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 del Instituto Nacional Penitenciario y Carcelario.

Marco Legal

• Ver normograma del Instituto Nacional Penitenciario y Carcelario .

Glosario

- **Acción correctiva:** medida de tipo reactivo orientada a corregir un problema real detectado y evitar su repetición.
- **Acción preventiva:** medida de tipo pro-activo orientada a prevenir posibles problemas y evitar su probable aparición.

- **Acuerdo de confidencialidad:** documento en que los funcionarios del INPEC 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.

- **Activo de información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del instituto y, en consecuencia, debe ser protegido.

- **Amenaza informática:** toda circunstancia, evento o individuo que tiene el potencial de causar daño a un sistema en forma de hurto, plagio, destrucción, divulgación, modificación de datos o denegación de servicio.

- **Antispam:** producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios.

- **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.

- **Caballo de Troya:** código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de Troya tienen códigos maliciosos que cuando se activan causa pérdida y robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

- **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.

- **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.

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

- **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.

- **ISO:** Organización Internacional de Estandarización

- **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. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

- **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.

- **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.

- **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.

- **Titular:** funcionario 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.

- **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. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam 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 la forma como funciona una computadora, sin permiso o conocimiento del usuario. Están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

- **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, es un documento construido para implementar, mejorar continuamente e innovar la seguridad de la información que suministra la orientación y recomendaciones y herramientas, que permiten la construcción de una cultura de Seguridad de la Información.

2. Compromiso de la Dirección General

La Dirección General del Instituto Nacional Penitenciario y Carcelario - INPEC - 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. Sanciones para las infracciones al Sistema de Gestión de Seguridad de la Información.

El Sistema de Gestión de Seguridad de la Información pretende instituir y afianzar la cultura de seguridad de la información entre los funcionarios administrativos, del cuerpo de custodia y vigilancia, contratistas, personal externo y proveedores del INPEC. En el caso de que se constate alguna infracción de las directrices establecidas en la presente guía, se sancionará al infractor de acuerdo a lo establecido en el Decreto 407 de 1994 y ley 734 de 2002, aplicando medidas que van desde lo administrativo, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias.

4. Seguridad en relación al acceso de sistemas de información por partes externas.

El INPEC establece mecanismos de vigilancia en sus relaciones con entes externos; con el propósito de asegurar que la información que es consultada por partes externas debe cumplir con las normas y operaciones de seguridad de la información, aplicadas a contratistas, proveedores, consultores y en general a los usuarios de la información.

- La Oficina de Sistemas de Información con el apoyo de la Oficina Asesora Jurídica, establece acuerdos de confidencialidad y de intercambio de información con los que deben cumplir las partes externas o proveedores de servicios informáticos.
- El Grupo Administración de las Tecnologías de la Información de la Oficina de Sistemas de Información, debe establecer las normas de conexión a la red 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.
- Toda información, utilizada, manejada, tratada o consultada en las bases de datos del Instituto, por terceros, es propiedad del INPEC y por ningún motivo debe ser modificada, reformada o utilizada para fines fraudulentos.
- 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.

5. Concienciación de funcionarios y/o contratistas.

Es necesario sensibilizar a los funcionarios, y/o contratistas frente a las amenazas y debilidades con respecto a la seguridad de la información, así mismo dar a conocer las responsabilidades y deberes, para apoyar la ejecución de las normas y recomendaciones del Sistema Gestión de Seguridad de la Información durante su vinculación a la entidad.

- La Subdirección Talento Humano en el programa de inducción; debe incluir la capacitación en el cumplimiento del Sistema de Gestión de Seguridad de la Información, complementándolo con un acuerdo de confidencialidad soportado y firmado por los funcionarios al momento de vincularse al Instituto.

- 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.
- La Oficina Control Interno Disciplinario, debe aplicar el proceso disciplinario del Instituto cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información por parte de los funcionarios.
- 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.
- Los recursos tecnológicos y de software asignados a los funcionarios del INPEC son responsabilidad de cada funcionario.

