado instalará, hará operable u otra cosa que permita un camino de acceso el cual no ha sido aprobado por los responsables de seguridad.
- No se permitirán puertas traseras las cuales pretendan evitar los métodos y seguridad de acceso aprobados.

Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones del INSOR, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

- Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma. Para esto se debe tener en cuenta:
  - Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
  - Evitar la navegación ilimitada por la red.
  - Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
  - Controlar activamente las comunicaciones con origen y destino autorizados a través de un Gateway utilizando Firewalls.
  - Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera del INSTITUTO NACIONAL PARA SORDOS INSOR.

Monitoreo de red.

Las herramientas de monitoreo, equipos, hardware y software, tales como analizadores de protocolo y sniffers, pueden ser únicamente utilizados por empleados específicos para realizar actividades autorizadas por el INSOR. Se requiere autorización específica escrita de los responsables de seguridad para utilizar este tipo de facilidades y herramientas de diagnóstico.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Seguridad de los Servicios de Red.

El Responsable de Seguridad y privacidad Informática junto con el responsable del Proceso de Gestión de las TIC definirán las pautas para garantizar la seguridad de los servicios de red del INSOR, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de segurid-ad.

Dicha configuración será revisada periódicamente por el responsable de Seguridad y privacidad Informática.

Conexión a redes externas.

La conexión a redes externas tales como Internet y proveedores de servicios de información deberán ser controlada para prevenir el que se revele sin autorización alguna información, el ingreso de código malicioso y otros eventos que afecten el servicio.

Identificación y Autenticación de los Usuarios.

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar a la persona responsable

En circunstancias excepcionales, cuando existe un claro beneficio para INSOR, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Autenticación de Usuarios para Conexiones Externas.

Las conexiones externas son un potencial peligro para accesos no autorizados a la información del INSOR. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Seguridad y privacidad Informática, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

Protección de los Puertos (Ports) de Diagnóstico Remoto.

Muchos computadores y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "Autenticación de Usuarios para Conexiones Externas". También para este caso deberá tenerse en cuenta el punto "Camino Forzado".

Segmentación de Redes.

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados y VLANs. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

La segmentación en dominios y VLANs de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Comunicaciones electrónicas.

Las comunicaciones electrónicas son necesarias para desarrollar el aspecto misional del INSOR, y se reconoce que incrementan la productividad. Los funcionarios del INSOR, son responsables de su uso en el ambiente de cómputo y deben cumplir con las políticas aquí definidas.

- Todas las comunicaciones oficiales electrónicas generadas y procesadas a nivel de entrada, internas y de salida que deben estar en la plantilla vigente y con el consecutivo de radicado en el Sistema de Información Orfeo. Las copias de respaldo de los usuarios finales son consideradas de propiedad del INSOR.
- La capacidad de comunicación electrónica del ambiente de cómputo del INSOR, debe ser únicamente utilizado para funciones de las actividades autorizadas por la entidad. El uso personal en forma incidental y responsable es permitido siempre que no sea excesivo y que no interfiera con la productividad y que no compita con actividades legítimas de la entidad.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Todas las transmisiones o recepciones de correo electrónico están sujetas a monitoreo por empleados autorizados del INSOR.
- Los funcionarios del INSOR, no deben esperar Privacidad relativa al envío o recepción de comunicaciones electrónicas. Todas las transmisiones podrán ser monitoreadas y revisadas por empleados autorizados en algún momento sin notificación. Sin embargo, el INSOR no monitoreará regularmente el contenido de las comunicaciones electrónicas a menos que alguna razón legítima de la entidad haga requerir tal monitoreo.
- Los funcionarios del INSOR no deben transmitir vía comunicación electrónica información restringida o confidencial de la Entidad, a menos que tal información sea encriptada.
- Es prohibido enviar cadenas electrónicas de cartas.
- Es prohibido enviar mensajes ofensivos o acosadores.
- Es prohibido enviar mensajes anónimos.
- Es prohibido realizar solicitudes impropias.
- Todo funcionario debe participar en las capacitaciones periódicas que el INSOR imparta sobre el uso adecuado y seguro de las comunicaciones electrónicas.

Conexiones a Internet.

El INSOR provee servicios de Internet a sus funcionarios para acceder información, comunicar, recuperar o divulgar información relacionada con la Entidad.

Las conexiones a Internet deben seguir los requerimientos que a continuación se describen:

- Todos los accesos a Internet deben ser vía un dispositivo de Comunicación aprobado o administrado por el área tecnológica.
- Los Ingenieros adscritos a la Oficina Asesora de Planeación son los responsables de revisar regularmente todos los logs (registro oficial de eventos durante un rango de tiempo en particular: quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.) y archivos de auditoría de la actividad en línea de los usuarios de Internet, para asegurar que los servicios están siendo utilizados para beneficio del INSOR.
- Todos los servicios de Internet deben ser configurados para evitar que servicios no deseados estén siendo habilitados o reenrutados.

Es responsabilidad de la Oficina Asesora de Planeación y sistemas en título de su comité técnico evaluar e implementar las nuevas herramientas tanto de software como de hardware para que esta conexión sea lo más eficaz y

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

eficientemente posible.

Carga y descarga de archivos.

- La transferencia de información entre dos computadores del INSOR o entre un computador de la Entidad, y otro que no lo es, está autorizado únicamente para propósitos legítimos de la entidad.
- Está prohibido cargar o descargar información a/desde computadores externos a menos que sea específicamente autorizado como parte de las funciones propias del trabajo.
- Los usuarios deben realizar una evaluación para virus de los archivos descargados.
- Todos los archivos descargados en las estaciones de trabajo deberán Ser examinados a través de los anti-virus establecidos y autorizados.
- Los usuarios deben cumplir los requerimientos de licencia y las restricciones De copia asociadas con cualquier archivo descargado. Únicamente los archivos (ejecutables) absolutamente necesarios para las funciones del INSOR, deben ser encargados por el personal técnico de la Oficina Asesora de Planeación, buscando con esto conservar el espacio de almacenamiento, el desempeño de la red y evitar posibles virus en el ejecutable.

Estándares.

