TABLA CONTENIDO

Objetivo

Impartir recomendaciones sobre normas y buenas prácticas de la Seguridad de la Información para establecer, implementar, mejorar continuamente e innovar el Sistema de Gestión de Seguridad de la Información SGSI del Instituto Nacional Penitenciario y Carcelario.

Marco Legal

• Ver normograma del Instituto Nacional Penitenciario y Carcelario .

Glosario

- **Acuerdo de confidencialidad:** documento en que los servidores públicos o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información del instituto, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tenga acceso en virtud de la labor que desarrollan dentro de la misma

- **Antivirus:** software de seguridad que protege un equipo de virus, a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus.

- **Aplicación:** tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

- **Autenticación:** procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

- **Base de datos:** bancos de información que contienen datos, herramienta para recopilar y organizar información.

- **BCP:** Plan de Continuidad de Tecnología de Información, es un documento que describe cómo seguirá funcionando un negocio durante una interrupción no planificada del servicio.

- **BIA:** por sus siglas en inglés Bussiness Impact Analysis, (Análisis de Impacto del Negocio), permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

- **Caballo de troya:** código malicioso que parece ser algo que no es. Causando pérdida y robo de datos.

- **Código Fuente:** en informática, se denomina código fuente al conjunto de líneas de texto que expresan, en un lenguaje de programación determinado, los pasos que debe seguir el computador para la correcta ejecución de un programa específico.

- **Concienciación:** pautas que debe seguir todo el personal para ser considerado consciente de los requisitos de la seguridad de la información.

- **Datos personales:** Cualquier información de las personas, que tengan carácter privado, ligadas a su intimidad y que toque temas susceptibles de discriminación, como orientación sexual, religiosa, étnica, entre otros.

- **Cifrado:** método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

- **Confidencialidad:** condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. Capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

- **Control de acceso:** se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.

- **Copia de seguridad o respaldo (Backup):** duplicado de información que suele guardarse en un sitio lógico y/o físico distinto de aquel en el cual reside la información original. La importancia de tener copias de seguridad radica en poder recuperar la información de forma íntegra frente a una contingencia.

- **Dark Web:** red de datos de Internet Oscura que intencionalmente se oculta a los motores de búsqueda como Google, Baidu, Yahoo, entre otros.

- **Deep Web:** red de datos de internet profunda o invisible cuyo contenido público online no es rastreado ni encontrado por un usuario convencional.

- **Derechos de autor:** conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

- **Desmagnetización**: método válido para la destrucción de datos de los dispositivos magnéticos, como, por ejemplo, discos duros, cintas, magnéticas de backup, entre otros.

- **Disponibilidad:** garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

- **ERON:** Establecimiento de Reclusión del Orden Nacional.

- **Firewall:** aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

- **Gusanos:** programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

- **Hacking:** búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

- **Incidente de Seguridad:** se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información.

- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de la Integridad se presenta cuando un empleado, programa o proceso por accidente o con mala intención, modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por el personal autorizado; y esta modificación será registrada, asegurando su precisión y confiabilidad.

- **ISOlucion:** herramienta integral que facilita la planeación, implantación, automatización, administración y mantenimiento de la información asociada al Sistema de Gestión Integrado.

- **Licencia de software:** contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

- **Malware:** descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.

- **MSPI**: Modelo de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos.

- **No repudio:** sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto.

- **Partes interesadas**: las partes interesadas según la norma ISO/IEC 27001, en una organización típica son, entre otras: empleados, clientes, proveedores, socios, contratistas, entidades gubernamentales con autoridad regulatoria, entre otros.

- **Perfiles de usuario:** opciones de configuración que hacen que el equipo tenga el aspecto y funcione de la manera que usted desee. Contiene la configuración para fondos de escritorio, protectores de pantalla, preferencias de puntero, configuración de sonido y otras características. Los perfiles de usuario permiten que se usen sus preferencias personales siempre que inicie sesión.

- **Phishing:** es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

- **Política de seguridad:** documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/27001:2005) intención y dirección general expresada formalmente por la Dirección.

- **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.

- **Servidor público:** funcionario que se encuentra vinculado a la planta global del INPEC ya sea por carrera administrativa, nombramiento en provisionalidad, orden de prestación de servicios, libre nombramiento y remoción.

- **SSL:** acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas.

- **Responsable por el activo de información:** persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- **TI:**Tecnología de la información.

- **Titular:** servidor penitenciario cuyos datos son objeto del tratamiento de la información

- **Token de Seguridad:** (También Token de autenticación o Token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

- **TRD:** Tablas de Retención Documental.

- **Usuario de la información** persona, grupo o entidad que utiliza la información o los servicios de información.

- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad. No repudio y fiabilidad.

- **SGSI**: Sistema de Gestión de Seguridad de la Información.

- **Spam:** también conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios, generalmente se utilizan como un método de propagación de los ataques de phishing.

- **VGA:** Video Graphics Array (VGA) o Adaptador Gráfico de Video se utiliza para denominar a: Una pantalla estándar analógica de computadora.

- **VPN:** red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

- **Virus:** programa informático escrito para alterar de forma intencional la forma como funciona un computador, sin permiso o conocimiento del usuario.

- **Vulnerabilidad:** son todas aquellas debilidades que se están presentando en el sistema, lo cual hace susceptible de ser afectado, alterado o destruido por alguna circunstancia indeseada, que afectan al funcionamiento normal o previsto de dicho sistema informático.

1. Generalidades

La Guía de normas y buenas prácticas de seguridad de la información, es un documento enfocado al cumplimiento de los requisitos y lineamientos del Modelo de Seguridad y Privacidad de la Información **MSPI** de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia; construido para implementar, mejorar continuamente e innovar la seguridad de la información que suministra la orientación, recomendaciones y herramientas, que permiten la construcción de una cultura de Seguridad de la Información al interior del Instituto.

2. Compromiso de la Dirección General

La Dirección General del Instituto Nacional Penitenciario y Carcelario aprueba esta guía de buenas prácticas del Sistema de Gestión de Seguridad de la Información, como muestra de su liderazgo, compromiso y apoyo en el diseño y ejecución de estrategias eficientes, que garantizan la seguridad de la información en la entidad a través de la promoción activa de una cultura de seguridad, protección de los recursos adecuados para realizar y mantener dichas estrategias, tomando decisiones sobre las oportunidades de mejora encontradas en el sistema, para así aplicar las medidas necesarias en el manejo de los riesgos que puedan afectar negativamente el cumplimiento de la misión y los objetivos estratégicos del INPEC.

3. Organización de seguridad de la información

El INPEC en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información, SGSI, crea un esquema de seguridad de la información estableciendo roles y responsabilidades que involucran actividades de operación, gestión y administración de la seguridad de la información a través de la **PA-TI-G08 Guía Roles y Responsabilidades para la Seguridad de la Información** versión oficial.

4. Uso de dispositivos móviles Institucionales

Adoptar y tomar medidas de seguridad de la información en el uso de dispositivos móviles Institucionales, (teléfonos móviles, teléfonos inteligentes "smart phones", tablets entre otros), suministrados por el INPEC.

1. El Grupo de Manejo Bienes Muebles, realizará la entrega y cargará al inventario respectivo de cada servidor público los dispositivos móviles Institucionales; adquiriendo responsabilidad el servidor público sobre el elemento asignado.

2. El Grupo Administración de las Tecnologías realizará la distribución de los dispositivos móviles a cada dirección, oficina establecimiento o regional según sea su necesidad y establecerá las configuraciones aceptables para los dichos dispositivos Institucionales.

3. Para el nivel directivo se autoriza el uso de WhatsApp, no se permite por esta aplicación, el envío de fotografías, audios, videos y cualquier otro tipo de archivo clasificados como **información pública reservada o información pública clasificada (privada o semiprivada) de la Institución.**

Los usuarios no están autorizados a:

1. Cambiar la configuración, instalar, desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

2. Tomar fotografías, grabar audios y videos de la información clasificada como información pública reservada o información pública clasificada (privada o semiprivada) propiedad del Instituto.

3. Utilizar los equipos móviles en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos, modificar las configuraciones de seguridad

4. Hacer uso de redes inalámbricas de uso público

5. Almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

5. Seguridad de los recursos humanos

El INPEC reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con personal competente y calificado, garantizará que la vinculación de nuevos servidores públicos en las modalidades de libre nombramiento y remoción, provisionalidad o por orden de prestación de servicios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los servidores en sus cargos.

El Grupo Administración de Talento Humano debe, antes de asumir el empleo el aspirante:

1. Verificar antecedentes de los candidatos a un empleo de acuerdo con leyes y normas establecidas por la entidad y el gobierno.

2. La verificación debe tener en cuenta la privacidad pertinente a la protección de datos personales dentro de los cuales debe considerar:

    - Confirmación de certificados académicos y profesionales declarados
    - Verificación de identidad
    - Ratificación y veracidad de la hoja de vida del aspirante al empleo
    - Validación de referencias.

Al momento de la vinculación del aspirante al empleo, le debe informar:

1. Sobre las responsabilidades que tienen frente al Sistema de Gestión de Seguridad de la Información.

2. Al presentarse ante el jefe inmediato asignado, deberá diligenciar y firmar el formato **PA-TI-G02 Acuerdo de confidencialidad y compromiso con la seguridad de la información** versión oficial,

antes de tener acceso a la información digital o física del Instituto, como a los sistemas de información y/o aplicaciones. Formato el cual debe ser entregado al Grupo Administración de Historias Laborales cuando la vinculación sea en la modalidad de libre nombramiento y remoción o provisionalidad.

El Grupo de contratos, recibirá y archivará en los contratos de prestación de servicios el formato **PA-TI-G02-F01 Acuerdo de confidencialidad y compromiso con la seguridad de la información** versión oficial debidamente diligenciado por el contratista.

Terminación y/o cambio de empleo

1. El servidor público debe entregar los activos de información de acuerdo al **PA-TH-P28 Procedimiento para la entrega del puesto de trabajo** versión oficial.

El personal provisto por terceras partes que realicen labores en o para el INPEC, deben firmar el **PA-TI-G02-F01 Acuerdo de Confidencialidad y Compromiso con la Información** versión oficial, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica y dar cumplimiento a la **PA-TI-PL01 Política de Seguridad de la Información** versión oficial y a la presente guía.

6. Concienciación en seguridad de la información

La concienciación en seguridad de la información es básica para el éxito de un Sistema de Gestión de Seguridad de la Información SGSI. Por ello es necesario involucrar a los servidores públicos, auxiliares del cuerpo de custodia, judicantes, pasantes, practicantes y todo aquel que tenga un vínculo con el INPEC con el objetivo de crear Cultura de Seguridad de la información al interior de la Entidad que servirá para establecer bases de protección, tanto de la información confidencial del Instituto como la de los clientes y proveedores, supervisando que se cumplen las buenas prácticas en seguridad establecidas; realizando acciones de sensibilización y concienciación en seguridad de manera continua.

Todo el personal del Instituto debe conocer y aplicar políticas y controles de seguridad de la información ya que como usuarios finales son los que gestionan, procesan, almacenan y transfieren información utilizando medios físicos, digitales (sistemas de información) y verbales.

1. El Grupo de Proyección, Seguridad e Implementación Tecnológica planea, ejecuta y orienta los planes de sensibilización y concienciación en seguridad de la información al interior del Instituto con el apoyo del responsable de seguridad designado y lo líderes de procesos o dependencias. Al finalizar la concienciación, sensibilización, cursos, talleres, charlas de seguridad de la información entre otros se puede llevar a cabo una valoración de la comprensión de los usuarios finales para poner a prueba la transferencia del conocimiento.

2. A través de la guía **PA-TI-G08 Roles y Responsabilidades para la Seguridad de la Información** versión oficial, en su numeral 1.13 ítem 3; la Subdirección de Talento Humano tiene la responsabilidad de: Definir, desarrollar e implementar en la inducción y reinducción sensibilización y/o concienciación en cultura de seguridad de la información, para los servidores públicos.

3. La Subdirección Gestión Contractual, debe incluir acuerdos de confidencialidad en los contratos de prestación de servicios con el fin de proteger la confidencialidad de la información del Instituto, así mismo el Grupo de contratos, recibirá y archivará en los contratos de prestación de servicios el **PA-TI-G02 Acuerdo de confidencialidad y compromiso con la seguridad de la información** version oficial, debidamente diligenciado por el contratista.

4. La Dirección Escuela de Formación facilita los mecanismos necesarios para la sensibilización y/o concienciación en seguridad de la información en el Instituto. Guía **PA-TI-G08 Roles y Responsabilidades para la Seguridad de la Información** versión oficial, en su numeral 1.10

5. La Oficina Asesora de Comunicaciones debe apoyar y asesorar al responsable de seguridad de la información de la Entidad en el diseño y edición de vídeos, fondos de pantallas, personaje, eslogan, folletos, afiches y todos aquellos artes visuales y auditivos en relación con la sensibilización en Seguridad de la Información. Guía **PA-TI-G08 Roles y Responsabilidades para la Seguridad de la Información** versión oficial, en su numeral 1.5 ítem 1.

Responsabilidad de los usuarios:

1. Los Servidores Públicos, auxiliares del Cuerpo de Custodia, contratistas, subcontratistas, judicantes, pasantes, practicantes del INPEC tiene el deber de asistir a las sensibilizaciones y capacitaciones del SGSI cuando sean previamente citados.