6. Acceso de funcionarios y/o contratistas a los sistemas de información.

Al momento de la vinculación del funcionario deberá solicitar el acceso a los sistemas de información así mismo al momento de su desvinculación deberá solicitar la cancelación del acceso autorizado.

- La Subdirección Talento Humano debe enviar mensualmente a la Oficina Sistemas de Información el listado de los diferentes estados de los funcionarios (vinculación, licencias, incapacidades entre otros), para la correspondiente activación o en su defecto desactivación del usuario a los sistemas de información.
- La Oficina Sistemas de Información debe asegurar que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean habilitados, inhabilitados o eliminados de los sistemas de información.
- El funcionario al registrarse en los diferentes sistemas de información del Instituto, como correo electrónico, Intranet, Sisipec, Sistema de ingreso y salida, desprendible de pago, etc.; le permite realizar sus labores de manera efectiva y eficiente presentando la información en tiempo real.
- 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 ésta recomendación será una infracción a la seguridad de la información.
- 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.
- Una vez finalizada la relación contractual bien sea contratista ó funcionario, según sea el caso, el acceso a su equipo de trabajo debe ser bloqueado con una 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.
- Los servidores públicos y/o contratistas deben realizar la devolución de las herramientas de trabajo que tienen bajo su responsabilidad una vez cese la relación contractual o cuando existan traslados por necesidades del servicio, entrega que se hará al Grupo de Manejo de Bienes e Inmuebles del Instituto o el encargado en el establecimiento. Al igual se debe realizar la entrega del carné a la Subdirección de Talento Humano.

7. Seguridad física y del entorno

La seguridad física y del entorno pretende prevenir el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información del Instituto.

- El Grupo Logístico de la Dirección Gestión Corporativa, debe garantizar la protección del perímetro de las instalaciones físicas donde laboran los funcionarios, controlar el acceso de los funcionarios y visitantes, así como el acceso a áreas restringidas, además de mitigar los riesgos de amenazas internas, externas y ambientales.
- La Oficina de Sistemas de Información, debe velar porque los recursos de la plataforma tecnológica del Instituto ubicados en el centro de cómputo o centros de cableado se encuentren protegidos contra fallas o interrupciones eléctricas.
- Las áreas restringidas respecto a los sistemas de la información se protegerán mediante el empleo de controles de acceso físico, los que serán determinados por la Oficina de Sistemas de Información, a fin de permitir el acceso sólo al personal autorizado.
- Los funcionarios y/o contratista 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; 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.
- El carné institucional es personal e intransferible.
- El uso indebido del carné Institucional se sancionará de acuerdo con las normas legales y reglamentarias vigentes.
- El visitante debe registrarse en el sistema de ingreso y salida y portar en un lugar visible el sticker generado por el mismo sistema y estar acompañado por un funcionario o contratista según sea el objeto del ingreso al Instituto
- El personal de empresas contratistas que desempeñen funciones en el Instituto; deben estar identificados con carné, chalecos o distintivos y acompañados por funcionarios del Instituto y a cargo de los supervisores del contrato.

8. 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.

- El Grupo de Manejo de Bienes e Inmuebles de la Dirección Gestión Corporativa debe llevar a cabo el levantamiento y la actualización permanente del inventario de activos físicos al interior de Instituto.
- La Oficina de Sistemas de Información, es la responsable de 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, a su vez es responsable de generar copias de seguridad.
- Para la adquisición de equipos informáticos, software o tecnología debe contar con la ficha técnica suministrada por la Oficina de Sistemas de Información (Grupo Administración de las Tecnologías de la Información). Para realizar la adquisición de los mismos.
- La información del Instituto, como los activos donde ésta se almacena y se procesa (Equipos de cómputo o dispositivos tecnológicos) deben ser asignados y administrados bajo un responsable e inventariados.
- Los responsables y/o administradores de la información, archivos físicos, manejo de sistemas de información, seguridad electrónica o servicios tecnológicos tales como computadores, equipos portátiles, servidores, fotocopiadoras, escáner, impresoras, internet, redes, correo electrónico, aplicaciones,

herramientas de acceso remoto, teléfonos, dispositivos móviles, video beam entre otros, son propiedad del Instituto y son suministrados a los funcionarios 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.