- Los últimos service pack deberán ser instalados una vez se haya hecho Oficial su lanzamiento con sus respectivas pruebas.
- El protocolo de comunicación interno y externo debe ser TCP/IP.
- Los nombres de las comunidades SNMP en los servidores no deben ser público (public), privado (private) ó sistema (system). Se deben asignar nombres que lo relacionen con la función que ese servidor desempeñe.
- La auditoría debe ser habilitada en los servidores más sensibles para la Entidad.
- Las cuentas con ID supervisor, administrator o similares deben ser Eliminadas de todos los servidores, se deben crear estas mismas cuentas sin privilegios y auditar su intento de uso no autorizado.
- Se debe crear un grupo administradores donde se le atribuirán permisos De admin Para las tareas de soporte en la red.
- El uso de las cuentas de administrador o admin deberán ser conocidas por dos o tres personas y su password debe ser cambiado cada 30 días.
- El user name y el password deben ser diferentes y sin nada que los relacione.
- Las cuentas de usuario son de uso personal y su contraseña debe ser secreta y no compartida.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Se deben definir los usuarios con permisos de backup y restore por la persona encargada del centro de cómputo y/o servicios de Red.
- Los permisos sobre las carpetas compartidas serán definidos según las aplicaciones o responsabilidades que el usuario maneje y/o administre.
- El password debe tener un mínimo de ocho (8) caracteres obligatorios y no Repetitivos.
- En el momento en que un empleado se retire de la entidad, su jefe inmediato debe notificar su retiro al administrador de los sistemas de información y revisar con prontitud los archivos y documentos guardados en el computador, con el fin de reasignar las tareas y delegar específicamente la responsabilidad de estos archivos que anteriormente estaban en manos del ex-empleado.
- A los usuarios en período de vacaciones se les debe suspender su cuenta en la red, por un período equivalente a dicho tiempo.
- Se deben bloquear las cuentas con más de cuatro intentos fallidos al ingresar al sistema.
- Se debe otorgar un tiempo para que la cuenta del usuario expire y deba cambiar su password.
- Los usuarios deben restringirse a una dirección IP para aquellos trabajos donde se vea comprometida la seguridad de la información.
- El antivirus debe estar programado para ejecutarse y actualizarse automáticamente con las opciones de "scan and cure".
- Todo el software utilizado en el INSOR, debe tener su respectiva licencia de uso.
- Todo el software comprado o desarrollado debe ser contabilizado a través de un sistema de inventario.

Control de Conexión a la Red.

Sobre la base de lo definido en el punto "Requerimientos", se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios o VLANs de la red.

Algunos de los entornos a los que deben implementarse restricciones son:

- Correo electrónico.
- Transferencia de archivos.
- Acceso interactivo.
- Acceso a la red fuera del horario laboral.
- Redes sociales.

Gestión De Elementos De Red.

- Los elementos y servicios de red no deben permitir que cuentas de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

usuario que presenten contraseñas en blanco o nulas, obtengan acceso remoto a cualquier computador, sistema o servicio de la red interna del INSOR.

- Todas las cuentas de usuario de los elementos y servicios de red otorgados a los funcionarios del INSOR o terceros, constituyen un activo de la institución que permite identificar de manera única e irrepetible a cada usuario. En ninguna circunstancia las cuentas de usuario deberán ser compartidas o reasignadas y su contraseña revelada.
- Los administradores de los elementos y servicios de red deben definir actividades de control que permitan detectar, analizar y notificar brechas de seguridad. En algunos casos se requiere implementar logs de registro de los incidentes presentados, para detectar oportunamente intentos de violación a los sistemas de información.
- Salvo expresa autorización del Despacho de la Dirección General, ningún usuario está autorizado para escanear, acceder o manipular directa o indirectamente los sistemas de información y de comunicaciones de la red de datos del INSOR, e instalar nuevos sistemas de comunicaciones de redes que se conecten con la red de datos de la institución.
- Realizar pruebas periódicas de identificación de vulnerabilidades y test de penetración a través de personas técnicamente preparadas (área de Sistemas o contratistas). Los responsables de la administración y/o del manejo de los sistemas de comunicaciones correspondientes no deben realizar estas pruebas.
- Definir, preparar y probar los planes de contingencias que permitan restablecer los servicios de red y la infraestructura que los soporta en el menor tiempo posible en caso de presentarse fallas o incidentes de seguridad que interrumpan las operaciones. Antes de implementar cualquier plan de contingencia las áreas responsables de la gestión de redes deben solicitar la autorización la Oficina de Planeación del INSOR.
- Los Switches, Routers y Firewalls que se involucren en las conexiones de redes de INSOR, deberán estar convenientemente asegurados de acuerdo con un estándar mínimo de configuración de seguridad.

Control de Acceso al Sistema Operativo. Identificación Automática de Terminales

El Responsable de Seguridad Informática junto con el responsable del Proceso de Gestión de las TIC realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

- El método de identificación automática de Terminales.
- El detalle de transacciones permitidas por terminal.

Procedimientos de Conexión de Terminales.

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá:

- Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
- Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder al servicio o al servidor.
- Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
- 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 debe indicar que parte de los datos es correcta o incorrecta.
- Limitar el número de intentos de conexión no exitosos permitidos y:
- Registrar los intentos no exitosos.
- Impedir otros intentos de identificación, una vez superado el límite permitido.
- Desconectar conexiones de comunicaciones de datos.
- Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.

Uso de Utilitarios de Sistema.

La mayoría de las infraestructuras informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

- Utilizar procedimientos de autenticación para utilitarios del sistema.
- Separar entre utilitarios del sistema y software de aplicaciones.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
- Evitar que personas ajenas al INSOR tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
- Establecer autorizaciones para uso gratuito (free) de utilitarios de sistema.
- Registrar todo uso de utilitarios del sistema.
- Definir y documentar los niveles de autorización para utilitarios del sistema.
- Remover todo el software basado en utilitarios y software de sistema innecesarios.

Uso de Utilitarios de Sistema.

La mayoría de las infraestructuras informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

- Utilizar procedimientos de autenticación para utilitarios del sistema.
- Separar entre utilitarios del sistema y software de aplicaciones.
- Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
- Evitar que personas ajenas al INSOR tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
- Establecer autorizaciones para uso gratuito (free) de utilitarios de sistema.
- Registrar todo uso de utilitarios del sistema.
- Definir y documentar los niveles de autorización para utilitarios del sistema.
- Remover todo el software basado en utilitarios y software de sistema innecesarios.

Desconexión de Terminales por Tiempo Muerto.

El Responsable de Seguridad y privacidad Informática, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo o que sirven a sistemas de alto riesgo. Las mismas se desconectarán después de un periodo definido de los sistemas críticos, tiempo muerto, para evitar el acceso de personas no autorizadas.

Para las PC’s, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un funcionario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

sesión de usuario habilitada.

Control de acceso a las aplicaciones: restricción del acceso a la información.

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política del INSOR para el acceso a la información.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

- Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrado será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.
- Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
- Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- Garantizar que las salidas de los sistemas de aplicación que administran Información sensible contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a los PCs y Ubicaciones autorizadas.
- Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

Aislamiento de los Sistemas Sensibles.

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en un equipo de cómputo dedicado, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

- Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación.
- Identificar y acordar con el administrador de la aplicación sensible

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
- Coordinar con el responsable del Proceso de Gestión de las TIC, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo con los requerimientos de operación y seguridad especificados por el administrador de la aplicación.

- Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
- Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

Monitoreo del Acceso y Uso de los Sistemas: Registro de Eventos.

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad y la privacidad.

Los registros de auditoría deberán incluir:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Identidad de la terminal (por dirección IP).
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Monitoreo del Uso de los Sistemas: Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de los recursos de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

8.15 Política de control de accesos Lógico .

Generalidades.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad de los equipos de cómputo y dispositivos activos de la infraestructura tecnológica del INSOR.