2. Cuando los usuarios reciban las sesiones de sensibilización se llevarán registros de calidad y controles sobre la participación a través de los formatos **PA-DO-G01-F07 Asistencia a evento** versión oficial o **PA-DO-G01-F01 Acta** versión oficial (se pueden incluir registros fotográficos); con el propósito de que los servidores públicos, contratistas, judicantes, practicantes y todos aquellos que participen de las concienciaciones en seguridad asuman sus respectivos compromisos con la preservación de la seguridad de la información en la Entidad. Esta evidencia puede servir para justificar algún tipo de sanción a comportamientos inadecuados o incumplimiento al Sistema de Gestión de Seguridad de la Información SGSI Institucional.

3. Todo personal externo que desarrolle labores al interior del Instituto; debe contribuir al cumplimiento del Sistema de Gestión de Seguridad de la Información disponible en la web e intranet Institucional, observando sus directrices y colaborando en su aplicación dentro del ámbito de actuación de cada uno.

7. Gestión de activos

Una adecuada gestión de activos garantiza que los activos de la información reciban un apropiado nivel de protección.

El Instituto como propietario de la información física así como de la información generada, procesada, recopilada y transferida a través de su plataforma tecnológica, asignará responsabilidades a las oficinas, dependencias, establecimientos y demás sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

Responsabilidad del Grupo de Manejo de Bienes e Inmuebles:

1. Debe llevar a cabo el levantamiento y la actualización permanente del inventario de activos físicos al interior de Instituto, asignando un custodio, propietario o administrador con responsabilidades de protección de los activos.

Responsabilidad de la Oficina de Sistemas de Información:

1. Los activos de información correspondientes a la plataforma tecnológica del Instituto y, en consecuencia, debe asegurar su apropiada configuración, operación y administración, con el fin de preservar la confidencialidad, disponibilidad e integridad de la información.

2. Generar copias de seguridad de los aplicativos misionales, estratégicos y de apoyo del Instituto

3. Los activos de información de TI deben estar clasificados según la sensibilidad y criticidad de la información que contienen, de acuerdo a la Guía **PA-TI-G06 Inventario de Activos de la Información de las TIC** y el formato **PA-TI-G06-F01 Inventario de Activos de la Información de las TIC** en sus versiones oficiales, en la cual se describe la metodología que permite identificar, valorar y clasificar los activos de información, servicios, medios de procesamiento que soportan la gestión de los procesos y establecer su nivel de clasificación de acuerdo con las escalas contenidas en la misma.

Responsabilidad de los usuarios y/o administradores:

1. Son responsables de la información física como digital, del manejo de sistemas de información asignados o servicios tecnológicos tales como computadores, equipos portátiles, servidores, equipos de seguridad electrónica, fotocopiadoras, escáner, impresoras, internet, redes, correo electrónico, aplicaciones, herramientas de acceso remoto, teléfonos, dispositivos móviles, video beam entre otros, estos activos **son propiedad del Instituto** y son suministrados a los servidores públicos y terceros para cumplir con la misión del Instituto, deben emplearse exclusivamente con propósitos laborales de tal forma que se mantengan los niveles de protección durante el ciclo de vida de la información.

2. Deben realizar la devolución de los activos a su cargo en caso de terminación del empleo o traslado, de acuerdo al **PA-TH-P28 Procedimiento para la entrega del puesto de trabajo** versión oficial.

Responsabilidad de las dependencias:

1. Para la adquisición de equipos informáticos, software, hardware o tecnología debe contar con el visto bueno en la ficha técnica de la Oficina de Sistemas de Información.

2. Cada dueño de proceso debe controlar el copiado no autorizado de la información, cuando exista una desvinculación definitiva o traslado de un empleado ya que la información almacenada en los activos de información son propiedad del INPEC.

Los recursos informáticos del INPEC no podrán ser utilizados, para divulgar, propagar, almacenar contenido personal o comercial de publicidad, promociones, organizaciones, ofertas, promesas, programas destructivos (malware), propaganda política, material religioso o cualquier otro que no esté autorizado.

Los usuarios de partes externas que usen activos de la entidad, deben tomar conciencia de los requisitos de seguridad de la información de los activos asociados con la información y recursos de procesamiento de información y de cualquier uso ejecutado bajo su responsabilidad.

8. Clasificación de la información

El INPEC consiente de la necesidad de asegurar y clasificar la información en función de la confidencialidad, integridad, disponibilidad, requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada; establece a través de la guía **PA-TI-G08 Roles y Responsabilidades para la Seguridad de la Información** versión oficial, las responsabilidades del Grupo de Gestión Documental en su numeral 1.11. el cual lidera y define las reglas o lineamientos de como clasificar la información a través de la guía **PA-DO-G02 Guía para la Elaboración del Inventario de Activos de Información** versión oficial, y el formato **PA-DO-G02-F01 Inventario de Activos de Información versión oficial** teniendo en cuenta:

1. Las fuentes de información como insumo principal tomando las TRD actualizadas de la entidad. Si las fuentes de información no han sido identificadas, la mejor fuente de información son los jefes de dependencias, los administradores de sistemas de información o tecnología y los usuarios finales del INPEC.

2. El resultado de la fuente de información debe producir una descripción de:

    - El idioma en el que se encuentra la información

    - Medio de conservación o soporte (Físico, electrónico o digital), formato (papel, word, excel, pdf, otros).

    - Información publicada o disponible, lugar de consulta donde se puede acceder a la información.

    - Nombre del responsable de la producción de información, (quienes son los custodios de los datos, por ejemplo: servidores públicos, se debe enunciar el cargo más no el nombre)

    - Niveles de clasificación de la información, ejemplo: reservada, clasificada o pública.

- Validación de las medidas de protección asociadas con los niveles de clasificación de la información apropiadas para las fuentes de datos. (autenticación, controles administrativos, cifrado de datos, entre otros) según corresponda con el apoyo de lo Oficina de Sistemas de Información.

La clasificación de la información debe ser consistente, clara y coherente para toda la Institución, los resultados de los niveles de clasificación se deben actualizar dependiendo de su sensibilidad y criticidad durante el ciclo de vida de la información. La información física y digital del INPEC debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las Tablas de Retención Documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

Etiquetado de la información:

Se recomienda al Grupo de Gestion Documental que dentro del **PA-DO-M01 Manual de Gestión Documental**, versión oficial, se incluya el etiquetado de la información, de acuerdo con el esquema de clasificación de información que adoptado el Instituto teniendo en cuenta:

1. Los procedimientos para el etiquetado de la información deben abarcar los formatos físicos y electrónicos.

2. Las etiquetas se deben reconocer fácilmente.

3. Orientación acerca de dónde y cómo se colocan las etiquetas.

4. Seguir lineamientos Guía No. 5 Guía para la Gestión y Clasificación de Activos de Información, numeral 7.4 Etiquetado de Activos de Información, de MINITC.

Responsabilidad de la Oficina de Sistemas de Información:

1. Proveer las herramientas tecnológicas para el respectivo almacenamiento de la información, con medidas de protección de criptografía entre otros.

Responsabilidad de los usuarios:

1. Deben verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras para asegurarse que no queden documentos en los dispositivos y así evitar su divulgación no autorizada.

2. Está prohibido la toma de fotografías y videos a documentos propiedad de la entidad, sin previa autorización.

3. El dueño de la información es el único responsable de su protección.

4. Sea precavido en el transporte y almacenamiento de la información, tanto a nivel digital como físico.

5. Proteja la información de la Institución incluso fuera del ámbito de la entidad.

6. La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y condiciones adecuadas de almacenamiento y resguardo.

9. Manejo de activos

La Oficina de Sistemas de información desarrolla e implementa procedimientos para el manejo de activos TI, con el objetivo de minimizar el riesgo de fuga de información confidencial a personas no autorizadas, considerando las siguientes recomendaciones:

1. Los medios y equipos donde se almacena, procesan o comunican la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

2. Para conservar la integridad y confidencialidad de la información, se deben utilizar procedimientos y técnicas criptográficas; dependiendo de la criticidad de la información que circula a través de la red o la que se encuentre alojada en un dispositivo o sistema determinado.

3. Desarrollar e implementar un procedimiento de borrado seguro para los equipos de cómputo y demás dispositivos tecnológicos que almacenen información, una vez se realice su devolución al Grupo de Manejo de Bienes Muebles para dar de baja o para aquellos dispositivos que se reutilicen, usando métodos como: desmagnetización, destrucción física, sobre-escritura entre otros, teniendo en cuenta ventajas e inconvenientes de los métodos de borrado seguro, como cumplimientos legales.

4. Los dispositivos de almacenamiento dañados que contengan datos sensibles deben requerir una valoración de riesgos para determinar si los elementos se deberían destruir físicamente o enviarlos a reparación.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la Oficina de Sistemas de Información autorizada por los jefes de dependencia y será objeto de auditorías de seguridad mediante el software de PC SECURITY.

10. Seguridad en relación al acceso de sistemas de información y aplicaciones por partes interesadas

El INPEC establece mecanismos de vigilancia en relación al acceso de sistemas de información y aplicaciones por partes internas como externas; con el propósito de asegurar que la información que es consultada cumpla con las normas y operaciones de seguridad de la información.

Responsabilidades de la Oficina de Sistemas de Información:

1. Clasificar la información para la asignación de roles y privilegios de los sistemas de información y aplicaciones.

2. Llevar un listado de usuarios con sus correspondientes privilegios y derechos que se deberá revisar de forma periódica para mantenerlo actualizado, controlando la autorización, concesión o revocación de privilegios.

3. Controlar los permisos y privilegios de usuario (lectura, escritura, borrar y modificar).

4. Documentar los procedimientos de ingreso seguro a los sistemas de información y aplicaciones para minimizar la oportunidad de acceso no autorizado.

5. Llevar un registro de intentos exitosos y fallidos de acceso a los sistemas de información y aplicaciones, fecha y hora.

6. Terminar sesiones inactivas de los sistemas de información y aplicaciones después de un tiempo de inactividad definida.

7. Restringir tiempos de conexión para brindar seguridad adicional para los sistemas de información y aplicaciones de alto riesgo, reduciendo oportunidad de acceso no autorizado.

8. Forzar a los sistemas de información para que los usuarios cambien sus contraseñas cuando ingresen por primera vez.

9. Exigir a los usuarios que cambien las contraseñas en forma regular.

10. Exigir a los usuarios que escojan contraseñas seguras y de calidad.

11. Almacenar y transmitir contraseñas de forma protegida, garantiza que estas sean de calidad, que cumplan con el nivel requerido y se apliquen de manera consistente.

12. Establecer normas de conexión a la red de datos, apropiadas para los equipos de cómputo, como también verificar los medios de comunicación seguros, para la transmisión de información desde y hacia los proveedores de servicios.

13. Con el apoyo de la Oficina Asesora Jurídica, establecer acuerdos de confidencialidad y de intercambio de información con los que deben cumplir las partes externas o proveedores de servicios informáticos.

14. Asegurar que los usuarios o perfiles de usuario que tienen asignados por defecto diferentes recursos de la plataforma tecnológica sean habilitados, inhabilitados o eliminados de los sistemas de información según reporte periódico enviado por la Subdirección de Talento Humano de los diferentes estados de los servidores públicos (vinculación, licencias, incapacidades entre otros).

15. Toda información, utilizada, manejada, tratada o consultada en los sistemas de información, aplicaciones o bases de datos del Instituto, por parte de personas y organizaciones públicas,

privadas, internas o externas, es propiedad del INPEC y por ningún motivo debe ser modificada, reformada o utilizada para fines fraudulentos.

16. En ningún caso se otorgará acceso a partes externas a las instalaciones de procesamiento, almacenamiento, tratamiento y transporte, sin previa autorización y en cumplimiento de la presente guía.

Responsabilidades de los usuarios:

1. Al momento de la vinculación, el servidor público o parte interesada deberá solicitar el acceso a los sistemas de información (previo a la firma de acuerdos de confidencialidad) según sus funciones y autorización del jefe inmediato, así mismo al momento de su desvinculación deberá solicitar la cancelación del acceso autorizado.

2. El servidor público al registrarse en los diferentes sistemas de información del Instituto, como correo electrónico, Intranet, SISIPEC, Sistema de ingreso y salida, desprendible de pago, entre otros; le permite realizar sus labores de manera efectiva y eficiente presentando la información en tiempo real.

3. Cada usuario es responsable por sus acciones mientras utilice cualquier recurso de Información del Instituto, por lo tanto, la identidad de cada usuario de los recursos de información está establecida de una manera única. Esta identidad de ninguna manera o por ninguna circunstancia podrá ser compartida. No seguir esta recomendación será una infracción a la seguridad de la información.

4. Cada supervisor de contrato deberá consolidar en un informe un listado de los contratistas que por diversas circunstancias ya no laboren al interior del Instituto, remitiéndolo a la Oficina Sistemas de Información para el control a los Sistemas de Información.

5. Una vez finalizado el vínculo laboral del usuario con la entidad, por solicitud del jefe inmediato o supervisor del contrato, según sea el caso, se debe bloquear el acceso al equipo de cómputo donde desarrollaba las actividades el usuario, solicitud dirigido a la Oficina Sistemas de Información, con el objetivo de evitar la exposición de la información y el acceso a terceros que puedan generar suplantación, deterioro, alteración, perdida o uso indebido de la información.

6. Los servidores públicos deben realizar la devolución de las herramientas de trabajo que tienen bajo su responsabilidad una vez cese la relación con la entidad o cuando existan traslados por necesidades del servicio, entrega que se hará de acuerdo al procedimiento **PA-TH-P28 Procedimiento para la entrega del puesto de trabajo** versión oficial.

11. Seguridad en relación al acceso a códigos fuente de programas

La Oficina de Sistemas de Información, como responsable de la administración de los sistemas de información, aplicativos, bases de datos y códigos fuente, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los programadores internos como externos, acojan buenas prácticas de desarrollo en los sistemas generados, para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Se deben considerar las siguientes directrices:

1. Controlar estrictamente el acceso a los códigos fuente de programas y elementos asociados (tales como diseño, especificaciones, planes de verificación y de validación) con el fin de evitar cambios involuntarios o no autorizados y mantener la confidencialidad de propiedad intelectual.