- 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 (virus), propaganda política, material religioso o cualquier otro que no esté autorizado.

9. Acceso a la información pública (clasificada y reservada)

Asegurar que la información reciba un nivel apropiado de protección de acuerdo a su importancia.

- Siguiendo directrices de Gobierno en Línea, el Instituto Nacional Penitenciario y Carcelario definirá los niveles más adecuados para clasificar y manejar la información con base a los criterios de seguridad: confidencialidad, integridad y disponibilidad de la información, para garantizar que los usuarios autorizados tengan acceso a la información cuando esta sea solicitada.
- El Grupo Administración de las Tecnologías de la Información de la Oficina Sistemas de Información debe proveer las herramientas tecnológicas para el respectivo almacenamiento de la información.
- Los usuarios 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.
- Está prohibido la toma de fotografías a documentos propiedad de la entidad.
- El dueño de la información es el único responsable de su protección.
- Sea precavido en el transporte y almacenamiento de la información, tanto a nivel digital como físico.
- Proteja la información de la Institución incluso fuera del ámbito de la entidad.
- Para mayor información remítase a la Circular No.020 del 30 agosto de 2016. "Derecho de acceso a la información pública (clasificada y reservada) e insistencia".

10.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.

- La Oficina de Sistemas de Información es quien genera las contraseñas para el ingreso a los sistemas de información; 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.
- La Oficina Asesora de Planeación, crea contraseña para el uso del sistema de información de Isolución.
- Las contraseñas se utilizan para permitir o denegar el acceso a un recurso.
- Los funcionarios 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.
- 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).
- No utilice datos personales o de seres queridos para formar la contraseña. (Nombre, fecha de cumpleaños, aniversario, graduación, artistas favoritos, novio/novia, mascotas, etc.).
- No use contraseñas completamente numéricas con algún significado (teléfono, cédula de ciudadanía, fecha de nacimiento, placa del automóvil, etc.).

- 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.
- Evite la contraseña por correo electrónico, mencionarla en conversaciones.
- No utilice la contraseña en equipos no confiables o públicos, como un café Internet.

Ejemplo de algunas contraseñas seguras:

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

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

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

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

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

f. 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:

a. La protección de la contraseña recae en el funcionario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

b. Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

c. 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.

11. Equipo informático de usuario desatendido.

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 concientizar, exigir a los funcionarios las responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación con el uso y la seguridad del equipo del usuario.
- Los usuarios deben 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.
- Los equipos tecnológicos (computador, escáner, etc.), serán utilizados sólo por el responsable asignado a ellos, y no por otro funcionario ajeno a la dependencia.

12. Uso y servicio de impresoras y fotocopiadoras.

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

- La Oficina Sistemas de Información 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.
- 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 según sea el caso.
- El uso de impresoras y fotocopiadoras, son sólo de carácter institucional y no personal.
- 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.
- 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.
- Separe o airee el papel con cuidado antes de colocarlo en la bandeja, esto evitará atascamientos
- El funcionario 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.
- Nunca 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.
- Reduzca al máximo el uso de impresoras. Imprimir sólo lo imprescindible, y utilizar más el correo electrónico.
- Imprimir por ambas caras del papel.
- Revise que el papel no contenga ganchos o elementos extraños que pueden dañar la impresora.

13. Uso de periféricos y medios de almacenamiento

Establecer técnicas para la utilización de periféricos y medios de almacenamiento para prevenir la pérdida de información.

- La Oficina Sistemas de Información reglamentará 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.
- 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 funcionario solicitante y con visto bueno de su jefe inmediato.
- 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.
- Los funcionarios del Instituto 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.