Objeto.

- Impedir el acceso no autorizado a los sistemas de información, bases de datos, servicios de información digital y documentada, teniendo en cuenta los respectivos controles de acceso.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red del INSOR y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad y privacidad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance.

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del INSOR, cualquiera sea la función que desempeñe.

Así mismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad.

El responsable de Seguridad y privacidad Informática estará a cargo de:

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas y la revisión de registros de actividades.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, firewalls, etc.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- 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, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos, segmentación 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.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

Evaluar los riesgos a los cuales se expone la información con el objeto de:

- Determinar los controles de acceso, autenticación y utilización a ser implementados en cada caso.
- Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de Revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

Cada jefe de área, junto con el Responsable de Seguridad y privacidad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad y privacidad de la información. Asimismo, autorizarán el acceso de los usuarios a su cargo a los servicios y

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

recursos de red y a Internet.

El responsable del Proceso de Gestión de las TIC cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo con lo definido por los propietarios de la información, 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.
- 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 con el pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

Requerimientos para el Control de Acceso.

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.
- Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

- Indicar expresamente si las reglas son obligatorias u optativas.
- Establecer reglas sobre la premisa "Todo debe estar prohibido a

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".
- Prever los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario.
- Regular los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.

Creación Y Eliminación De Usuarios (Internos Y Externos).

Los funcionarios, contratistas, outsourcing o terceros, antes de solicitar acceso a los sistemas de información deben firmar un acuerdo de confidencialidad.

- La asignación de los privilegios de acceso de todos los usuarios en los sistemas informáticos del INSOR debe regirse de acuerdo a las actividades que el usuario vaya a realizar.
- Las cuentas de usuario (internas/externas) creadas en los sistemas de información de la entidad deben tener un identificador único y deberán solicitarse mediante un requerimiento formal, especificando su identificación, nombres y apellidos y sus funciones que va a desempeñar, y autorizado por el jefe inmediato del usuario. Las cuentas de usuarios externos deben ser solicitadas y autorizadas a través del Gerente General del INSOR.
- La creación de las cuentas de usuario en los sistemas de información del INSOR, están sujetas a la adopción de un estándar de identificadores de usuario establecido por la Oficina de Planeación, salvo que existan impedimentos técnicos justificables que impidan la adopción de dicho estándar.
- La creación de cuentas genéricas, deben contar con el aval de la Oficina de Planeación. La persona responsable de su utilización es la encargada de notificar las novedades correspondientes de la cuenta.
- Los terceros están obligados a reportar, cualquier novedad que se presente con sus funcionarios (vacaciones, licencias, incapacidades, etc.) a la Oficina de Planeación y/o la Secretaria General del INSOR, para que éste, a su vez, gestione ante el administrador de los sistemas de información, la solicitud de retiro inmediato de accesos.
- Los terceros están obligados a reportar, el retiro de cualquiera de sus funcionarios a la Oficina de Planeación y/o la Secretaria General del INSOR, para que éste, a su vez, gestione ante el administrador de los sistemas de información, la solicitud de retiro inmediato de accesos.
- Cuando un empleado se retira del INSOR o no requiere seguir utilizando los sistemas de información, el administrador de los sistemas de información debe asegurarse que el usuario no pueda

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

ingresar modificando la contraseña actual, esto se requiere para guardar el log de transacciones que el usuario realizo.

Aspectos Importantes Para La Gestión De Cuentas Con Perfil De Administración.

Las cuentas de usuario con privilegios de administración y que son propias de los sistemas de información y equipos de red, deben cumplir con el procedimiento de administración de cuentas especiales definido por el responsable de la Seguridad y privacidad Informática y el responsable del área de informática.

Los privilegios especiales en los sistemas de información y equipos de red, deben limitarse a aquellos que están encargados directamente de la administración o seguridad de los sistemas, y sólo deben otorgarse a aquellos usuarios designados explícitamente como administradores de sistema.

Todas las Cuentas con privilegios administrativos deben estar dentro de un inventario de cuentas, especificando su relación con cada uno de los sistemas de información, a nivel de sistema operativo, base de datos y aplicación, especificando la siguiente información:

- Nombre de la Cuenta y propietario o Responsable de la cuenta.
- Ubicación de la cuenta (servidor, sistema o aplicativo)
- Ambiente al que pertenece la cuenta (Producción, Desarrollo, etc.)
- Tipo de Cuenta (Default, Genérica o de Conexión).
- Descripción general de la cuenta (que hace la cuenta y para que se usa).
- Vigencia de la contraseña de la cuenta (Cada cuanto debe cambiarse).

Todas las cuentas de usuario relacionadas con los servicios que presentan los sistemas de información y que son propias de los mismos, no se pueden deshabilitar y eliminar, salvo expresa autorización de la Oficina de Planeación y/o el despacho del INSOR.

Administración de Accesos de Usuarios.

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Registro de Usuarios.

El Responsable de Seguridad y privacidad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la Función del usuario de la función del usuario y es coherente con la política de Seguridad y privacidad de la información INSOR, por ejemplo, que no compromete la separación de tareas.
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización o se desvincularon del INSOR.
- Efectuar revisiones periódicas con el objeto de:
    - Cancelar cuentas de usuario redundantes.
    - Inhabilitar cuentas inactivas por más de 60 días.
    - Eliminar cuentas inactivas por más de a 120 días.
    - En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

Administración de Privilegios.

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a funcionarios sobre la base de la necesidad de uso y evento por evento.
- Mantener un proceso de autorización y un registro de todos los Privilegios asignados.
- Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
  Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad y privacidad Informática.

8.16 Política de administración de contraseñas de usuario.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración puede estar incluida en el Acuerdo de confidencialidad.
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- Generar contraseñas provisionales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- Configurar los sistemas de tal manera que:
  - Las contraseñas tengan más de 8 caracteres.
  - Suspendan o bloqueen permanentemente al usuario luego de 4 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda).
  - Solicitar el cambio de la contraseña cada lapso no mayor a 45 días.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Administración de Contraseñas Críticas.

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas, como instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad y privacidad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- Se definirán las causas que justificarán el uso de contraseñas críticas, así como el nivel de autorización requerido.
- Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad y privacidad de la información junto con el Responsable del Proceso de Gestión de las TIC.

Responsabilidades del Usuario- Uso de Contraseñas.

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- Mantener las contraseñas en secreto.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, que:
    - Sean fáciles de recordar.
    - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
    - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisionales en el primer inicio de sesión ("log on").
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus Contraseñas: pérdida o indicio de pérdida de confidencialidad.
- Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas.

Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad y privacidad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad y privacidad, para la protección de equipos desatendidos, así como de sus funciones en relación con la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- Proteger los PC contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

8.17 Política de dispositivos móviles, trabajo remoto y teletrabajo.

Computación Móvil.

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información del INSOR.