2. La entrega de códigos fuente, librerías de programas y elementos asociados, a los desarrolladores o programadores solo se debe hacer una vez hayan firmado los acuerdos de confidencialidad y compromiso con la seguridad de la información.

3. Se debe conservar registro de auditoría de accesos, desarrollo, actualización y/o modificación del código fuente y librerías de programas.

4. El mantenimiento y copia de las bibliotecas de fuentes de programas deben estar sujetos a procedimientos estrictos de control de cambios.

5. Proteger y ser objeto de inscripción en el Registro de la Propiedad Intelectual el software, desarrollo y/o código fuente propiedad de INPEC, con el objetivo de otorgar seguridad jurídica a su titular respecto de sus derechos de autor.

6. Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

12. Controles criptográficos y gestión de claves

La Oficina de Sistemas de Información asegura el uso apropiado y eficaz de la criptografía y gestión de llaves para proteger la confidencialidad, autenticidad y/o integridad de la información.

En los siguientes casos se debe considerar controles criptográficos:

1. Cumplimiento de todos los acuerdos, legislación y reglamentación criptográfica pertinente al Estado Colombiano con el apoyo y asesoramiento de la Oficina Asesora Jurídica.

2. Análisis previo que determine claramente que datos de la Institución se deben cifrar con el apoyo de las diferentes dependencias de la Institución y que situaciones o usuarios requieren de firma digital para verificar la autenticidad o integridad de la información almacenada o transmitida.

3. Protección de la información, clasificada como reservada, sensible, critica o restringida, al momento de almacenarse y/o transmitirse por cualquier medio tecnológico, con el propósito de proteger su confidencialidad e integridad

4. Protección de contraseñas de acceso a sistemas de información y demás servicios que requieran autenticación.

5. Uso de correo electrónico institucional, vía web.

6. Uso de información en dispositivos móviles corporativos.

7. Establecer e implementar certificados SSL (Secure Sockets Layer) y los que hubiere en el momento del avance en tecnología, para garantizar la transferencia y navegabilidad segura de datos en servicios web críticos. Garantiza la transferencia de datos a través canales cifrados (vía VPN o cifrando los datos antes de ser enviados).

8. Garantizar que las copias de seguridad en la nube de ficheros que contengan datos confidenciales o datos personales de empleados o clientes, sean cifradas.

9. Conexiones inalámbricas (Wifi) con protocolos seguros de encriptación para evitar que las comunicaciones puedan ser interceptadas fácilmente.

Gestión de claves criptográficas

1. Mantener activos y documentados los controles del ciclo de vida de las claves criptográficas en su generación, uso, almacenamiento, distribución, recuperación, retiro y destrucción de las mismas.

2. Determinar las fechas de activación y desactivación de claves con el objetivo de reducir riesgos de seguridad.

3. Proteger las claves criptográficas contra modificación, perdida, uso y divulgación no autorizada.

4. Realizar copias de respaldo de las llaves.

Cuando las claves públicas se emitan desde un proveedor externo, debe existir un "Acuerdo de nivel de servicio" para definir las responsabilidades del proveedor.

13. Seguridad física y del entorno

El INPEC proporcionará y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de las instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido. La aplicación de los controles físicos, se deben adaptar a las circunstancias técnicas y económicas de la Entidad y a la valoración de riesgos.

El Grupo Logístico debe garantizar:

1. La protección del perímetro de las instalaciones físicas donde laboran los servidores públicos, las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (por ejemplo: alarmas, cerraduras, cámaras, entre otros).

2. Las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión.

3. Un área de recepción con vigilancia para controlar el acceso físico a las edificaciones, únicamente al personal autorizado.

4. Las puertas contra incendio deben tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo a las normas nacionales e internacionales, con el apoyo de la brigada de emergencia institucional.

5. Registro de los visitantes de la fecha y hora de entrada y salida de las instalaciones Institucionales, se debe otorgar acceso para propósitos específicos autorizados y supervisados. Las identidades de los visitantes se deben autenticar por medios apropiados, teniendo en cuenta la Ley 1582 de 2012 protección de datos personales, con apoyo de los medios tecnológicos de la Oficina de Sistemas de Información.

6. Los visitantes deben portar algún tipo de identificación visible (strikes, fichas, entre otros), los servidores públicos deben informar de inmediato al personal de seguridad si se encuentran visitantes no acompañados y sin identificación visible.

7. No se debe permitir ingreso de equipo fotográfico, de video, audio, u otro equipo de grabación a los visitantes, a menos que se cuente con autorización para ello.

8. Controlar los puntos de acceso de despacho y descarga, donde pueden entrar personas no autorizadas, actividad que también es responsabilidad del Grupo de Manejo de Bienes Muebles.

9. El material que ingresa se debe examinar para determinar presencia de explosivos, químicos u otros materiales peligrosos, antes que se retiren del área de despacho y carga, actividad que también es responsabilidad del Grupo de Manejo de Bienes Muebles.

La Oficina de Sistemas de Información debe garantizar:

1. Las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación o Establecimientos de Reclusión del Orden Nacional, deben velar porque los recursos de la plataforma tecnológica del Instituto ubicados en centros de cómputo o centros de cableado (donde existan) se encuentren protegidos contra ingresos no autorizados, fallas o interrupciones eléctricas.

2. Las áreas restringidas respecto a los sistemas de la información se protegerán mediante el empleo de controles de acceso físico y lógico, los que serán determinados por la Oficina de Sistemas de Información, a fin de permitir el acceso sólo al personal autorizado.

3. Asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, como de equipos de cómputo o servidores sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos y correctivos.

Responsabilidades:

1. Los servidores públicos, judicantes, practicantes, pasantes (mayores de 18 años), auxiliares del cuerpo de custodia y contratistas que se encuentren en las instalaciones físicas del Instituto deben

registrarse en el sistema de ingreso y salida según sea el caso y portar el carné en un lugar visible que los identifica como empleados, judicantes, practicantes o pasantes; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible a las autoridades competentes (realizar el trámite correspondiente, es necesario el denuncio y demás trámites) y notificar a la Subdirección de Talento Humano.

2. El carné institucional es personal e intransferible.

3. El uso indebido del carné Institucional se sancionará de acuerdo con las normas legales y reglamentarias vigentes.

4. El personal de empresas contratistas que desempeñen funciones en el Instituto; deben estar identificados con carné, chalecos o distintivos y acompañados por servidores públicos y a cargo de los supervisores del contrato.

14. Seguridad en el cableado

Con el objetivo de la protección y seguridad del cableado estructurado del Instituto contra interceptación, interferencia, o daño, la Oficina de Sistemas de Información con el apoyo de las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación o Establecimientos de Reclusión del Orden Nacional, deben ejecutar las siguientes directrices:

1. Velar por la protección del acceso lógico y físico a los puertos de configuración y diagnóstico de los equipos de red y demás que sean considerados como críticos.

2. Los cables de potencia deben de estar separados de cables de comunicaciones para evitar interferencia.

3. Controlar el acceso a los paneles de conexión y recintos de cables, como el uso de blindaje electromagnético para proteger los cables.

4. Controlar y monitorear el acceso a los gabinetes rack destinados a alojar equipamiento electrónico, informático y de comunicaciones solo a personal autorizado por el responsable encargado.

5. Asegurar el almacenamiento y la debida protección de las llaves de los gabinetes rack.

6. Los patch panels deben estar identificados en cada uno de sus puertos en la parte frontal.

7. Mantener y actualizar cuando sea necesario los planes o diagramas físicos o digitales de la red de datos lógica como física con sus respectivos componentes.

8. La información relacionada con la red de datos, el direccionamiento interno, así como las configuraciones y demás datos relacionados con las redes y sistemas de comunicación de la entidad, deberá ser confidencial y estará bajo la responsabilidad del Grupo de la Administración de las Tecnologías.

9. Asegurar que las redes inalámbricas del Instituto cuenten con métodos de autenticación que evite accesos no autorizados.

10. Velar por el mantenimiento preventivo de los equipos que conforman el cableado estructurado para asegurar su disponibilidad e integridad continua.

11. Gestionar e inspeccionar la red de datos para proteger la información en los sistemas y aplicaciones.

Responsabilidad de los usuarios:

1. Los usuarios deben emplear los puntos de red, para la conexión de equipos informáticos autorizados por el Instituto.

2. Los equipos de uso personal, que no son de propiedad del Instituto, no deben ser conectados a la red de datos, sin previa autorización por la Oficina Sistemas de Información o las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación o Establecimientos de Reclusión del Orden Nacional, según sea el caso.

3. La instalación, activación y gestión de los puntos de red es responsabilidad de la Oficina Sistemas de Información, áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación o Establecimientos de Reclusión del Orden Nacional.

4. El uso de módems no autorizados o soluciones de acceso remoto no aprobadas está prohibido y es una infracción a la seguridad de la información del Instituto.

5. La red de energía regulada de los puestos de trabajo no se debe sobrecargar con instalaciones eléctricas tales como secadores, planchas de peinar, hornos microondas y todo elemento que sea ajeno a su desempeño laboral. Recuerde que las conexiones múltiples pueden producir sobrecalentamientos y fallas eléctricas.

6. No bloquear los puntos de red de datos y eléctricos con carpetas, cajas y escritorios, entre otros.

7. Cuando se detecte un uso no adecuado de la red por favor, informe inmediatamente a la Oficina de Sistemas de Información.

15. Gestión de acceso de usuarios a los sistemas de información y conexiones de red

La Oficina de Sistemas de Información establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información del instituto.

1. Establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información del Instituto, que contemple la creación, activación, modificación, bloqueo o eliminación de las cuentas de usuario.

2. Definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica del Instituto, los servicios de red y los sistemas de información; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo

por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

3. Asegurar la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los servidores públicos se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo, con base en informe periódico enviado desde la Subdirección de Talento Humano.

4. El control de acceso a los sistemas de información y conexión de red de datos debe ser concedido a los usuarios de acuerdo con lo que necesita saber, que necesita usar y hasta cuánto tiempo de acceso requieren.

5. Otorgar controles de acceso basado en roles.

Responsabilidad de los usuarios:

1. Los usuarios de los recursos tecnológicos y los sistemas de información del INPEC realizarán un uso adecuado y responsable de los mismos, salvaguardando la información a la cual les es permitido el acceso.

16. Seguridad Centro de Cómputo

Para garantizar la protección de los servicios de procesamiento, información y comunicaciones de una manera segura al interior del Instituto, la Oficina de Sistemas de Información y las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional (donde existan centro de cómputo) deben:

1. Desarrollar un plan de contingencia del centro de cómputo para garantizar la continuidad de las operaciones de los elementos críticos que componen los Sistemas de Información.

2. Implementar y velar por las integridades físicas externas e internas y control de acceso de los centros de cómputo (donde existan) asegurando la infraestructura y soporte a los sistemas de información y comunicaciones. Para así reducir los riesgos potenciales de modificación, destrucción, revelación de datos, programas e interrupciones.

3. Asegurar que los mantenimientos preventivos y/o correctivos de redes lógicas, eléctricas, servidores entre otros sean realizados por personal capacitado; así mismo, llevar control sobre los mantenimientos cuando sean necesarios programarlos.

4. Eliminar, bloquear o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un servidor autorizado.

5. Velar porque los controles y otros mecanismos de seguridad de acceso a las áreas solo sean utilizados por los servidores autorizados; salvo en situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran.

6. El administrador asignado al centro de cómputo principal y alterno debe llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados, para tener como referencia en futuras fallas y soluciones.

7. Se debe mantener un inventario físico de los equipos y accesorios existentes.

8. La oficina de Sistemas lidera el control de acceso a los centros de cómputo a través de un formato debidamente aprobado, en el cual se registren como mínimo los siguientes datos:

    - Fecha y hora de ingreso y salida
    - Nombre completo del usuario
    - Identificación
    - Dependencia, área o empresa externa
    - Actividad a realizar
    - Firma

Responsabilidad de los usuarios autorizados:

1. Queda estrictamente prohibido sustraer equipos o materiales propiedad del centro de cómputo sin previa autorización por la oficina encargada.

2. Se prohíbe ingresar alimentos de cualquier tipo al centro de cómputo.

3. Las solicitudes de acceso al centro de cómputo deben ser aprobadas por el encargado de la Oficina Sistemas de Información o según corresponda en los establecimientos o regionales; no obstante, los visitantes siempre deberán estar acompañados de un servidor de dicha oficina durante su visita al centro de cómputo o los centros de cableado.

4. Respetar y seguir las instrucciones que en su momento le indique el responsable a cargo.

5. Se prohíbe mover, desconectar y/o conectar dispositivos tecnológicos dentro del centro de cómputo sin autorización.

6. Se prohíbe modificar la configuración de los equipos almacenados en el centro de cómputo sin autorización.

7. Se prohíbe la toma de fotografías y videos al interior de los centros de cómputo sin autorización.

8. Está prohibido alterar el software instalado en los equipos del centro de cómputo sin autorización.

9. Prohibido alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.

10. La limpieza y aseo del centro de cómputo debe efectuarse en presencia del responsable a cargo.

11. El personal de limpieza debe ser orientado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza por el responsable encargado.

12. Se prohíbe el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

17. Ubicación y protección de equipos

Para evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades del Instituto, se debe aplicar las siguientes normas y buenas practicas:

La Oficina de Sistemas de Información:

1. Lidera e implementa controles para la seguridad de equipos y activos tecnológicos fuera de las instalaciones de la Institución, tales como trabajo en casa o teletrabajo (si se llegare adaptar), según sea el caso determinando valoración del riesgo, estableciendo límites de tiempo para retiro y devolución de recursos tecnológicos.