14. Escritorio despejado y pantalla despejada.

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 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.
- 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 de la Oficina de Sistemas de Información. Para lo anterior, la Oficina Asesora de Comunicaciones debe diseñar el protector de pantalla.
- 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.
- Toda información crítica deberá ser guardada en lugares seguros, archivadores bajo llave.
- el usuario debe clasificar y protege los objetos e información susceptible de pérdidas.
- Los funcionarios deben cerrar los cajones de su escritorio bajo llave.
- La pantalla de autenticación a la red del Instituto debe requerir solamente la identificación de la cuenta y una clave.
- 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.
- El usuario debe 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.
- En caso que se utilice portátiles para presentaciones, si éste fuera de uso corporativo, debe eliminarse la información antes presentada.
- Al finalizar la jornada laboral, el funcionario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, así mismo desconectar los equipos tecnológicos que estén a su cargo.
- Las salas o áreas de reuniones, salas de conferencias y de capacitación, deben quedar limpias de todo el material utilizado.

15. Conexión a la red de datos y eléctrica.

Evitar el acceso no autorizado a servicios en red.

- La Oficina de Sistemas de Información, velará 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.
- 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 de la Información de la Oficina Sistemas de Información.
- Los usuarios deben emplear los puntos de red, para la conexión de equipos informáticos autorizados por el Instituto.
- 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.

- La instalación, activación y gestión de los puntos de red es responsabilidad de la oficina Sistemas de Información.
- 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.
- 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.
- No bloquee los puntos de red de datos y eléctricos con carpetas, cajas, escritorios, etc.
- Cuando detecte un uso no adecuado de la red por favor, informe inmediatamente a la Oficina Sistemas de Información.
- Las redes deberán ser gestionadas e inspeccionadas para proteger la información en los sistemas y aplicaciones, por parte de la Oficina de Sistemas de Información.

16. Uso de conexiones remotas.

Ofrecer acceso remoto para gestionar equipos con medidas de seguridad.

- La Oficina de Sistemas de Información debe establecer conexiones remotas seguras dentro de la plataforma tecnológica del Instituto.
- 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.
- Todo usuario autorizado para conexiones remotas VPN debe con antelación firmar un acuerdo de confidencialidad para hacer uso de la información.
- Estas conexiones únicamente se deben permitir a personal interno o externo con periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- 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.
- 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 funcionario o contratista que requiera del soporte apruebe dicha conexión hacia el equipo de cómputo asignado para sus labores.

17. Copia y respaldo de la información

Con el fin de mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información, tenga en cuenta las siguientes normas y buenas practicas:

La Oficina de Sistemas de Información debe:

- Documentar los procedimientos para la generación de copias de respaldo, almacenamiento y restauración de información sensible para el Instituto, facilitando los medios necesarios; estableciendo operaciones y mecanismos para la realización de estas actividades.
- Generar las copias de seguridad de los servidores de red y bases de datos, o demás servicios identificados como críticos, en horas no laborables para la entidad. Como también mantiene un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas del Instituto, disponiendo de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física con su respectiva fecha de reproducción, puntualizando las condiciones de

transferencia o transmisión y custodia de las copias de respaldo de la información en caso que sean almacenadas externamente.

- Ejercer control sobre las operaciones de restauración de las copias de seguridad de la información de las bases de datos o diferentes aplicativos existentes en el Instituto. Para garantizar la disponibilidad de la información en caso de contingencia o desastre.
- Restaurar las copias de seguridad de información de los equipos de los funcionarios, una vez el funcionario haya realizado el respectivo oficio dirigido a la Oficina de Sistemas de Información. Los funcionarios y contratistas no deben:
- Almacenar en los discos duros de los equipos de trabajo información personal u otra que no haga parte del desarrollo laboral.

18. Protección de los datos personales y privacidad de la información.

En cumplimiento de la Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, el Instituto Nacional Penitenciario y Carcelario velará por el correcto desempeño de la protección de los datos personales 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, proveedores y demás terceros de los cuales reciba y administre información.