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CD, DVD, etc. y cualquier dispositivo de almacenamiento de conexión USB, cámaras digitales, etc. Así como también la red inalámbrica del INSOR.

Esta lista no es exclusiva o única, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial del INSOR y, por lo tanto, ser susceptibles de sufrir un incidente en el que se comprometa la seguridad de la entidad.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

- La protección física necesaria.
- El acceso seguro a los dispositivos.
- El acceso a los sistemas de información y servicios del INSOR a través de dichos dispositivos.
- Los mecanismos de resguardo de la información contenida en los dispositivos.
- La protección contra software malicioso.
- Protección y seguridad en el entorno de la red inalámbrica.

Por otra parte, se desarrollarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la entidad.

Trabajo Remoto y teletrabajo

El trabajo remoto y teletrabajo utiliza tecnología de comunicaciones para permitir que el funcionario trabaje en forma remota desde un lugar externo a INSOR.

El trabajo remoto y sólo será autorizado por el responsable del área, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad y privacidad de la Información, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad y privacidad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

En el caso de teletrabajo serán autorizados por el Jefe directo y llevados al comité de gestión y desempeño para su revisión de cumplimiento y aprobación.

Para esto, se establecerán normas y procedimientos para el trabajo remoto y teletrabajo, que consideren los siguientes aspectos:

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Utilización en lo posible de VPN entre el usuario el INSOR.
- En lo posible no utilizar o restringir el uso de programas de acceso remoto como TeamViewer, a menos que sea expresamente autorizado su uso por parte del despacho.
- El ambiente de trabajo remoto propuesto.
- Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Instituto, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
- La amenaza de acceso no autorizado a información o recursos por parte de Otras personas que utilizan el lugar, por ejemplo, familia y amigos.
- Evitar la instalación / desinstalación de software no autorizada por el INSOR.

Política de uso de redes inalámbricas.

Propósito

Garantizar el uso seguro, eficiente y responsable de las redes inalámbricas del INSOR, como herramienta de apoyo a sus funciones misionales, administrativas y de inclusión social, asegurando la disponibilidad del servicio y la protección de la información institucional.

La red inalámbrica ha sido implementada para brindar el servicio de Internet a través de dispositivos móviles dentro de las oficinas del Instituto Nacional para Sordos.

Alcance

Esta política aplica a todos los funcionarios, contratistas, visitantes y cualquier otra persona que acceda a las redes inalámbricas dentro de las instalaciones físicas del INSOR.

Aceptación de condiciones

El uso de la red inalámbrica implica la aceptación plena y sin reservas de esta política y sus futuras actualizaciones, las cuales podrán ser emitidas por la Oficina Asesora de Planeación y Sistemas.

Responsabilidades

- Oficina Asesora de Planeación y Sistemas:
  - Administrar y mantener la infraestructura de red inalámbrica.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Realizar cambios periódicos de contraseñas de acceso.
- Establecer restricciones de uso y seguridad técnica.

- Usuarios:
  - Usar la red de forma ética, responsable y conforme a esta política.
  - Garantizar la seguridad física y lógica de sus dispositivos.
  - Reportar incidentes de seguridad o mal uso.
  - No compartir contraseñas ni realizar acciones que comprometan la seguridad de la red.
  - Es responsabilidad de los usuarios contar con el software y configuración de seguridad en su equipo para minimizar el riesgo al que se puede ver expuesto a un ataque al encontrarse conectado sobre esta red.

Acceso y autenticación

- El acceso a la red inalámbrica se realizará exclusivamente mediante credenciales autorizadas proporcionadas por el área de TIC.
- Está prohibido divulgar las credenciales de acceso a terceros no autorizados.
- El área de TIC podrá modificar las credenciales sin previo aviso por razones de seguridad.

Uso para visitantes

Los visitantes deberán contar con autorización expresa y temporal para el uso de la red. El funcionario que solicite el acceso será responsable de comunicar esta política y supervisar su cumplimiento.

Configuración y compatibilidad

Cada usuario es responsable de configurar su dispositivo conforme a los lineamientos básicos definidos por el área de TIC. El soporte se prestará dentro del horario hábil del INSOR.

Disponibilidad y cobertura

- El servicio estará disponible de lunes a viernes entre las 6:00 a.m. y 8:00 p.m.
- La calidad del servicio puede verse afectada por interferencias externas, cantidad de usuarios o mantenimiento de infraestructura.

Condiciones de uso

- El servicio debe utilizarse exclusivamente para fines institucionales o de apoyo a actividades laborales.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- El proceso de Gestión de TIC no se hace responsable por conductas difamatorias, obscenas u ofensivas que se realicen a través de los servicios que proporciona.
- El usuario es responsable de toda actividad que se lleve desde su equipo o dispositivo mientras esté conectado a la red inalámbrica.
- El ancho de banda es compartido (máximo 4 Mbps por usuario) y su uso debe ser racional.
- Es responsabilidad del usuario estar enterado de los cambios de las presentes políticas.
- El grupo de Gestión TIC no es responsable del contenido y veracidad de la información que se transporta en la red inalámbrica.
- Está prohibido:
  - Acceder a sitios con contenido inapropiado, ilegal o no relacionado con las funciones del INSOR.
  - Usar programas P2P, servicios de streaming, VPNs no autorizadas o redes extendidas no controladas.
  - Ejecutar software malicioso o realizar actividades de monitoreo, escaneo, intrusión o alteración de infraestructura.
  - Distribuir spam o realizar ataques a la red o terceros.
  - Transmitir y/o distribuir cualquier material que viole la ley o regulación. Incluyen sin estar limitados a: material que viole derechos de autor u otros derechos de propiedad intelectual, como software sin licencia, música, videos, películas, etc.
  - Manipular los equipos de transmisión de la red inalámbrica.
  - Transgredir cualquier recurso informático, sistema o sitios de telecomunicaciones a los que no le está permitido acceder.
  - Cualquier conducta que viole las normas generalmente aceptadas dentro de la comunidad de Internet.

Control y monitoreo

La Oficina Asesora de Planeación y Sistemas podrá monitorear el uso de la red para verificar el cumplimiento de esta política, respetando los principios de necesidad y proporcionalidad.

Suspensión del servicio

El servicio podrá ser suspendido de manera temporal o definitiva por:

- Incumplimiento de esta política.
- Uso indebido, intencional o reiterado del servicio.
- Finalización del vínculo del usuario con el INSOR.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Atentar contra la disponibilidad, integridad, confidencialidad de la red.
- Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.
- Manipular o intentar manipular cualquier componente de la infraestructura de red.

8.18 Política de desarrollo y mantenimiento de sistemas.

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas de información, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer y/o alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad, privacidad y validación de datos en el desarrollo de los sistemas de información e información documentada.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollo propio o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Instituto en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad y privacidad Informática y el responsable del Área de Informática, junto con el Propietario de la Información, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad y privacidad Informática, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos si es necesario. Luego, el Responsable de Seguridad y privacidad de la Informaicón definirá junto con el responsable del Área de Informática, los métodos de encripción a ser utilizados.