2. El Grupo Administración de las Tecnologías de la Información, en conjunto con los Directores Regionales, Directores Establecimientos de Reclusión del Ordena Naciona ly los Jefes de Oficina y/o dependencia deben proveer los mecanismos para evitar la pérdida, daño, robo, riesgo de fuego, explosión, humo, agentes químicos o puesta en peligro de los activos y la interrupción de las actividades de la Entidad.

3. Atiende los soportes técnicos junto con las áreas de sistemas de las regionales y/o Establecimientos de Reclusión del Orden Nacional de una forma eficaz y oportuna con un tiempo de respuesta acorde a las solicitudes.

Responsabilidad de los usuarios:

1. Los Directores Regionales, Directores Establecimientos de Reclusión del Orden Nacional y Director Escuela de Formación son los únicos facultados para autorizar movimientos y asignaciones de recursos tecnológicos, previo visto bueno de la Oficina de Sistemas de Información; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier servidor de los recursos tecnológicos del Instituto ya sea para mantenimiento preventivo, correctivo o fines laborales y se debe garantizar que en dichos elementos no se encuentre información sensible para el Instituto.

2. Los equipos de cómputo deben ser transportados siempre y cuando se requiera con las medidas de seguridad apropiadas, que garanticen su integridad física, previa autorización de la Oficina de

Sistemas de Información, o según sea el caso los Directores de Establecimientos de Reclusión del Orden Nacional, Directores Regionales ó Director Escuela de Formación.

3. En caso de pérdida o robo de un equipo de cómputo del Instituto, se debe informar de manera inmediata con un oficio o correo electrónico dirigido al Grupo de Administración de las Tecnologías de la Información, para que se inicie el trámite interno y se debe instaurar denuncia ante la autoridad competente.

4. No tapar los orificios de ventilación de los equipos de cómputo. El calor es su peor enemigo.

5. Se prohíbe que los visitantes manipulen o manejen los equipos de cómputo del Instituto sin previa autorización del dueño, responsabilidad que recae sobre el servidor público propietario del equipo en el caso de fuga o sustracción de información, daño o pérdida de elementos.

6. No ingerir alimentos o bebidas sobre equipos informáticos, teclado o CPU.

7. Desconectar el teclado de forma repentina, mientras está conectado al CPU encendido podría hacer que funcione mal, o peor, dejarlo inoperativo, debido al cambio de voltaje.

8. No debe desconectar el monitor mientras la CPU esté encendida, ni retirarlo de la salida VGA de la tarjeta de video. Esto podría dañar tanto el monitor como la torre.

9. No coloque objetos magnéticos tales como teléfonos, parlantes grandes o imanes muy cerca de la torre, porque podría dañar alguno de sus pequeños componentes. Los parlantes normales están hechos para no repercutir en éste ámbito.

10. Apague correctamente la CPU, ya que, si queremos que el disco duro, dure lo suficiente, debemos evitar que este sea bruscamente apagado, se corre el riesgo de un inminente deterioro.

11. Para limpiar el equipo en su parte externa, debe usar un paño seco, franela de algodón para remover el polvo, siempre que éste se encuentre apagado.

12. Golpear o mojar el mouse puede dejarlo inservible, ya que contiene piezas muy pequeñas y propensas a dejar de operar, debido a que están prácticamente al descubierto.

13. No escuche música a través de los equipos de cómputo en horas laborales ya que puede interferir con la concentración y el buen desempeño laboral de los servidores públicos.

18. Mantenimiento de equipos de cómputo Institucionales

la Oficina de Sistemas de Información debe proveer los mecanismos y estrategias necesarios para el correcto mantenimiento preventivo y correctivo de los equipos de cómputo institucionales, por lo anterior debe considerar las siguientes directrices para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos:

1. Realizar los mantenimientos preventivos de acuerdo con los intervalos y especificaciones de servicios recomendados por el proveedor.

2. Solo el personal de mantenimiento autorizado debe llevar a cabo las reparaciones.

3. Llevar registro de todas las fallas y de todo el mantenimiento preventivo y correctivo.

4. Generar estándares de configuración segura para los equipos de cómputo de los servidores del Instituto y configurar dichos equipos acogiendo los estándares generados.

5. Generar y aplicar lineamientos o procedimientos para la disposición segura de los equipos de cómputo del instituto, ya sea cuando son dados de baja o cambian de usuario.

6. Previamente a la puesta de operación del equipo después del mantenimiento, se debe inspeccionar para asegurar que no ha sido alterado y que su funcionamiento es adecuado.

Responsabilidad de los usuarios:

1. La Oficina de Sistemas de Información y las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional, son los únicos autorizados para emitir conceptos, autorizar o realizar mantenimientos preventivos y correctivos; por consiguiente, se encuentra prohibida la manipulación en referencia a los mantenimientos de equipos de cómputo institucionales por parte de los usuarios.

2. Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad del INPEC el usuario responsable debe informar al Grupo Administración de las Tecnologías de la Información o a las áreas encargadas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional, según sea el caso, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

19. Uso de periféricos y medios de almacenamiento

Establecer técnicas para la utilización de periféricos y medios de almacenamiento para prevenir la pérdida destrucción o accesos no autorizados de la información.

La Oficina de Sistemas de Información debe:

1. Reglamentar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica del Instituto tales como USB, grabadora y/o lector de CD, grabadora y/o lector de DVD, grabadora y/o lector de HD-DVD, discos externos, micro memorias entre otros de acuerdo con los lineamientos y condiciones establecidas.

2. El Grupo Administración de la Tecnologías de la Información, debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica del Instituto de acuerdo con el perfil del cargo del servidor solicitante, con visto bueno de su jefe inmediato.

Responsabilidad de los usuarios y personal provisto por terceras partes:

1. Deben acatar las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Oficina de Sistemas de Información.

2. El personal autorizado para usar medios de almacenamiento se hace responsable y es custodio de la información que se almacene y de la protección de la misma.

3. Los servidores públicos y el personal provisto por terceras partes no deben cambiar o modificar la configuración de periféricos y medios de almacenamiento, no se debe utilizar medios de almacenamiento personales en la plataforma tecnológica propiedad del INPEC.

20. Uso de Token de seguridad

Para administrar la información de usuarios en el portal de información financiera en los cuales el Instituto realiza transacciones electrónicas, a través de la creación, activación, modificación, desactivación o eliminación de usuarios con roles de aprobador, preparador o de consulta y de la modificación de cuentas asociadas, para dar cumplimiento a las políticas de seguridad en el manejo de transacciones electrónicas, se debe tener en cuenta:

1. La Dirección Gestión Corporativa como administradora de los Token de seguridad deben procesar las solicitudes de dichos Token según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria.

Responsabilidad de los usuarios:

1. Recibir y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de los mismos.

2. Dar aviso al Grupo de Presupuesto en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.

3. Realizar el cambio de los Token, cuando presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la Dirección Gestión Corporativa Grupo Presupuesto y devolviendo los dispositivos asignados.

4. Los usuarios que requieren utilizar los Token de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de los mismos.

5. Devolver el Token asignado a la Dirección del establecimiento cuando el vínculo laboral con el Instituto del servidor se dé por terminado o haya cambio de cargo, el cual será requerido para legalizar la finalización del vínculo con el Instituto.

6. Tener en cuenta que el Token es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso. El usuario es el único responsable de su uso o manejo.

7. Responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como servidores públicos. En caso de que suceda algún evento irregular con los Token los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

8. Evitar el uso de los Token fuera de las instalaciones del INPEC para evitar pérdida o robo de estos, que terceras personas observen la clave que genera el Token, no utilizarlo como llavero con las llaves de su auto o casa, dejarlo en estacionamientos públicos u olvidados.

9. Mantener el Token en un lugar seguro, seco y alejado de altas temperaturas. No sumerja el Token en líquidos ni lo arroje al suelo, ya que esto podría ocasionar fallas en su funcionamiento.

10. No abrir el Token. Éste es un dispositivo de seguridad y al intentar abrirlo lo dañará de manera permanente.

11. Cerrar la sesión cuando termine de hacer sus transacciones.

12. Las empresas proveedoras de los Token deben entregar a los usuarios designados los seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de un acta para la custodia de los mismos.

21. Disposición segura o reutilización de dispositivos tecnológicos

Se deben verificar los dispositivos tecnológicos que contengan medios de almacenamiento, para garantizar que cualquier dato sensible o software con licencia se hayan retirado o sobrescrito de manera segura antes de su disposición o reutilización.

La Oficina de Sistemas de Información:

1. Genera y aplica lineamientos, guías o procedimientos para la disposición o reutilización segura de los dispositivos tecnológicos del instituto.

2. Para la reutilización de un dispositivo tecnológico se debe tener en cuenta el borrado seguro para los medios de almacenamiento que contengan información confidencial o protegida por derechos de autor, utilizando técnicas para que la información no sea recuperable (previa valoración y análisis de riesgo).

3. Los dispositivos dañados que contengan medios de almacenamiento pueden requerir una valoración de riesgos para determinar si los elementos se deberían destruir físicamente en lugar de enviar a reparación o desecharlos. La información se puede comprometer debido a una disposición descuidada o reutilización.

4. Las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional, deben acatar los lineamientos de la Oficina de Sistemas de Información.

22. Equipo informático de usuario desatendido

Los usuarios deben tomar conciencia de los requisitos de protección y seguridad de los equipos desatendidos, al igual que sus responsabilidades para la implementación de esa protección y evitar el acceso de usuarios no autorizados, la sustracción o la puesta en peligro de la información y de los servicios de procesamiento de información.

La Oficina de Sistemas de Información debe:

1. Programar un bloqueo automático de sesión en los equipos de cómputo institucionales al no detectarse actividad del usuario en un corto periodo de tiempo. Adicionalmente debe llevar a cabo la programación del apagado general de equipos una vez terminada la actividad laboral.

2. Exigir a los servidores las responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación con el uso y la seguridad del equipo del usuario.

Responsabilidad de los usuarios

1. Mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por la Oficina de Sistemas de Información, cuando no se encuentren en su lugar de trabajo. Para ello se recomienda presionar botón Windows del teclado + letra L. Al volver el usuario, el sistema solicitará nuevamente usuario y contraseña para ingresar al equipo.

2. Apagar su equipo de computo asignado al finalizar la jornada laboral.

3. Los equipos tecnológicos (computador, escáner, entre otros), serán utilizados sólo por el responsable asignado a ellos, y no por otro servidor público ajeno a la dependencia.

4. Toda información crítica deberá ser guardada en lugares seguros, archivadores bajo llave.

5. Clasificar y protege los objetos e información susceptible de pérdidas.

23. Escritorio despejado y pantalla despejada

Prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral, mediante lineamientos.

La Oficina de Sistemas de Información debe:

1. Dar a conocer y sensibilizar en las técnicas adecuadas para mantener el escritorio despejado al igual que la pantalla de los equipos de cómputo con el apoyo de cada jefe de oficina o dependencia; para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

2. Los equipos de cómputo y portátiles deben tener implementado la activación del protector de pantalla ejecutado por el Grupo Administración de las Tecnologías de la Información. Para lo anterior, la Oficina Asesora de Comunicaciones debe orientar y aprobar el protector de pantalla.

3. La pantalla de autenticación a la red del Instituto debe requerir solamente la identificación de la cuenta y una clave.

4. Para desactivar el protector de pantalla y volver al modo normal de funcionamiento del equipo de cómputo, el sistema solicitará nuevamente usuario y contraseña para ingresar al equipo.

Responsabilidad de los usuarios:

1. Al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan información pública clasificada o pública reservada, así mismo desconectar los equipos tecnológicos que estén a su cargo.

2. Los equipos que queden ubicados cerca de zonas de atención al público, deben situarse de forma que las pantallas no puedan ser visualizados por personas externas.

3. Toda información crítica deberá ser guardada en lugares seguros, archivadores bajo llave.

4. Clasificar y protege los objetos e información susceptible de pérdidas.

5. Cerrar los cajones de su escritorio bajo llave.

6. Ser cuidadoso de no dejar archivos o información sensible en el escritorio (pantalla inicial) del equipo de cómputo, se recomienda el uso de la estructura de árbol de las carpetas del sistema para así no acumular información en la pantalla inicial.

7. En caso que se utilice portátiles para presentaciones, si éste fuera de uso corporativo, debe eliminarse la información antes presentada.

8. Los puestos de trabajo deben permanecer limpios y ordenados.

9. Los cajones y archivadores de contengan documentos y/o medios extraíbles con información pública, pública clasificada o pública reservada deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral.

10. Las salas o áreas de reuniones, salas de conferencias y de capacitación, deben quedar limpias de todo el material utilizado.

24. Uso y servicio de impresoras y fotocopiadoras

Lograr el buen uso, y manejo y protección de impresoras y fotocopiadoras al servicio del Instituto.

1. La Oficina Sistemas de Información con apoyo de las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional debe realizar mantenimiento preventivo y correctivo, vigilar e incentivar el buen uso de las impresoras y fotocopiadoras del Instituto, para que no se afecte su correcto funcionamiento.

Responsabilidad de los usuarios:

1. Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras o fotocopiadoras en caso de presentarse alguna falla, esta se debe reportar vía correo o telefónicamente a la Oficina Sistemas de Información, áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional, según sea el caso.

2. El uso de impresoras y fotocopiadoras, son sólo de carácter institucional y no personal.

3. El usuario no debe sobrepasar la capacidad máxima de papel en el cargador, esto puede ocasionar problemas en la impresora o fotocopiadoras y retener las tareas.