- La protección de datos son las medidas que se toman, tanto a nivel técnico como jurídico, para garantizar que la información de los usuarios de la entidad o de cualquier base de datos, esté segura de cualquier ataque o intento de acceder a esta, por parte de personas no autorizadas.
- Así mismo, buscará proteger la privacidad de los datos que pertenecen a la vida privada y familiar de sus funcionarios, 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 funcionarios o terceras partes sin autorización o sin una orden judicial.
- Si usted es titular de la información debe tener claridad dónde se encuentran sus datos personales actualmente, saber quién custodia sus datos personales, conocer qué personas tienen acceso a su información personal, conocer los mecanismos legales con que puede defender sus derechos de información ante las entidades ya sean públicas o privadas, e identificar sus bases de datos.
- Debe saber que su información constituye un derecho y sobre ella usted tiene el poder de decidir, quién la tiene, en qué condiciones y hasta cuándo.
- La importancia de los datos personales radica en que la información personal puede ser utilizada para varios fines, como la comercialización, la vida laboral, e incluso para cometer delitos, ya que su identidad puede ser suplantada si es que se tiene acceso a la información adecuada.
- La Oficina de Sistemas de Información debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, 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.
- La Oficina Sistemas de Información, protegerá los datos de prueba que se entregarán a los desarrolladores externos, asegurando que no revelen información confidencial de los ambientes de producción.

- La Subdirección de Talento Humano en conjunto con el Grupo Administración Historias Laborales son los responsables de los datos personales de los funcionarios que reposan en la historia laboral para que sean tratados con la seguridad e integridad necesaria.

- Es deber de los funcionarios, guardar reserva de la información personal o del Instituto en ejercicio de sus funciones y evitar su divulgación por medios telefónicos, correo electrónico, entre otros. En caso de no identificarse la persona o no justificar su solicitud abstenerse de entregar información salvo a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios y contractuales del Instituto.
- Los funcionarios del Instituto deberán acceder únicamente a los datos que se requieran para el desarrollo de las funciones, guardando estricta reserva y no divulgarlos más allá de lo estrictamente necesario.
- Los funcionarios del Instituto no deberán retirar de la entidad ninguna clase de datos sin autorización expresa del director de establecimiento, regional o jefe de oficina.

19. Licenciamiento de Software

La Oficina de Sistemas de Información debe:

- Vigilar que el software instalado cumpla con los requisitos legales y de licenciamiento necesarios. A su vez establece 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.
- Estarán bajo custodia de la Oficina Sistemas de Información y de las áreas de sistemas de las regionales y establecimientos los 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.
- 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 ésta práctica no está autorizada.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.
- Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor.
- 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 regionales o establecimiento de reclusión; de no realizar esta acción las partes involucradas estarán sujetas a sanciones administrativas de orden disciplinario o penal, de acuerdo a las circunstancias.
- 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 funcionarios o contratistas.

20. Ubicación y protección de los equipos

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

- El Grupo Administración de las Tecnologías de la Información, en conjunto con los Directores Regionales, Directores Establecimientos de Reclusión y los Jefes de Oficina y/o dependencia debe 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.
- La Oficina Sistemas de Información, los directores regionales y directores de establecimientos son los únicos facultados para autorizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario 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.

- Los soportes técnicos deben ser atendidos por el personal de la Oficina de Sistemas y áreas de sistemas de las regionales y/o establecimientos de una forma eficaz y oportuna con un tiempo de respuesta acorde a las solicitudes.
- 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 ó regionales
- En caso de pérdida o robo de un equipo de cómputo del Instituto, se debe informar de forma 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.
- No tape los orificios de ventilación de los equipos de cómputo. El calor es su peor enemigo.
- Se prohíbe que los visitantes manipulen o manejen los equipos de cómputo del Instituto sin previa autorización del dueño, responsabilidad que recae sobre el funcionario propietario del equipo en el caso de fuga o sustracción de información, daño o pérdida de elementos.
- No ingiera alimentos o bebidas sobre equipos informáticos, teclado o CPU
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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 funcionarios.