Asimismo, el Responsable de Seguridad y privacidad Informática cumplirá las siguientes funciones:

- 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; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El responsable del Proceso de Gestión de las TIC, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal del área de Informática que considere adecuado. Asimismo, verificará el cumplimiento de las definiciones

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Informática propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

Los Responsables de La Secretaria General y Oficina Jurídica, incorporarán aspectos relacionados con el licenciamiento, la calidad del software y la seguridad y privacidad de la información en los contratos con terceros por el desarrollo de software.

Requerimientos de Seguridad de los Sistemas.

Análisis y Especificaciones de los Requerimientos de Seguridad.

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o desarrollados por terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

- Definir un procedimiento para que, durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad y privacidad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad y privacidad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas y de seguridad y privacidad informática, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
- Evaluar los requerimientos de seguridad, privacidad, y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
- Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Seguridad en los Sistemas de Aplicación.

Para evitar la pérdida, modificación o uso inadecuado de los datos

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

- La validación de datos de entrada.
- El procesamiento interno.
- La autenticación de mensajes (interfaces entre sistemas)
- La validación de datos de salida.

Validación de Datos de Entrada.

Se definirá un procedimiento que, durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

- Control de secuencia.
- Control de monto límite por operación y tipo de usuario.
- Control del rango de valores posibles y de su validez, de acuerdo con criterios predeterminados.
- Control contra valores cargados en las tablas de datos.
  Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

- Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.
- Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.
- Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.
- Controles de Procesamiento Interno.

Se definirá un procedimiento para que, durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

- Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
- Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

secuencia o cuando falle el procesamiento previo.
- Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
- Procedimientos que realicen la validación de los datos generados por el sistema.
- Procedimientos que verifiquen la integridad de los datos.
- Procedimientos que controlen la integridad de registros y archivos.
- Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
- Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización del programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

Autenticación de Mensajes.

Cuando una aplicación tenga previsto el envío de mensajes que contengan Información clasificada, se implementarán los controles determinados en el punto "Controles Criptográficos".

Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

- Comprobaciones de la razonabilidad para probar si los datos de salida son óptimos.
- Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
- Provisión de información suficiente, para que el receptor o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
- Procedimientos para responder a las pruebas de validación de salidas.
- Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

8.19 Política Controles Criptográficos.

Se utilizarán sistemas y técnicas criptográficas para la protección de la información con base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. Estos controles son potestad del responsable de la Seguridad y privacidad de la Información en conjunto con el responsable del Área de Informática.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Política de Utilización de Controles Criptográficos.

El INSOR establece la presente Política de uso de controles criptográficos, acorde con la norma numeral 10.1.1. Política sobre el empleo de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que se utilizaran controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito de la Entidad.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad y privacidad Informática.
- Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

Cifrado

Sobre la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad y privacidad de la Información, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del Algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la Política Del INSOR en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.

Firma Digital.

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente mediante Autenticator (código para logearse) , token digital, control de QR para crear las firma digital. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Al utilizar firmas y certificados digitales, se considerará la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.

Servicios de No Repudio.

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

Normas, Procedimientos y Métodos.

Se redactarán las normas y procedimientos necesarios para:

- Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- Generar y obtener certificados de clave pública de manera segura.
- Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
- Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
- - Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
- Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo, cuando las claves están comprometidas o cuando un usuario se desvincula del Instituto.
- Recuperar claves pérdidas o alteradas como parte de la administración de la Continuidad de Operaciones del INSOR, por ejemplo, para la recuperación de la información cifrada.
- Archivar claves, por ejemplo, para la información archivada o resguardada.
- Destruir claves.
- Registrar y auditar las actividades relativas a la administración de claves.
- A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso no mayor a 12 meses.

Gestión de claves

Los medios de cifrado implican mantener una gestión de claves criptográficas utilizadas por los medios de cifrado. Se debe tener en cuenta el cumplimiento del ciclo completo, así:

- La generación

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Su uso y protección
- La distribución
- La renovación o destrucción
- Como parte de la función de gestión deberemos determinar las fechas de activación y desactivación de claves en orden a reducir los riesgos mencionados anteriormente, una vez más sujetos a una evaluación de riesgos.

8.20 POLÍTICA DE SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA.

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

Control del Software Operativo.

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

Toda aplicación, desarrollada por el INSOR o por un tercero tendrá un único responsable designado formalmente por el responsable del Proceso de Gestión de las TIC.

- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrán acceder a los ambientes de producción.
- El responsable del Proceso de Gestión de las TIC, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:
    - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
    - Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
    - Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable.
    - Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

- Guardar sólo los ejecutables en el ambiente de producción.
- Llevar un registro de auditoría de las actualizaciones realizadas.
- Retener las versiones previas del sistema, como medida de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

contingencia.
- Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
- Denegar permisos de modificación al implementador sobre los programas Fuentes bajo su custodia.
- Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

Protección de los Datos de Prueba del Sistema.

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos operativas o en producción. En caso contrario se deben despersonalizar los datos antes de su uso.
- Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
- Eliminar inmediatamente, una vez completadas las pruebas, la Información operativa utilizada.

Control de Cambios a Datos Operativos.

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo con el esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad Informática definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

- Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
- El Propietario de la Información afectada y del Responsable de Seguridad y privacidad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
- Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.

- Se designará un encargado de implementar los cambios, el cual no será personal del Grupo de Desarrollo (propio o de terceros).
- Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad y privacidad Informática.

Control de Acceso a las Bibliotecas de Programas Fuentes.

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

El responsable del Proceso de Gestión de las TIC, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá:

- Proveer al Grupo de Desarrolladores los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente ejecutable.
- Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
- Administrar las distintas versiones de una aplicación.
- Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.
- Denegar al "administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.
- Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
- Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
- Evitar que la función de "administrador de programas fuentes" sea ejercida por personal que pertenezca al grupo de desarrollo y/o mantenimiento (propio o de terceros).
- Prohibir el resguardo de programas fuentes históricos (que no sean

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

los correspondientes a los programas operativos) en el ambiente de producción.
- Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
- Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el INSOR en los procedimientos que surgen de la presente política.

8.21 POLÍTICA DE PROCESOS DE DESARROLLO Y SOFTWARE.

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto, se controlarán los entornos y el soporte dado a los mismos.

Procedimiento de Control de Cambios.

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

- Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- Obtener aprobación formal por parte del responsable del Proceso de Gestión de las TIC para las tareas detalladas, antes que comiencen las tareas.
- Solicitar la revisión del Responsable de Seguridad y privacidad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

software.
- Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
- Garantizar que sea el implementador quien efectúe el paso de los objetos modificados al ambiente operativo o de producción, de acuerdo a lo establecido en "Control del Software Operativo".

Revisión Técnica de los Cambios en el Sistema Operativo.

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

- Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
- Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
- Asegurar la actualización del Plan de Continuidad de Operaciones del INSOR.

Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del responsable del Proceso de Gestión de las TIC, se deberá:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea efectuada por el INSOR, por el proveedor o por un tercero.
- Evaluar el impacto que se produce si el INSOR se hace cargo del mantenimiento.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando por si fuera necesario aplicarlo a nuevas versiones.

Desarrollo Externo de Software.

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

- Acuerdos de licencias, propiedad de código y derechos conferidos (Derechos de Propiedad Intelectual).

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

- Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad y privacidad del software establecidos, etc.
- Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto "Requerimientos de Seguridad en Contratos de Tercerización".
- Formalizar acuerdos para la entrega y custodia segura del código fuente y demás documentación crítica del software, incluyendo mecanismos para garantizar su disponibilidad en caso de incumplimiento contractual, disolución o quiebra del proveedor.

Anexo

Para cumplir con esta Política, en lo referente a los puntos "Seguridad de los Archivos del Sistema y "Seguridad de los Procesos de Desarrollo y Soporte", se sugiere implementar un modelo de separación de funciones entre los distintos ambientes involucrados.

Toda aplicación generada en el grupo de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

A continuación, se presenta un modelo ideal formado por tres ambientes que debe ser adoptado teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir alguna fuente para modificar, quedando registrado en el sistema de control de versiones que administra el Administrador De Programas Fuentes.

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Ambiente de Pruebas

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible.

El testeador o probador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctas de acuerdo con las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

Ambiente de Producción

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El "implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el paso para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

8.22 POLÍTICA DE ADMINISTRACIÓN DE LA CONTINUIDAD DE OPERACIONES.

Generalidades

La administración de la Continuidad de Operaciones es un proceso crítico que debe involucrar a todos los niveles del INSOR.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del INSOR puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la entidad y asegurar la reanudación oportuna de las

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

operaciones indispensables.

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales del INSOR (sean éstas resultado de desastres naturales, accidentes, fallas en la infraestructura tecnológica, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia del INSOR con el establecimiento de planes que incluyan al menos las siguientes etapas:

Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.

Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la entidad y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos críticos de infraestructura tecnológica identificados en el INSOR.

Responsabilidad

El Responsable de Seguridad y privacidad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información y el Responsable de Seguridad y privacidad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del INSOR.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

el que se abordará la continuidad de las actividades del INSOR.

- Elaborar los planes de co ntingencia necesarios para garantizar la continuidad de las actividades del INSOR.

Los Responsables de Procesos que involucren tecnología, revisarán periódicamente los planes bajo su responsabilidad, así como también identificar cambios en las disposiciones relativas a las actividades del INSOR aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

Control: La organización debe establecer y mantener contacto con las autoridades pertinentes, con grupos de interés especial u otros foros y asociaciones profesionales especializados en seguridad.

9. CONCIENTIZACIÓN Y CAPACITACIÓN

INSOR a través de su grupo interno de trabajo de Talento Humano y Contratación, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones. La entidad implementara las estrategias adecuadas para crear y fortalecer una cultura, cambio y apropiación de Seguridad de la información, lo cual implica un cambio en el comportamiento de los colaboradores en relación a las políticas y directrices que deben cumplir. Esto debe generar la identificación de perfiles de conocimiento, público objetivo, temáticas identificadas para el año, y finalmente la medición de esta gestión.

La presente política será de aplicación obligatoria para todos los servidores públicos, contratistas y terceros que, en el ejercicio de sus funciones, accedan, procesen o gestionen información institucional, independientemente del tipo de vínculo contractual, modalidad de trabajo o nivel jerárquico. INSOR promoverá acciones de formación continuada y sensibilización que permitan fortalecer la cultura organizacional en torno a la protección de la información, incluyendo temas como gestión de contraseñas, uso adecuado de los recursos tecnológicos, prevención de incidentes de seguridad digital, protección de datos personales y buenas prácticas frente a amenazas cibernéticas.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

La responsabilidad de coordinar y liderar las actividades de capacitación recae en el Responsable de Seguridad y privacidad de la información, quien deberá definir un plan de formación anual en articulación con el área de Talento Humano. Este plan deberá contemplar contenidos ajustados a los perfiles de los funcionarios, priorizando los riesgos identificados en el proceso de valoración institucional. El área de Talento Humano apoyará en la planeación, ejecución y seguimiento de las actividades, incluyendo el registro de asistencia y el diseño de mecanismos de evaluación del nivel de apropiación.

Los líderes de proceso y coordinadores tendrán la obligación de asegurar la participación de su equipo en las actividades programadas, así como de verificar que todo nuevo integrante reciba inducción en seguridad de la información al momento de su vinculación. Cada servidor público y contratista, por su parte, será responsable de aplicar en el ejercicio de sus funciones los conocimientos adquiridos y de actuar de forma diligente para prevenir, detectar y reportar comportamientos o situaciones que puedan afectar la seguridad de la información institucional.

INSOR se compromete a revisar y actualizar periódicamente sus estrategias de concientización, de acuerdo con la evolución de los riesgos y las necesidades detectadas, propiciando una cultura preventiva, proactiva y alineada con los principios del MSPI y los estándares internacionales de seguridad de la información.

10. PROCESO DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DEL INSTITUTO NACIONAL PARA SORDOS INSOR.

El comité de Gestión y Desempeño, será el responsable de la coordinación del desarrollo de los procesos que garanticen la Continuidad de Operaciones del INSOR.

Este comité tendrá a cargo la coordinación del proceso de administración de la continuidad de operaciones de los sistemas de procesamiento de información del INSOR y la infraestructura de tecnología en general frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades del INSOR.
- Asegurar que todos los funcionarios del INSOR comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del INSOR.
- Elaborar y documentar una estrategia de continuidad de operaciones

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

del INSOR consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de operaciones del INSOR de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de operaciones del INSOR.
- Proponer las modificaciones a los planes de contingencia.

11. CONTINUIDAD DE LAS ACTIVIDADES Y ANÁLISIS DE LOS IMPACTOS.

Con el fin de establecer un Plan de Continuidad de operaciones del INSOR se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en la infraestructura de tecnología y su equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos Producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.
- Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad y privacidad de la Información, considerando todos los procesos de las actividades de la entidad y no limitándose a las instalaciones de procesamiento de la información.
- Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las operaciones del INSOR. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Subcomité de Gestión y Desempeño de la Información a la máxima autoridad del INSOR para su aprobación.

Elaboración e Implementación de los Planes de Continuidad de las

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Actividades del Instituto

Los dueños de procesos y recursos de información, con la asistencia del Responsable de Seguridad y privacidad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del INSOR, y darán cumplimiento al Procedimiento Continuidad del Negocio código PRGT05.

El proceso de planificación de la continuidad de las operaciones considerará los siguientes puntos:

- Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos.
- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
    - Objetivo del plan.
    - Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
    - Procedimientos de divulgación.
    - Requisitos de la seguridad.
    - Procesos específicos para el personal involucrado.
    - Responsabilidades individuales.
    - Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades misionales del INSOR requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable.