4. Nunca forzar el papel: jamás se debe forzar la salida del papel, tirándolo antes que termine su proceso de impresión o fotocopiado se pueden dañar los rodillos de la impresora/fotocopiadora y lo más habitual es que se acabe por romper el papel y lo que es peor, se quede alguna pequeña parte enganchada que provoque atascos.

5. Separar o airear el papel con cuidado antes de colocarlo en la bandeja, esto evitará atascamientos.

6. El servidor público no debe manipular partes internas cómo la tarjeta electrónica de las impresoras/fotocopiadoras u otros, ya que puede alterar el buen funcionamiento de los mismos.

7. Nunca se debe aplicar ningún tipo de producto de limpieza ni de aceites en spray directamente sobre las partes internas de la impresora/fotocopiadora, ya que estos sí que pueden dañar seriamente el funcionamiento de la misma. Utilizar un paño ligeramente húmedo para quitar el polvo.

8. Reducir al máximo el uso de impresoras. Imprimir sólo lo imprescindible, y utilizar más el correo electrónico.

9. Imprimir por ambas caras del papel.

10. Revisar que el papel no contenga ganchos o elementos extraños que pueden dañar la impresora.

25. Seguridad, responsabilidades y procedimientos de operación

Con el objetivo de evitar el acceso físico no autorizado, daños e interferencias a la información de la Institución y las instalaciones de procesamiento de la información, la Oficina de Sistemas de Información debe:

1. Generar procedimientos y/o guías de operación y administración de la plataforma tecnológica del Instituto, tales como:
    - Copias de respaldo y restauración
    - Encendido y apagado
    - Reinicio y recuperación de los sistemas en caso de fallas en el mismo.
    - Mantenimiento de equipos
    - Borrado seguro
    - Configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información entre otros.
    - Actualizar contactos de apoyo y soporte externo en caso de dificultades operacionales o técnicas inesperadas.

26. Gestión de cambios

Con el fin de evaluar y controlar el posible impacto operativo de los cambios previstos a sistemas de información y equipamiento tecnológico, la Oficina de Sistemas debe realizar:

1. La identificación y registro de cambios significativos.
2. La planificación y puesta a prueba de cambios.
3. Valoración de cambios potenciales, incluidos los impactos de estos cambios en la seguridad de la información.
4. El desarrollo del procedimiento de aprobación formal para los cambios propuestos
5. Verificación de que se han cumplido los requisitos de seguridad de la información
6. La comunicación de los detalles de los cambios a las personas pertinentes.
7. Los procedimientos de apoyo, incluido responsabilidades para interrumpir cambios no exitosos y recuperarse de ellos, y eventos no previstos.
8. Conservar registros de auditoria de la información pertinente a la gestión de cambios a sistemas de información y equipamiento tecnológico.

27. Gestión de capacidad

Con el fin de evitar potenciales amenazas a la seguridad de los sistemas o a los servicios del usuario, es necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad. La Oficina de Sistemas de Información debe:

1. Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica, considerando aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, almacenamiento, anchos de banda, internet y tráfico de la red de datos, entre otros.

2. Buenas prácticas para suministrar, incrementar o disminuir la demanda de capacidad:

    - Eliminación de datos obsoletos (espacio en disco) previo análisis y aprobación.
    - Cierre definitivo de aplicaciones, sistemas, bases de datos o ambiente, previo análisis y aprobación
    - Optimización de consultas de bases de datos o lógicas de aplicaciones, entre otros.
    - Tener en cuenta la capacidad de los recursos humanos, al igual de oficina e instalaciones.

28. Separación de ambientes de desarrollo, pruebas y operación

Con el objetivo de reducir los riesgos de acceso o cambios no autorizados a los ambientes de operación se debe implementar el nivel de separación entre los ambientes de desarrollo, prueba y operación; la Oficina de Sistemas de Información debe:

1. Definir y documentar las reglas para la transferencia de software de desarrollo al de operación.

2. Los cambios en los sistemas de información se deben poner a prueba antes de aplicarlos a los sistemas operacionales.

3. Los datos sensibles no se deben copiar en el ambiente de sistemas de pruebas.

4. Los compiladores, editores y otras herramientas de desarrollo no deben ser accesibles desde los sistemas operacionales.

5. El personal de desarrollo y pruebas deben firmar y aplicar acuerdos de confidencialidad, garantizando la total reserva de la información.

29. Controles de protección contra códigos maliciosos

Con el objetivo de definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra código o software malicioso, como para garantizar la seguridad de los datos y los servicios conectados a las redes de la Institución, la Oficina de Sistemas de Información debe:

1. Implementar controles para evitar o detectar el uso de software no autorizado (ejemplo: lista blanca de aplicaciones).

2. Implementar controles para evitar o detectar el uso de sitios web maliciosos o que se sospeche que lo son. (ejemplo: listas negras).

3. Suministrar los elementos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles precisos para evitar la divulgación, alteración, modificación o daño permanente ocasionados por el contagio de software malicioso en los equipos del Instituto. Además, proporcionará los mecanismos para generar cultura de seguridad y conciencia entre los servidores públicos y personal provisto por terceras partes frente a los ataques de software malicioso.

4. Velar porque todos los equipos de cómputo del Instituto tengan instalado el software de antivirus con su respectiva licencia actualizada, como una medida de control rutinaria, con el apoyo de las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional.

5. Asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, instalado en cada uno de los equipos del Instituto, ni alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Oficina Sistemas de Información.

6. Definir procedimientos y responsabilidades relacionadas con la protección contra software o código malicioso.

7. Desarrollar planes de continuidad del negocio, apropiados para la recuperación frente ataques de software o código malicioso.

Responsabilidad de los usuarios:

1. Verificar que la información y los medios de almacenamiento utilizados, estén libres de cualquier tipo de código malicioso, para lo cual deben identificar que el software antivirus autorizado por la Oficina Sistemas de Información se ejecute correctamente, debido a que algunos virus son extremadamente complejos, ningún usuario o servidor del INPEC, distinto al personal de la Oficina Sistemas de Información o encargados del área de sistemas de establecimientos o regionales, deberá intentar erradicarlos de los Pc.

2. Notificar si detectan alguna infección por software malicioso a la Oficina Sistemas de Información al correo antivirus@inpec.gov.co, o a las áreas de sistemas de las Direcciones Regionales, Establecimientos de Reclusión del Orden Nacional ó Dirección Escuela de Formación, para que tomen las medidas de control correspondientes.

3. Asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provengan de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

4. Comunicar si el software antivirus no está actualizado o no funciona correctamente al correo antivirus@inpec.gov.co, o en su defecto con las áreas encargadas de Sistemas de las Direcciones Regionales, Establecimientos de Reclusión del Orden Nacional ó Dirección Escuela de Formación.

30. Copias de respaldo y restauración

El control de la realización de las copias de respaldo de información, así como la prueba periódica de su restauración; permiten garantizar la continuidad de las operaciones en la Entidad, con tiempos de recuperación asumibles para la Institución.

La Oficina de Sistemas de Información debe:

1. Documentar procedimientos formales para la generación de copias de respaldo y restauración de los sistemas y aplicativos del Instituto, facilitando los medios necesarios; estableciendo operaciones, tiempos de recuperación y mecanismos para la realización de estas actividades.

2. Los procedimientos deben definir requisitos de retención y protección de la información.

3. Generar las copias de seguridad de las imágenes de los sistemas y bases de datos, o demás servicios identificados como críticos, en horas no laborables para la entidad.

4. Ejercer control sobre las operaciones de pruebas de restauración de las copias de seguridad de la información de las bases de datos, imágenes, o diferentes aplicativos existentes en el Instituto. Para garantizar la disponibilidad de la información en caso de contingencia o desastre.

5. Realizar seguimiento a la ejecución de las copias de respaldo y tener en cuenta las fallas de las copias programadas, para asegurar la integridad de la información.

6. Programar copias de respaldo de información de los equipos de cómputo de los usuarios, con el apoyo de las áreas de sistemas de las Direcciones Regionales, Dirección Escuela de Formación y Establecimientos de Reclusión del Orden Nacional .

7. En caso de daño o perdida de la información de los equipos de los usuarios, se debe restaurar las copias de respaldo una vez el servidor haya realizado el respectivo oficio dirigido a la Oficina de Sistemas de Información, áreas encargadas de sistemas, de las Direcciones Regionales, Dirección Escuela de Formación o Establecimientos de Reclusión del Orden Nacional, según sea el caso.

8. En situaciones en que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.

9. Las copias de respaldo se deben almacenar en lugar externo, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en la sede principal.

10. Mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas del Instituto, teniendo en cuenta como mínimo:

    - Identificación de los medios de almacenamiento.

- Tipo de información almacenada.
- Frecuencia de realización.
- Ubicación física o lógica.
- Fecha de reproducción.
- Condiciones de transferencia.
- Custodia de las copias.
- Responsable operativo.

Responsabilidad de los usuarios:

1. Identificar la información sensible o privada que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.
2. No almacenar en los discos duros de los equipos de trabajo información personal u otra que no haga parte del desarrollo laboral.

31. Registro de eventos, monitoreo y seguimiento de los sistemas de información y recursos tecnológicos

Con el objetivo de monitorear permanentemente el uso que le dan los servidores públicos y el personal provisto por terceras partes a los recursos tecnológicos y sistemas de información del INPEC, la Oficina de Sistemas de Información debe:

1. Elaborar, conservar y revisar regularmente los registros acerca de las actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información a través de informes consolidados incluyendo:
    - Identificación de usuarios.
    - Actividades del sistema.
    - Fechas, horas y detalles de los eventos por ejemplo entradas y salidas de los sistemas.
    - Identidad del equipo de cómputo y ubicación.
    - Registro de intentos de accesos a los sistemas exitosos y rechazados.
    - Cambios en la configuración del sistema.

- Uso de privilegios.
- Archivos a los que se tuvo acceso, y el tipo de acceso.
- Direcciones y protocolos de red.
- Activación y desactivación de los sistemas de protección, tales como antivirus y sistemas de detección de intrusión.
- Registro de transacciones ejecutadas por los usuarios en las aplicaciones.

2. Se debe guardar copias de seguridad de los registros de eventos con requisitos de protección y retención.
3. Los administradores de estos registros deben firmar acuerdos de confidencialidad y contar con privilegios limitados para borrar o desactivar logs de sus propias actividades.
4. Se deben proteger los logs de los sistemas contra cambios, eliminaciones o accesos no autorizados.

32. Sincronización de relojes

Los relojes de los sistemas de procesamiento de información se deben sincronizar con una única fuente de referencia de tiempo, asegurando la exactitud de los logs de auditoria, que pueden ser necesarios para investigaciones o como evidencia en casos legales o disciplinarios, la Oficina de Sistemas de Información debe:

1. Sincronizar los relojes de los sistemas de procesamiento de información dentro de la Institución o del dominio de seguridad, por lo anterior deben estar con el Instituto Nacional de Metrología fuente de tiempo exacta y acordada, con el fin de garantizar la exactitud veracidad de los registros de auditoría, al menos de los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes.

33. Control de software operacional: instalación de software en Sistemas Operativos

Con el fin de controlar la instalación de software en sistemas operativos la Oficina Sistemas de Información debe considerar las siguientes directrices:

1. Establecer responsabilidades y procedimientos para controlar la instalación del software operativo.

2. Asegurar que el software operativo instalado en la plataforma tecnológica del INPEC cuente con soporte de proveedores.

3. Asegurar que las contraseñas que traen por defecto los sistemas operativos no sean utilizadas, incluyen el firewall y las bases de datos.

4. La actualización de software operacional, aplicaciones y bibliotecas de programas se deben de llevar a cabo solo por los administradores de los sistemas autorizados.

5. Asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

6. Establecer una estrategia de retroceso (rollback) antes de implementar cambios en los sistemas operativos.

7. Mantener un log de auditoria de las actualizaciones de las bibliotecas operacionales.

8. Aplicar parches de seguridad para ayudar a eliminar o reducir debilidades de seguridad de la información.

34. Gestión de las vulnerabilidades técnicas de los sistemas de información

Con el objetivo de obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información, la Oficina de Sistemas de Información debe considerar lo siguiente:

1. Adoptar controles de acceso como: Firewall, sistema de detección de intrusos (IDS), Sistema de prevención de intrusos (IPS) entre otros.

2. Definir línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas.

3. Definir roles y responsabilidades asociados con las vulnerabilidades técnicas, incluido el seguimiento y toma de conciencia.

4. Generar, ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

5. Establecer e implementar reglas tecnológicas para la instalación de software por parte de los usuarios no autorizados

35. Gestión de seguridad de las redes

La Oficina de Sistemas de información con el fin de establecer mecanismos de control necesarios para proteger la integridad, disponibilidad y confidencialidad de la información que se transporta a través de las redes de datos, como del tráfico, debe:

1. Establecer responsabilidades y procedimientos para la gestión de equipos de red.

2. Adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red del Instituto.

3. Implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

4. Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

5. Establecer estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica del instituto, acogiendo buenas prácticas de configuración segura.

6. Identificar, justificar y documentar los servicios, protocolos y puertos permitidos para el Instituto en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

7. Asegurar la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos del INPEC.

8. Implementar controles de autenticación, y encriptación a nivel de usuario de las redes inalámbricas.

9. Segmentar las redes de datos por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier categorización que se considere conveniente para el Instituto.

36. Transferencia de información

Con el objetivo de asegurar la protección de la información transferida o intercambiada internamente o externamente, se deben implementar buenas prácticas de seguridad de la información.