Marco para la Planificación de la Continuidad de las Actividades del Instituto.

Se mantendrá un solo marco para los planes de continuidad de operaciones del INSOR, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deberán ser propuestas por el Subcomité de Gestión y Desempeño para su aprobación.

El marco para la planificación de la continuidad de operaciones del INSOR, tendrá en cuenta los siguientes puntos:

- Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
- Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del INSOR y/o la vida humana.
- Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del INSOR o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Instituto.
- Definir un cronograma de mantenimiento que especifique cómo y cuándo será aprobado el plan, y el proceso para el mantenimiento del mismo.
- Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de Continuidad las operaciones y garantizar que los procesos sigan siendo eficaces.

Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Instituto.

Debido a que los planes de continuidad de las actividades del INSOR pueden fallar, por suposiciones incorrectas, errores o cambios en la infraestructura de tecnología, se establecen las siguientes pautas de acción:

- El Responsable de Seguridad y privacidad de la información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

  El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Subsistema.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

- Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando pruebas de interrupciones).
- Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia). Realizar ensayos completos probando que el Instituto, el personal, el equipamiento, las instalaciones y los procesos se pueden afrontar.

Cada uno de los responsables de Procesos se encarga de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como también de la identificación de cambios en las disposiciones relativas a las actividades del INSOR aún no reflejadas en dichos planes.

Deberá prestarse especial atención a los cambios de:

- Personal.
- Direcciones o números telefónicos.
- Ubicación, instalaciones y recursos.
- Legislación.
- Contratistas, proveedores y clientes críticos.
- Procesos, o procesos nuevos / eliminados.
- Tecnologías.
- Requisitos operacionales.
- Requisitos de seguridad.
- Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- Requerimientos de los sitios alternativos.
- Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el comité de gestión y desempeño institucional para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

12. PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS

Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad y privacidad Informática.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- Procesamiento y manejo de la información.
- Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Restricciones en el uso de utilitarios del sistema.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, Incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

- Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- Instalación y mantenimiento de las plataformas de procesamiento.
- Monitoreo del procesamiento y las comunicaciones.
- Inicio y finalización de la ejecución de los sistemas.
- Programación y ejecución de procesos.
- Gestión de servicios.
- Resguardo de información.
- Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
- Uso del correo electrónico.
- Uso de Internet.

13. CUMPLIMIENTO

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

Todos los procedimientos, manuales, instructivos, etc., a los que se hacen alusión en este Manual de Seguridad y privacidad de la Información, harán parte de este, en la medida que se vayan aprobando y formalizado por parte de quien corresponda.

Objetivos

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al INSOR y/o al funcionario que incurra en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad Del INSOR.
  Revisar la seguridad y privacidad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.
- Optimizar la eficacia del proceso de auditoría y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
- Garantizar la existencia de controles que protejan los sistemas en Producción y las herramientas de auditoría en el transcurso de las auditorías.
- Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Instituto.

Alcance

Esta Política se aplica a todo el personal del INSOR, cualquiera sea su situación.

Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas del INSOR y a las auditorías efectuadas sobre los mismos.

Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

responsabilidades y funciones individuales para cumplir con dichos requisitos.

Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los funcionarios únicamente podrán utilizar material autorizado por el INSOR. El INSOR solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Derecho de Propiedad Intelectual del Software.

El software es considerado una obra intelectual que goza de la protección de la Ley.

La Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El responsable del Área de Informática y el responsable de la Seguridad y privacidad de la Información, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

- Aplicar las normas y políticas de desarrollo y mantenimiento de sistemas de información, para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
- Alinearse a los controles exigidos en la norma ISO 27001:2022 en cuánto a análisis y especificación de requisitos de seguridad, aseguramiento de los servicios de aplicación en las redes públicas y transacciones en línea, seguridad en los procesos de desarrollo y datos de prueba.
- Implementar una herramienta para la gestión que permita detectar, responder, reportar y aprender del incidente presentado.
- Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

tomar acciones disciplinarias contra el personal que las violen.
- Mantener un adecuado registro de activos.
- Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
- Implementar controles para evitar el exceso del número máximo permitido de usuarios.
- Verificar que sólo se instalen productos con licencia y software autorizado.
- Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
- Utilizar herramientas de auditoría adecuadas.
- Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

Protección de Datos y Privacidad de la Información Personal.

Todos los funcionarios deberán conocer las restricciones al tratamiento de los datos y de la información respecto de la cual tengan conocimiento con motivo del ejercicio de sus funciones.

El INSOR redactará un "Acuerdo de confidencialidad", el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por el INSOR.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, difundir o de alguna otra forma hacer pública la información a ninguna persona, firma, entidad o tercera persona, salvo autorización previa y escrita del responsable del Activo de que se trate. A través del "Acuerdo de confidencialidad" Dese deberá advertir al funcionario que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se debe diligenciar el formato de ACUERDO DE CONFIDENCIALIDAD DE FUNCIONARIOS PARA LA NO DIVULGACIÓN DE INFORMACIÓN.

Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información.

Los recursos de procesamiento de información del INSOR se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

Recolección de Evidencia.

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, El INSOR garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

14. REVISIONES DE LA POLÍTICA DE SEGURIDAD PRIVACIDAD Y LA COMPATIBILIDAD TÉCNICA.

Cumplimiento de la Política de Seguridad.

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad y privacidad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad y privacidad de la Información y el responsable del Área de Informática, realizarán revisiones semestrales en el año o cuando se precise de algún cambio de la política de Seguridad y Privacidad de la Información. Los cambios deben hacerse de forma planificada de acuerdo con el numeral 6.3 de la norma ISO 27002:2022. Las revisiones se harán efectivas a todas las áreas del Instituto a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- Sistemas de información.
- Proveedores de sistemas.
- Propietarios de información.
- Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

Verificación de la Compatibilidad Técnica.

El Responsable de Seguridad y privacidad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

especializada.

El resultado de la evaluación se plasmará en un informe técnico para su posterior interpretación por parte de los especialistas. Para esto, la tarea podrá ser realizada por un profesional experto (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo supervisión.

Sanciones Previstas por Incumplimiento.

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad y privacidad de la información conforme a lo dispuesto por las normas estatutarias y convencionales que rigen al personal de la Administración Pública Nacional, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Institutos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

Además de las sanciones disciplinarias o administrativas, el funcionario Que no da debido cumplimiento a sus obligaciones puede incurrir también en Responsabilidad civil o patrimonial cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

14. Sensibilización y Comunicación en Seguridad de la Información

El Responsable de Seguridad y privacidad de la Información y el Responsable del Área de Informática es el encargado de definir y actualizar los lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cubra en su totalidad los

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

funcionarios y servidores públicos de la Entidad, para lo cual aplicará el documento instructivo de comunicación, sensibilización, y capacitación de seguridad de la información, código ITGT01, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro del INSOR, se busca:

· Definir los temas para la capacitación en seguridad de la información, de acuerdo con el público objetivo.