La Oficina de Sistemas de Información debe:

1. Implementar herramientas digitales seguras con métodos de cifrado y autenticación para la transferencia de información al interior y exterior de la Entidad, considerando firmas digitales entre otras.

La oficina Asesora Jurídica debe:

1. Asesorar al INPEC para que cumpla las normas legales y regulatorias locales en referencia a la Seguridad de la Información que afecten al Instituto. **PA-TI-G08 Guía Roles y Responsabilidades para la Seguridad de la Información** versión oficial numeral 1.4. ítem 1.

2. Apoya en el diseño de los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por el INPEC a los servidores públicos y terceros con quienes se establecen estos acuerdos y la destrucción de dicha

información una vez cumpla su cometido, con el apoyo de la Subdirección de Gestión Contractual y la Oficina de Sistemas de Información.

La Subdirección de Gestión Contractual debe:

1. Instituir en los contratos que se establezcan con terceras partes, o prestación de servicios los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios del instituto que les ha sido entregada en razón del cumplimiento de los objetivos misionales del INPEC.

El Grupo Gestión Documental debe:

1. Controlar que todo envió de información física a terceros (documentos o medios magnéticos) utilicen únicamente los servicios de transporte o mensajería autorizados por el Instituto, y que estos permitan efectuar rastreo de las entregas.

2. Controlar que el embalaje de los documentos sea se suficiente para proteger el contenido contra cualquier daño físico que pudiera presentarse durante el transito ante cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor o humedad, como también ante cualquier acceso no autorizado.

3. Los dispositivos que contengan información se deben proteger contra el acceso no autorizado, así como uso inadecuado o la adulteración durante el transporte más allá de los límites físicos de la Institución.

Responsabilidad de los usuarios:

1. Velar porque la información del INPEC o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

2. Abstenerse de tener conversaciones confidenciales para el Instituto en lugares públicos o mediante canales de comunicación no seguros, oficinas abiertas y lugares de reunión.

3. La Información física como digital disponible al público debe estar protegida para evitar la modificación no autorizada, y así conservar su integridad.

4. Dejar registro del intercambio de información con terceros, del emisor y receptor de la misma y la fecha de entrega/recepción.

37. Uso del correo electrónico

El correo electrónico como herramienta para facilitar la comunicación entre los servidores públicos y terceras partes, proporciona un servicio eficiente y seguro para la ejecución de las actividades laborales, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio. Con el fin de garantizar la seguridad y disponibilidad del servicio del correo electrónico, se deben implementar buenas prácticas de seguridad.

La oficina de Sistemas de Información debe:

1. Proveer un ambiente seguro, encriptado y controlado para el funcionamiento de la plataforma de correo electrónico, como el de su direccionamiento y transporte correcto de los mensajes. (para el enlace el proveedor es el responsable de garantizar su disponibilidad, en un 100%.)

2. Establecer controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

3. Generar campañas para concientizar a los servidores públicos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Responsabilizad de los usuarios:

1. Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional del Instituto, el correo institucional no debe ser utilizado para actividades personales, la información contenida en los buzones de correo son propiedad del INPEC y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

2. La cuenta de correo electrónico asignada a los servidores públicos es de carácter particular; por consiguiente, ningún servidor del Instituto o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

3. El uso indebido del servicio del correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

4. Ningún usuario externo a la Institución, puede usar los servicios del correo electrónico proporcionado por la red del Instituto.

5. La información que se recibe de manera personal y confidencial por correo electrónico ó medio físico, no se debe reenviar a otra persona, sin la autorización del remitente.

6. Utilizar la función de correo no deseado para aquellos mensajes de publicidad, ventas, etc.

7. Un correo electrónico, deberá ser impreso únicamente cuando sea necesario, ya que esta herramienta fue creada para tener un archivo electrónico, agilizar las comunicaciones, para descartar en la medida de lo posible el archivo tradicional y lograr un ahorro de papel.

8. No descargue archivos adjuntos si no está seguro de su procedencia. En caso de hacerlo, revíselo con la solución antivirus con capacidades de detección instalado en cada uno de los equipos de cómputo del Instituto y así garantizar que no se trate de algún código dañino que pueda afectar su

equipo. Además, verifique si estos archivos tienen doble extensión; si es así, sea precavido ya que probablemente se trate de un gusano o troyano, los cuales utilizan este modo de engaño para su propagación.

9. No publique el correo electrónico Institucional en foros, sitios web, blog, redes sociales, conversaciones en línea y demás, ya que esto lo que hace es facilitarle las cosas a los usuarios dedicados al envío de spam que podrán capturar su cuenta e incluirla en su selecta lista para envió masivo de spam.

10. No responda a los correos tipo spam, ya que, de hacerlo, le estará confirmando al spammer que su cuenta de correo se encuentra activa y en consecuencia seguirá recibiendo más mensajes de esta clase.

11. No envíe correos en cadena. Evite esta práctica ya que, este tipo de mensajes generalmente suelen estar relacionados con algún tipo de engaño. Ahora bien, si por algún motivo se desea reenviar el mensaje a muchos destinatarios, se recomienda entonces usar el campo CCO (con copia oculta) para insertar allí las direcciones. De esta manera las direcciones de correo de los usuarios de destino, no podrán ser visualizadas. Además, tómese un segundo para borrar aquellas direcciones del mensaje anterior que, por lo general, al momento de reenviar quedan consignadas en el cuerpo del mensaje.

Tenga en cuenta que al aplicar lo anterior aumentaremos los niveles de prevención y de esta manera mitigar el riesgo de sufrir un potencial ataque durante el uso del correo electrónico, cualquier anomalía por favor escribir a solicitud.correoinstitucional@inpec.gov.co

38. Uso de contraseñas

Evitar el acceso de usuarios no autorizados, la sustracción o la puesta en peligro de la información y de los servicios de procesamiento de información.

1. La Oficina de Sistemas de Información es la encargada de generar los estándares para la creación de las contraseñas en los aplicativos Institucionales; el usuario es responsable de realizar el cambio de la primera contraseña para una mayor seguridad; a su vez la Oficina de Sistemas debe exigir y controlar que los usuarios cumplan prácticas de seguridad en la selección, uso y protección de las contraseñas.

Responsabilidad de los usuarios:

1. Las contraseñas se utilizan para permitir o denegar el acceso a un recurso.

2. Los servidores públicos son responsables de proteger las contraseñas que utilizan para el acceso a los distintos servicios y recursos ofrecidos por el Instituto, por lo tanto, son de uso exclusivo, e intransferibles.

3. Es importante que las contraseñas que se usen sean seguras y/o robustas, para evitar que un usuario no autorizado pueda obtenerlas y utilizarlas para propósitos no deseados. En

general una contraseña más larga será más segura (contraseña fácil de recordar y no fácil de adivinar).

4. No utilice datos personales o de seres queridos para formar la contraseña. (Nombre, fecha de cumpleaños, aniversario, graduación, artistas favoritos, novio/novia, mascotas, etc.).

5. No use contraseñas completamente numéricas con algún significado (teléfono, cédula de ciudadanía, fecha de nacimiento, placa del automóvil, etc.).

6. No utilice la misma contraseña para sistemas diferentes. La contraseña debe ser única para cada sistema de manera que, si una de las contraseñas es hurtada, el resto de los sistemas no se verá afectado.

7. Evite la contraseña por correo electrónico, mencionarla en conversaciones.

8. No utilice la contraseña en equipos no confiables o públicos, como un café Internet.

Ejemplo de algunas contraseñas seguras:

9. Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3.

10. Usar un acrónimo de alguna frase fácil de recordar: A rio Revuelto Ganancia de Pescadores -> ArRGdP.

11. Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P.

12. Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar, Win8cackkenl2012.

13. Crear contraseñas con al menos tres de los siguientes cuatro conjuntos de caracteres: Minúsculas, mayúsculas, letras y símbolos especiales. (#$%&/=?!).

14. Ante la sospecha de que una contraseña haya sido revelada a terceros, se cambiará la misma de forma inmediata, y se procederá a notificar por oficio del incidente de seguridad, a la Oficina de Sistemas de Información

Recomendaciones para la protección de contraseñas:

15. La protección de la contraseña recae en el servidor público. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

16. Los servidores públicos no deben compartir sus cuentas de usuario y contraseñas con otros servidores o con personal provisto por terceras partes.

17. Desconfiar de cualquier correo que pida datos como usuario y contraseña, estos nunca son necesarios por un tercero salvo que quiera hurtar sus datos, por tanto de recibir un mensaje

de este tipo, no lo conteste y notifique por oficio escrito a la Oficina de Sistemas de Información de inmediato.

18. Evite utilizar la misma contraseña siempre en todos los sistemas o servicios.

19. No repetir los mismos caracteres en la misma contraseña. (ej.: "111222").

20. Evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")

Tenga en cuenta que para la Solicitud de Creación y/o Modificación de Permisos de Usuario y Contraseña de Sistemas de Información, debe diligenciar el formato anexo a presente guía.

39. Uso adecuado de Internet

La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

La Oficina de Sistemas de Información debe:

1. Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet.

2. Establecer normas, seguimientos y perfiles de acceso en el servicio de internet para la prestación segura del mismo, para optimizar y facilitar las labores de trabajo en el INPEC. Para el enlace el proveedor es responsable de garantizar su disponibilidad, en un 100%.

3. Monitorea continuamente el canal del servicio de Internet, para prevenir indisponibilidad del mismo.

4. La Oficina de Sistemas de Información se reserva el derecho de monitorear los accesos al servicio de Internet de los servidores públicos, además de limitar el acceso de algunas páginas de Internet, como los horarios de conexión y cualquier otro ajeno a los objetivos del Instituto. Los equipos que cuenten con internet, podrán ser sometidos a auditoria con el fin de verificar el buen uso del mismo.

5. Diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

6. Informar a los directivos o jefes inmediatos sobre el mal uso que se le está dando a Internet en su área.

7. Genera campañas para concientizar a los servidores públicos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Responsabilidad de los usuarios:

1. Para cualquier requerimiento de acceso a Internet es necesario realizar la solicitud de asignación de permisos a Internet a la Oficina de Sistemas de Información; para el caso de las aulas virtuales la solicitud debe realizarla el servidor público encargado del área de Educativas, con visto bueno del encargado del área de sistemas y con firma del Director Regional, Director Escuela de Formación o Director Establecimiento de Ordena Nacional según aplique. Para el caso de la Dirección General la solicitud debe ser firmada por el servidor público y su jefe inmediato.

2. Los privilegios de uso de internet estarán de acuerdo a la necesidad de acceso que requiera cada servidor con base a su desempeño laboral; por consiguiente, no debe ser utilizado con fines personales.

3. Deben hacer uso del mismo Internet de forma razonable en relación con las actividades laborales que así lo requieran.

4. No debe compartir la dirección IP asignado a su equipo de computo, usuario, contraseña de ingreso y/o de directorio activo según sea el caso.

5. El firewall es el principal escudo protector de la red Institucional para comprobar y permitir/denegar tanto el tráfico entrante o saliente de Internet; por lo tanto, esta prohibido la instalación de software localmente o remotamente en los PC, para la evasión del mismo. Esto acarrea sanciones disciplinarías.

6. No debe descargar ningún programa o software tales como: software de evaluación, archivos de música (MP3, WAV, etc.) videos, juegos, películas, protectores, software de libre distribución, que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

7. Evite acceder a sitios desconocidos o no confiables.

8. No acepte la instalación automática de software.

9. No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o controles establecidas en este documento.

10. Debe informar de manera inmediata cualquier anomalía, frente al servicio de internet y/o acceso prohibido del mismo por otro servidor público, comunicando a su jefe inmediato con copia al correo solicitud.permisosinternet@inpec.gov.co.

40. Uso de mensajería instantánea y redes sociales

Las redes sociales institucionales son un mecanismo de comunicación entre el Gobierno Nacional, la ciudadanía, los empresarios, los medios de comunicación, las organizaciones no gubernamentales y la sociedad en General. La Oficina Asesora de Comunicaciones como única dependencia autorizada para la gestión y creación de cuentas de usuarios en redes sociales; define pautas para asegurar una adecuada protección de la información del INPEC, en el uso del servicio de mensajería instantánea y de las redes

sociales, siguiendo directrices establecidas en la Circular 01 de 2019, de la Presidencia de la República.

Responsabilidad de los usuarios:

1. Los servidores públicos designados para la administración y manejo operativo de las redes sociales en la Entidad, deben aplicar complejidad en las contraseñas de las cuentas realizando el cambio periódicamente, acatando los protocolos de seguridad de las mismas.

2. La información que se publique o divulgue a través de Internet, de cualquier servidor público colaborador del INPEC, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instaram, WhatsApp, Messenger, WeChat, entre otros, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

3. La información distribuida en las redes sociales que sea originada por la Entidad, debe ser autorizada por los jefes de dependencia para ser socializadas y con un vocabulario institucional.

4. No se debe utilizar el nombre de la Institución en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la Entidad.

5. No se deben vincular cuentas de correo electrónico personales o comerciales, a las redes sociales que se apertura bajo el dominio @inpec.gov.co y @epn.gov.co

41. Uso de conexiones remotas.

Con el objetivo de prevenir la interceptación de posibles atacantes en conexiones remotas (VPN) Virtual Private Network (Red privada virtual), la Oficina de Sistemas de Información debe:

1. Establecer conexiones remotas seguras dentro de la plataforma tecnológica del Instituto, utilizando metodologías de autenticación robusta de los usuarios y dispositivos, entre otras.

2. Realizar pruebas de carga de VPN en entornos simulados, que ayuden a conocer y controlar el volumen de usuarios que pueden hacer uso de ella, con el objetivo de evitar cuellos de botella, latencia, lentitud o desconexiones.