· Establecer la metodología que les permita evidenciar cuales son las necesidades de capacitación para la entidad.

· Construir materiales para sensibilización y entrenamiento.

· Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la Entidad.

Acorde con la guía Plan de capacitación, sensibilización y comunicación de Seguridad de la Información del Ministerio de Tecnologías de la Información, dentro de la cual se clasifica los roles de acuerdo con el objetivo y necesidad específica, así:

EJECUTIVOS	Deben conocer y entender las leyes y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás unidades.
PERSONAL DE SEGURIDAD (OFICIALES DE SEGURIDAD)	Son los asesores expertos en seguridad, deben estar bien preparados en políticas de seguridad y buenas prácticas
DUEÑOS DE SISTEMAS	Deben entender bien las políticas de seguridad, así como también conocer sobre los controles de seguridad y la relación que tienen con los sistemas que manejan.
ADMINISTRADORES DE SISTEMAS Y PERSONAL DE SOPORTE	Estos funcionarios deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del Entidad de manera apropiada.
USUARIOS FINALES	Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición.

Tabla 1. Roles Y Necesidades En Capacitación Más Comunes

Fuente: Ministerio de Tecnologías y las comunicaciones

15. Consecuencias del Incumplimiento

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

El incumplimiento de las políticas, lineamientos, procedimientos y controles establecidos en materia de seguridad de la información por parte de servidores públicos, contratistas o terceros que tengan acceso a los activos de información del INSOR será considerado una falta grave, que podrá dar lugar a la aplicación de las sanciones administrativas, disciplinarias, contractuales, civiles o penales correspondientes, de acuerdo con la normatividad vigente.

Toda persona que, por acción u omisión, comprometa la confidencialidad, integridad o disponibilidad de la información institucional, o que propicie, facilite o no reporte incidentes de seguridad, será responsable por los perjuicios que su conducta ocasione, incluyendo los que afecten la prestación de los servicios, la continuidad operativa, la imagen institucional o la protección de datos personales.

INSOR deberá asegurar que todos los contratos que impliquen acceso, tratamiento o gestión de información institucional contengan cláusulas específicas que establezcan claramente los deberes de confidencialidad, el compromiso de cumplimiento de la Política de Seguridad de la Información, así como las consecuencias derivadas de su inobservancia. Estas cláusulas deberán contemplar la obligación de firmar acuerdos de confidencialidad, la posibilidad de aplicar sanciones por incumplimiento de las medidas de seguridad adoptadas y, en caso de negligencia comprobada, el pago de indemnizaciones por los daños ocasionados a la entidad o a terceros.

En el caso de los servidores públicos, la vulneración de estas disposiciones podrá dar lugar a investigaciones disciplinarias conforme al Código General Disciplinario. En el caso de contratistas, se podrá proceder con la imposición de sanciones contractuales, y la terminación anticipada del contrato. Para terceros, se procederá según lo estipulado en los respectivos convenios o acuerdos, sin perjuicio de las acciones legales a que haya lugar.

El desconocimiento de estas políticas no exime de responsabilidad. INSOR se reserva el derecho de emprender las acciones legales y administrativas pertinentes cuando el incumplimiento represente un riesgo o daño para la entidad, sus procesos, usuarios o sistemas de información. La aplicación efectiva de esta política requiere el compromiso activo de todos los actores involucrados con la gestión de la información institucional.

16. Auditorías

Con el fin de verificar la eficacia, adecuación y cumplimiento de las políticas, procedimientos y controles establecidos en materia de seguridad de la información, el INSOR realizará auditorías internas de forma periódica, programada y documentada. Estas auditorías tienen como objetivo identificar desviaciones, evaluar el nivel de madurez del Modelo de

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

Seguridad y Privacidad de la Información (MSPI) y proponer acciones de mejora continua, conforme al enfoque de gestión basado en el ciclo PHVA (Planear, Hacer, Verificar, Actuar).

Las auditorías permitirán verificar el cumplimiento de los requisitos legales, normativos y contractuales aplicables, así como el grado de implementación y efectividad de los controles definidos para proteger la confidencialidad, integridad y disponibilidad de la información institucional. Estas revisiones podrán abarcar todos los procesos misionales y de apoyo incluidos dentro del alcance del MSPI, incluyendo los activos de información, los sistemas tecnológicos, la infraestructura física y lógica, el cumplimiento de roles y responsabilidades asignadas y el manejo de incidentes de seguridad.

Las auditorías serán ejecutadas por personal con competencia técnica suficiente y con independencia frente a los procesos auditados, garantizando objetividad e imparcialidad en los resultados. Cuando sea necesario, el INSOR podrá apoyarse en auditores externos especializados o en instancias de control del orden nacional, conforme a las disposiciones legales aplicables.

Las observaciones o hallazgos detectados durante las auditorías deberán ser documentados y comunicados oportunamente a los responsables de los procesos auditados, quienes estarán obligados a implementar las acciones correctivas, preventivas o de mejora que se definan. Así mismo, los resultados de las auditorías serán insumo para la revisión por la alta dirección y para la actualización del plan de tratamiento de riesgos.

INSOR garantizará que el proceso de auditoría se integre dentro de su sistema de gestión institucional, asegurando su periodicidad, trazabilidad y seguimiento. La programación y ejecución de las auditorías deberá tener en cuenta los criterios de criticidad, riesgos identificados, cambios relevantes en la operación o en el entorno tecnológico, así como los incidentes que hayan impactado la seguridad de la información.

CONTROL DE CAMBIOS		
Versión	**Cambio**	**Fecha y acta de aprobación**
01	Documento nuevo	25 /11/2016
02	Se incluyeron nuevas políticas de seguridad y se actualizó el contenido del manual de	06/08/2018

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.

	conformidad con las directrices del decreto 1008 de 2018.	
03	Se actualiza el documento alineado con la política institucional actualizada, la nueva versión de ISO 27001:2022 a nivel de controles y Resolución 02277: Del 03 de Junio de 2025. Actualización del Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia. Adicionalmente se incorpora: • Ajustes en roles y responsabilidades de usuarios, informática y responsable de seguridad. • Fortalecimiento de controles sobre uso de correo electrónico, redes inalámbricas y respaldos. • Revisión y mejora en redacción de políticas clave del numeral 9 (accesos, activos, incidentes, cumplimiento, etc.). • Claridad terminológica y adecuación al lenguaje institucional.	

Elaboró	Abello Abogados S.A.S.	**Revisó:**	Rosa Moncada Magda Yusef Rojas	**Aprobó:**	Comité de Gestión y Desempeño	**Aprobó Publicación:**	Carolina Ramos
Car go:	Contratista	**Cargo:**	Profesional Especializado Contratista OAPyS	**Cargo:**		**Cargo:**	Jefe Oficina de Planeación y Sistemas

Este documento es propiedad del Instituto Nacional para Sordos, prohibida su reproducción sin previo aviso.