3. La conexión remota a la red de área local del INPEC debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

4. Monitorear toda la actividad de la red corporativa, en busca de cualquier vulnerabilidad como, por ejemplo, intentos de acceso fuera de horario, desde ubicaciones dudosas, o dispositivos no identificados, intentos recurrentes de autenticación fallida, accesos simultáneos, entre otros con el objetivo de detectar y tomar las medidas oportunas contra la actividad inapropiada.

5. Asegurar de que cada componente de la infraestructura de acceso remoto (servidores, pasarelas, servidores de autenticación, entre otros.) tenga su reloj sincronizado con la misma fuente, de modo que todas las medidas de tiempo coincidan con las generadas por otros sistemas.

6. Analizar y documentar las anomalías detectadas dentro de la infraestructura de acceso remoto.

7. Estas conexiones únicamente se deben permitir a personal interno o externo con periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

8. El personal de la Oficina Sistemas de Información que de soporte técnico a través de acceso remoto son los únicos autorizados para realizar dicha labor; siempre y cuando el servidor público requiera del soporte apruebe dicha conexión hacia el equipo de cómputo asignado para sus labores

Responsabilidad de los usuarios:

1. Todo usuario autorizado para conexiones remotas VPN debe con antelación firmar un acuerdo de confidencialidad para hacer uso de la información.

2. Los usuarios autorizados para las conexiones VPN únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en equipos de cómputo públicos, de hoteles o cafés internet, entre otros.

3. Los equipos a la previa configuración de la VPN, deben contar con una solución de antivirus, actualización de parches de seguridad, cifrado en conexión Wifi.

4. Bloquee su equipo cuando se aleje de él.

42. Seguridad en el uso de aplicaciones de videoconferencia

Con el fin de garantizar la protección, privacidad y disponibilidad del servicio de videoconferencias, se deben implementar buenas prácticas de seguridad.

La Oficina de Sistemas de Información debe:

1. Suministrar herramientas colaborativas para la conexión segura a videoconferencias, que cuentan con mecanismos de cifrado.

2. Implementa procedimientos formales para la solicitud de videoconferencias.

3. Una vez que todos los participantes se hayan incorporado a la videoconferencia, bloquea el acceso a nuevos participantes a la reunión. De esta forma, asegura que sólo los participantes autorizados estén en la reunión evitando intrusos que puedan espiar conversaciones.

Responsabilidad de los usuarios:

1. Solicitar formalmente la realización de videoconferencia, siguiendo procedimientos emitidos por la Oficina de Sistemas de Información.

2. Mantener vídeo y micrófono apagados por defecto, antes de empezar la videoconferencia, utilícelo solo cuando sea necesario.

3. No debe compartir su escritorio de forma predeterminada ya que esto puede provocar fugas de información.

4. Si el administrador pretende grabar la reunión, se lo comunicará a los participantes para que estos sean conscientes de ello.

5. Cuando comparta su pantalla con el resto de usuarios de la reunión debe evitar compartir información confidencial, como:

    - Nombres de usuario o nombre de dispositivo.
    - Documentos confidenciales.
    - Nombres de archivos o directorios sensibles,
    - Direcciones web del navegador.

43. Adquisición, desarrollo y mantenimiento de los sistemas de información.

Con el objetivo de garantizar la inclusión de controles de seguridad, validación de datos y buenas prácticas en la adquisición y el desarrollo de los sistemas de información internos, como de terceras partes, la Oficina de Sistemas de Información debe:

1. Definir y documentar normas y procedimientos que se aplicarán durante el ciclo de vida y control de cambios en los sistemas de información y de la infraestructura de base en la cual se apoyan.

2. Será la única dependencia con la capacidad de desarrollar, avalar y/o adquirir software de acuerdo a los requerimientos de manera coordinada con las demás dependencias, establecimientos o regionales que manifiesten la necesidad del software, En consecuencia, con lo anterior cualquier software que se encuentre ejecutándose dentro del Instituto, sin la aprobación, licenciamiento, medidas de seguridad y protección de la información no será responsabilidad de la Oficina Sistemas de Información, ni se le brindará soporte y no se protegerá la información.

3. Establece claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.

4. Establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

5. Realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.

6. Realiza pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.

7. Eliminar la información de los ambientes de pruebas, una vez estas han concluido.

8. Certifica que todo sistema de información adquiridos o desarrollados utilicen herramientas licenciadas.

9. Aprueba o no las migraciones entre los ambientes de desarrollo y producción y/o cambios de nuevas funcionalidades. Todos los cambios se registran y se documentan estrictamente

10. Implementa reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información del INPEC.

11. Establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

12. Debe asegurar que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

13. Incluye buenas prácticas de desarrollo seguro, teniendo en cuenta controles de acceso y arquitectura de aplicaciones, entre otros con el fin de suministrar a los programadores una visión clara de lo que se espera, como también supervisa y monitorea el desarrollo de software contratado externamente.

14. Lleva un registro actualizado de todos los programas fuente en uso, indicando nombre del programa, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

15. Verifica que los desarrollos propiedad del Instituto estén correctamente documentados y que sean registrados ante la Dirección General de Derechos de Autor, que las diferentes versiones se preserven adecuadamente en varios medios y se guarde copia de respaldo externa a la entidad.

Los desarrolladores internos como los previstos por terceras partes deben:

1. Firmar acuerdos de confidencialidad y seguridad de la información con el fin de evitar divulgar la información de la estructura de directorios de los sistemas de información construidos sin previa autorización.

2. Documentar y definir la arquitectura de software más conveniente para cada sistema de información que se desarrolle, de acuerdo con los requerimientos de información, seguridad y controles de acceso.

3. Proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

4. Suministrar opciones de cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión.

5. Proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software desarrollado propiedad del INPEC; dicho soporte debe contemplar tiempos de respuesta aceptables.

Otros:

1. El software proporcionado o desarrollado por el Instituto no puede ser copiado o suministrado a terceros sin previa autorización.

2. Toda contraseña de aplicativos desarrollados o adquiridos con terceros deben ser protegidas contra copia o divulgación no autorizada mediante almacenamiento cifrado.

3. Todo software que se vaya a adquirir y/o conectar a la plataforma tecnológica del Instituto, por cualquier dependencia o proyecto del INPEC, debe ir con el visto bueno de la por la Oficina Sistemas de Información. Cuando se cambien o se actualicen los sistemas operativos de las aplicaciones críticas para el Instituto se deben revisar y someter a prueba para asegurar que no hay impacto opuesto en las operaciones ni en la seguridad de la entidad.

4. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Oficina de Sistemas de Información justificada, quien analizará las propuestas presentadas para su evaluación y aprobación.

44. Seguridad de la información en las relaciones con terceras partes

Con el objetivo de establecer mecanismos de control en relaciones con terceras partes, se debe asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

La Oficina de Sistemas de Información, la Oficina Asesora Jurídica y la Subdirección de Gestión Contractual deben:

1. Elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

2. Generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

La Oficina de Sistemas de Información debe:

1. Establecer y documentar acuerdos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la Institución.

2. Establecer los protocolos y condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos del instituto.

3. Establecer condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

4. Prevenir y mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica del Instituto.

5. Controlar los aspectos de seguridad de la información sensible o critica para las instalaciones de procesamiento de información a las que tiene acceso un proveedor.

Supervisores de contratos:

1. Monitorear, revisar y auditar la prestación de servicios del proveedor regularmente.

2. Hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos.

3. Revisar reportes de servicio elaborados por el proveedor y concertar reuniones de avance regulares, según se exija en los acuerdos

4. Resolver e identificar cualquier problema que llegare a suceder.

5. Verificar que el proveedor mantenga una capacidad de servicio suficiente, junto con planes ejecutables destinados asegurar que se mantengan los niveles de continuidad acordados en caso de una falla considerable en el servicio o después de un desastre.

45. Gestión de incidentes y mejora en seguridad de la información

Con el objetivo de asegurar un enfoque coherente y eficaz para la gestión de eventos e incidentes de seguridad de la información incluyendo la comunicación de los eventos de seguridad y debilidades, se deben considerar las siguientes directrices:

La Dirección General como líder en el SGSI:

1. Designa responsables para el tratamiento de los incidentes de seguridad de la información; personal calificado y competente, quienes tendrán la responsabilidad gestionar los incidentes reportados, asegurando respuestas rápidas y efectivas.

La Oficina de Control Interno Disciplinario debe:

1. Establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la Entidad, el tratamiento de las faltas de cumplimiento a las políticas de seguridad, controles o los incidentes de seguridad que lo ameriten. **PA-TI-G08 Guía Roles y Responsabilidades para la Seguridad de la Información** versión oficial, numeral 1.8, ítem 1.

2. El proceso disciplinario se debe utilizar como disuasión para evitar que los servidores públicos y otros colaboradores del INPEC violen las políticas y los procedimientos de seguridad de la información.

Los responsables para el tratamiento de los incidentes de seguridad de la información asignados deben:

1. Clasificar, investigar, solucionar y responder a los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia, escalando los incidentes de acuerdo a su criticidad, activando procedimiento de contacto con autoridades, cuando lo estime necesario; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

2. Implementar procedimientos formalizados para promover entre los servidores públicos y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información utilizando un punto de contacto y canales de administración adecuados para la recopilación de la información.

3. Crear bases de conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información, para reducir el tiempo de respuesta, la probabilidad y/o impacto de incidentes en el futuro, con el apoyo técnico de la Oficina de Sistemas de Información, incluyendo mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones entre otros.

Responsabilidad de servidores públicos y personal provisto por terceras partes deben:

1. Tomar conciencia de su responsabilidad de reportar eventos o incidente de seguridad de la información a través del punto de contacto y canales apropiados, que se dispongan en los procedimientos respectivos cuando se amerite. No reportar eventos o incidentes es una infracción a la seguridad de la información.

Las situaciones que se deben considerar para el reporte de eventos de seguridad de la información incluyen entre otros:

1. Control de seguridad ineficaz

2. Violación de la confidencialidad, integridad o expectativa de disponibilidad de información o sistemas de información.

3. Errores humanos.

4. No conformidades con la Política de seguridad de la información y documentos asociados al SGSI.

5. Violaciones de acuerdos de confidencialidad.

6. Violaciones de accesos físicos como lógicos.

7. Cambios no controlados en un sistema.

8. Y otros que disponga los procedimientos de reportes de eventos o incidentes de seguridad de la información.

46. Seguridad de la información en la gestión de la continuidad del negocio

El INPEC, en cabeza de la Dirección General proporcionará los recursos suficientes para proteger los procesos críticos del Instituto en caso de eventos catastróficos, asegurando que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia, manteniendo canales de comunicación adecuados hacia los servidores públicos, proveedores y terceras partes interesadas.

La Dirección Gestión Corporativa, Dirección de Custodia y Vigilancia, Oficina Asesora de Planeación, Oficina Asesora Jurídica y la Oficina de Sistemas de Información, deben:

1. Liderar temas relacionados con la continuidad del negocio y la recuperación ante desastres.

2. Realizar una estimación de la magnitud del impacto operacional y financiero que se encuentra asociado a una interrupción en el Instituto.

3. Reconocer las situaciones que serán identificadas como emergencia o desastre para el instituto, los procesos o las dependencias y determinar cómo se debe actuar sobre las mismas.

4. Tomar la decisión de activar o no el Plan de Continuidad

5. Requerir, monitorear y velar por el cumplimiento de la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, de los procesos críticos a las diferentes dependencias que conforman el Instituto, solicitando documentación de dichas pruebas.

La Oficina de Sistemas de Información debe:

1. Desarrollar y ejecutar el Análisis de Impacto de Negocios BIA (Bussiness Impact Analysis) para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afectan las operaciones regulares de la Entidad.

2. Con el resultado del BIA debe realizar el Plan de Continuidad de Tecnología de Información BCP (Business Continuity Plan), aprobado y respaldado por los Directivos de la Entidad y que este alineado con el Plan General de Continuidad del Negocio de la Entidad; el plan debe permitir a la Institución continuar con sus operaciones, en caso de presentarse fallas inconvenientes en sus

sistemas que le impidan el normal funcionamiento de los servicios de TI, de esta manera, la correcta implementación del plan deberá permitir restaurar en el menor tiempo posible las operaciones de la Entidad.

3. Prevenir interrupciones en las actividades de la plataforma tecnológica del INPEC que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.

4. Participar activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité Institucional de Gestión y Desempeño.

5. Analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para el Instituto y la plataforma tecnológica que los apoya.

6. Evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor se adapte a la institución.

Los Directores, Subdirectores, Jefes de Oficinas Asesoras, Jefes de Oficina, Coordinadores, Directores Regionales, Directores de Establecimientos de Reclusión del Orden Nacional y Director de Escuela de Formación deben identificar y generar la documentación de los procedimientos de continuidad del negocio que podrían ser utilizados en caso de un evento adverso o catastrófico de su dependencia. Estos documentos deben ser probados para certificar su efectividad.

47. Cumplimiento de requisitos legales y contractuales

Con el objetivo de cumplir con las disposiciones normativas y contractuales pertinentes a cada sistema de información, derechos de autor y propiedad intelectual la **Oficina Asesora Jurídica:**

1. Debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicable al Instituto relacionados con seguridad de la información junto con el enfoque de la Institución.

La Oficina de Sistemas de Información debe:

1. Controlar y certificar que todo el software que se ejecuta en el Instituto esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

2. Adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violen los derechos de autor.

3. Establecer un inventario junto con el Grupo de Manejo de Bienes Muebles e Inmuebles, para llevar un control sobre el licenciamiento de software existente en el Instituto. Llevar de manera clara y organizada el registro de las licencias que fueron compradas o que les fueron donadas al Instituto.

4. Tener bajo custodia, junto con las áreas de sistemas de las Direcciones Regionales, Establecimientos de Reclusión del Orden Nacional y Dirección Escuela de Formación los discos

maestros, manuales de uso, medios magnéticos/CDs u otros que vengan originalmente con el software, licencias y manuales de uso, como también las claves para descargar el software del fabricante en internet y los password.

5. Llevar a cabo revisiones periódicas en los equipos de cómputo propiedad del INPEC, como de equipos móviles, de que solo haya instalado software autorizado y licenciado con el apoyo del área de sistemas de las Direcciones Regionales, Establecimientos de Reclusión del Orden Nacional y Dirección Escuela de Formación.

6. Los productos de software desarrollados por el INPEC, deben ser patentados, bajo un acuerdo de licencia que especifique términos y condiciones.

7. La Oficina Sistemas de Información no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus servidores públicos.

Responsabilidad de los usuarios:

1. El uso de programas sin su respectiva licencia (imágenes, videos, software o música), obtenidos a partir de otras fuentes (Internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la Entidad, por lo que esta práctica no está autorizada.

2. Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.

3. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor.

4. El software que infrinja estos acuerdos deberá ser desinstalado inmediatamente por el personal de la Oficina de Sistemas o áreas encargadas de sistemas de las Direcciones Regionales, Establecimientos de Reclusión del Orden Nacional y Dirección Escuela de Formación; de no realizar esta acción las partes involucradas estarán sujetas a sanciones administrativas de orden disciplinario o penal, de acuerdo a las circunstancias.

5. No copiar total ni parcialmente, libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derecho de autor.

6. Proteger los registros que manejen contra perdidas, destrucción o acceso no autorizado.

48. Privacidad y protección de información de datos personales.

En cumplimiento de la Ley 1581 de 2012, y a la **PA-TI-PL02 Política de Tratamiento y Protección de Datos Personales** versión oficial, el Instituto Nacional Penitenciario y Carcelario, velará por el correcto desempeño de la protección de los datos registrados en cualquier base de datos existente en el Instituto que permita realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) de sus, beneficiarios, servidores, proveedores y demás terceros de los cuales reciba y administre información.

La Dirección General como líder del Sistema de Gestión de Seguridad de la Información SGSI debe:

1. Revisar, modificar y aprobar la Política de Tratamiento y Protección de Datos Personales del Instituto, cuando sea necesario.

2. Designa o contrata el rol de Responsable del tratamiento de los datos personales competente, teniendo en cuenta los lineamientos de la Guía No. 4 Roles y Responsabilidades de MINTIC y quien tendrá las siguientes responsabilidades:

    - Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.

    - Tramitar las consultas, solicitudes y reclamos.

    - Utilizar únicamente los datos personales que hayan sido obtenido mediante autorización, a menos que los mismos no la requieran.

    - Respetar las condiciones de seguridad y privacidad de información del titular.

    - Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente, entre otras que requiera la institución.

La oficina de sistemas de información debe:

1. Implantar los controles necesarios para proteger la información personal de los beneficiarios, servidores públicos, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio para evitar su divulgación, alteración o eliminación sin la autorización requerida.

2. Proteger los datos personales de prueba que se entregarán a los desarrolladores externos, asegurando que no revelen información confidencial de los ambientes de producción, aplicando acuerdos de confidencialidad.

La Subdirección de Talento Humano:

1. Es responsable de la protección y tratamiento de los datos personales de los servidores y de Cuerpo y Custodia que reposan en la historia laboral, aplicando lineamientos de la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Así mismo, buscará proteger la privacidad de los datos que pertenecen a la vida privada y familiar de los servidores, estableciendo los controles necesarios para preservar aquella información que el Instituto conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del Instituto y no sea publicada, revelada o entregada a servidores públicos o terceras partes sin autorización o sin una orden judicial.

La Subdirección de Gestión Contractual:

1. Es responsable de la protección y tratamiento de los datos personales de los contratistas que reposan en sus hojas de vida, aplicando lineamientos de la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, como también buscará proteger la privacidad de los datos que pertenecen a la vida privada y familiar de los contratistas estableciendo los controles necesarios para preservar aquella información que el Instituto conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del Instituto y no sea publicada, revelada o entregada a servidores públicos o terceras partes sin autorización o sin una orden judicial.

Las dependencias o áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben:

1. obtener la autorización para el tratamiento de estos datos a través del **PA-TI-G03-F01 Autorización otorgada por el titular para el tratamiento de datos personales**, versión oficial, con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales, acorde a los lineamientos de la **PA-TI-PL02 Política de Tratamiento y Protección de Datos Personales** versión oficial, con el apoyo del responsable del tratamiento de los datos personales designado cuando se requiera.

49. Revisiones de seguridad de la Información

Se debe revisar el Sistema de Gestión de Seguridad de la Información SGSI periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, al interior del Instituto.

El Comité Institucional de Gestión y desempeño debe:

1. Revisar, modificar y aprobar la Política y los Planes de Seguridad de la Información, a intervalos planificados o cuando se tenga lugar a cambios significativos en la Institución, incluyendo valoración de oportunidades de mejora.

Los Directores, Subdirectores, Jefes de Oficina, Directores Regionales, Directores de los Establecimientos de Reclusión del Orden Nacional y Director Escuela de Formación deben:

1. Revisar con regularidad el cumplimento de la presente guía, política de seguridad de la información y documentos asociados al SGSI al interior de sus oficinas o áreas, evaluando las necesidades de acciones para lograr el cumplimiento, sus fortalezas y debilidades e implementar acciones correctivas apropiadas.

50. Revisión del cumplimiento técnico

Los sistemas de información se deben revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas para la información de la entidad.

La oficina de Sistemas de Información debe:

1. Revisar preferiblemente con la ayuda de herramientas automáticas el cumplimiento técnico de seguridad de los sistemas de información, con personal competente autorizado y experimentado, independientes, contratados específicamente para este propósito. Considerando análisis de vulnerabilidades, Pentesting y Ethical Hacking, pruebas internas entre otros.

51. Sanciones para las infracciones al Sistema de Gestión de Seguridad de la Información.

La Política de Seguridad de la Información Institucional dentro de uno de sus objetivos pretenden instituir y afianzar cultura de seguridad de la información entre los servidores públicos y personal externo. Por tal razón, es necesario que las infracciones a la seguridad y privacidad de la información sean clasificadas, con el objetivo de aplicar medidas correctivas y preventivas que mitiguen posibles afectaciones a la seguridad. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, lo anterior conforme a los dispuesto por las normas estatutarias que rigen al personal del sector Justicia y del Derecho, si así lo ameritan.

Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables. Por consiguiente, el Instituto debe contar con un proceso disciplinario formal, comunicado para emprender acciones en contra de servidores públicos del INPEC que hayan cometido una violación a la seguridad y privacidad de la información. El proceso disciplinario también se debe utilizar como disuasión para evitar que los servidores y otros colaboradores del INPEC infrinjan la política y los documentos asociados al SGSI; las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de Gestión Disciplinaria.

La Oficina de Control Interno Disciplinario debe:

1. Establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la Entidad, el tratamiento de las faltas de cumplimiento a las políticas de seguridad, controles o los incidentes de seguridad que lo ameriten. **PA-TI-G08 Roles y Responsabilidades para la Seguridad de la Información** versión oficial, en su numeral 1.8, ítem 1.
2. No se debe iniciar el proceso disciplinario sin antes verificar que ha ocurrido una infracción a la seguridad de la información, contando con apoyo del responsable para el tratamiento de los incidentes de seguridad de la información designado.
3. Debe asegurar el tratamiento correcto e imparcial a los servidores públicos de quienes se sospecha que han cometido una violación a la seguridad de la información.

Algunas actuaciones que conllevan a la violación de la seguridad de la información:

1. No firmar los acuerdos de confidencialidad.
2. Retirar de las instalaciones de la Institución, estaciones de trabajo o computadores portátiles que contengan información Institucional sin la autorización pertinente.

3. No mantener la confidencialidad de las contraseñas de acceso a la red LAN Institucional y cuentas de correo electrónico asociadas a las mismas, o permitir que otras personas accedan con el usuario y clave del titular.
4. El que suplante un usuario ante los sistemas de autenticación y autorización establecidos por el INPEC.
5. Permitir el acceso u otorgar privilegios de acceso a las redes sociales del Instituto a personas no autorizadas.
6. Ejecución de cualquier acción que conlleve a la difamación, que llegue afectar la reputación o presentar una mala imagen del Instituto Nacional Penitenciario y Carcelario.
7. Eliminar documentos con información sensible o critica tanto físicos, como digitales sin tener la debida autorización o justificación o enviar intencionalmente a un destinatario que no corresponde las comunicaciones recibidas en la Entidad.
8. Ocasionar daño o dar lugar a la pérdida de expedientes o documentos que hayan llegado a su poder por razón de sus funciones.
9. Dar lugar al acceso o exhibir expedientes, documentos, información o archivos a personas no autorizadas.
10. Tomar fotografías o videos a documentos e información física como digital.
11. Realizar actividades tales como borrar, alterar o eliminar información de manera malintencionada. Sustraer de las instalaciones del INPEC, documentos de archivo sin la debida autorización.
12. No hacer entrega de los documentos de archivos que se encuentren a cargo de los servidores públicos, debidamente inventariados, cuando se presente su retiro o traslado.
13. No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
14. Utilizar herramientas de software para evadir los equipos de seguridad (firewall) del INPEC.
15. Clasificar, almacenar, archivar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
16. Ingresar a la red oscura "Dark Web" y a la red profunda "Deep Web", desde los equipos Institucionales.
17. No asistir a capacitaciones o socializaciones en relación con la seguridad de la información sin justificación.
18. Cambiar la configuración, instalar, desinstalar software o formatear los equipos móviles institucionales, sin autorización.
19. Dejar información sensible, reservada en carpetas compartidas o en lugares distintos su puesto de trabajo, obviando las medidas de seguridad.
20. Copiar los programas propiedad del INPEC, o violar los derechos de autor o acuerdos de licenciamiento.
21. Conectar a las canaletas de red microondas, secadores de cabello o planchas, como también cafeteras y todo dispositivo ajeno a la Institución.
22. Permitir que personas ajenas al INPEC, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público
23. Almacenar información personal en los equipos de cómputos del Instituto.
24. Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
25. Hacer uso de la red de datos de la Institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
26. Instalar software ilegal.
27. Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos del INPEC para beneficio personal.
28. El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones del INPEC, sin estar autorizado.

29. El que distribuya, envíe, introduzca software malicioso u otros programas de computación en la red de datos Institucional.
30. El que viole, robe o suplante datos personales de las bases de datos del INPEC.

Y todas aquellas que hubiera lugar en la presente Guía como en la Ley de Delitos Informáticos 1273 de 2009, Derechos de Autor, Propiedad Intelectual, Protección de datos personales, entre otras, como también normatividad vigente en relación a la vulneración de seguridad de la información en Colombia.

52. Cumplimiento

Los diferentes aspectos contemplados en esta guía son de obligatorio cumplimiento para los servidores públicos, visitantes y terceros colaboradores del Instituto. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, el INPEC tomará las acciones disciplinarias y legales correspondientes.

Los Directores, Subdirectores, Jefes de Oficina, Directores Regionales, Directores de Establecimientos de Reclusión del Orden Nacional y Director escuela de Formación, deben:

1. Garantizar y verificar la aplicación de las recomendaciones y buenas prácticas de seguridad de la información y todo documento asociado al Sistema de Gestión de Seguridad SGS en sus oficinas/áreas.

Anexos

• PA-TI-G02-F01 V2 Acuerdo de Confidencialidad, Compromiso y no divulgación de la Información.

• PA-TI-G02-F02 V1 Solicitud de Creación y/o Modificación de Permisos de Usuario y Contraseña de Sistemas de Información

• PA-TI-G08 Guía Roles y Responsabilidades para la Seguridad de la Información

• PA-TI-PL02 V2 Política de Tratamiento y Protección de Datos Personales

• PA-TI-G03-F01 Autorización otorgada por el titular para el tratamiento de datos personales

• PA-TH-P28 Procedimiento para la entrega del puesto de trabajo versión oficial

• Guía No. 4 Roles y Responsabilidades de MINTIC

Lista de Versiones

Versión	Fecha de Emisión	Motivo de la Modificación	Modificaciones
1	26/Ene/2017	Creación nuevo documento	N.A
2	14/Ago/2018	Se incluye formato Acuerdo de Confidencialidad	Los acuerdos de confidencialidad deben celebrarse con los servidores públicos, judicantes, practicantes, pasantes y/o proveedores que tengan acceso a información sensible, contemplando así la necesidad de protección de la información del Instituto.
3	17/Mar/2022	Actualización de controles, acuerdo de confidencialidad y creación de formato.	Se actualiza y se incluyen nuevos controles para proteger la información Institucional y mitigar el impacto de los riesgos de seguridad d ela información. Se actualiza el acuerdo de confidencialidad y compromiso con la seguridad de la información, se amplía su alcance y se crea formato Solicitud de Creación y/o Modificación de Permisos de Usuario y Contraseña.

Elaboró	Revisó	Aprobó
Nombre: María Cristina Reyes Castillo **Cargo:** Técnico Operativo **Fecha:** 30/Nov/2022	**Nombre:** Alberto Mejía Jiménez **Cargo:** Profesional Especializado **Fecha:** 30/Nov/2022 **Nombre:** Juan Manuel Riaño Vargas **Cargo:** Jefe Oficina Asesora de Planeación **Fecha:** 30/Nov/2022	**Nombre:** Adriana Cetina Hernández **Cargo:** Jefe Oficina Sistemas de Información **Fecha:** 30/Nov/2022