21. Uso del correo electrónico

Con el fin de garantizar la seguridad y utilización del servicio del correo electrónico, implemente las siguientes recomendaciones:

- Los servicios de correo electrónico son administrados por la Oficina Sistemas de Información. Para el enlace el proveedor es el responsable de garantizar su disponibilidad, en un 100%. El correo electrónico tiene como objeto apoyar las funciones de comunicación, entre los funcionarios y terceros proporcionado un servicio seguro, eficaz y eficiente.
- El correo electrónico Institucional en sus mensajes debe llevar una sentencia de confidencialidad que será diseñado por la Oficina Asesora de Comunicaciones y publicado por los usuarios al momento de activarse la cuenta. Se debe respetar el estándar de la imagen corporativa definidos por el INPEC.
- La cuenta de correo electrónico asignada a los funcionarios es de carácter particular; por consiguiente, ningún funcionario del Instituto o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- 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.

- 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.
- Ningún usuario externo a la Institución, puede usar los servicios del correo electrónico proporcionado por la red del Instituto.
- 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.
- Utilice la función de correo no deseado para aquellos mensajes de publicidad, ventas, etc.
- 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.
- 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.
- No publique su correo electrónico 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.
- 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.

- 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 presente que las empresas, no adjuntan archivos en sus actualizaciones de productos. El envío de archivos con supuestas actualizaciones se constituye en un tipo de engaño muy común hoy día para propagar malware a través del correo. Del mismo modo la organización bancaria y financiera, nunca le solicitará información personal por medio del correo. Si llega a recibir un mensaje de este tipo, tenga cuidado ya que pude ser víctima de un ataque de phishing que busque robarle sus datos. En estos casos denuncie el hecho en su entidad financiera de confianza.
- Por último 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

22. Uso adecuado de Internet

Para navegar en Internet de una manera objetiva y segura:

- La Oficina de Sistemas de Información debe 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%.
- La Oficina de Sistemas de Información se reserva el derecho de monitorear los accesos al servicio de Internet de los funcionarios o contratistas del INPEC, 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.

- Los privilegios de uso de internet estarán de acuerdo a la necesidad de acceso que requiera cada funcionario con base a su desempeño laboral.
- Los usuarios del servicio de Internet del INPEC, deben hacer uso del mismo de forma razonable en relación con las actividades laborales que así lo requieran.
- El usuario no debe descargar ningún programa o software tales como: software de evaluación, archivos de música (MP3, WAV, etc.) videos, juegos, películas, protectores, fondos de pantalla, 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.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos, mensajería instantánea o redes sociales como facebook, kazaa, msn, hotmail, skype, y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del Instituto.
- Evite acceder a sitios desconocidos o no confiables.
- No acepte la instalación automática de software.
- El Director o Jefe de oficina o dependencia será informado sobre el mal uso que se le está dando a Internet en su área.

23. Manejo de antivirus

Para proteger la integridad del software y de la información.

El Grupo Administración de las Tecnologías debe:

- 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 entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.
- Velar porque todos los equipos de cómputo del Instituto tengan instalado el software de antivirus con su respectiva licencia actualizada.
- 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.

Los usuarios deben:

- 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 funcionario del INPEC, distinto al personal de la Oficina Sistemas de Información o funcionarios encargados del área de sistemas de establecimientos o regionales, deberá intentar erradicarlos de los Pc.
- Notificar si detectan alguna infección por software malicioso a la Oficina Sistemas de Información, o a las áreas de sistemas de los establecimientos, para que tomen las medidas de control correspondientes.

- 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.
- Comunicar si el software antivirus no está actualizado o no funciona correctamente a la Oficina Sistemas de Información o en su defecto con las áreas encargadas de Sistemas de su establecimiento o regional.

24. Control de acceso Centro de Cómputo.

Para garantizar los servicios de procesamiento, información y comunicaciones de una manera segura al interior del Instituto.

La Oficina de Sistemas de Información , ERON, y regionales deben:

- Implementar y velar por las integridad física externa e interna 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 y programas.
- 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.
- 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 funcionario autorizado.
- Velar porque los controles y otros mecanismos de seguridad de acceso a las áreas solo sean utilizados por los funcionarios autorizados; salvo en situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran.
- Los centros de cómputo destinados al procesamiento o almacenamiento de información sensible, reservada o crítica, así como aquellas en las que se encuentren los equipos y demás, son consideradas áreas de acceso restringido.
- 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 funcionario de dicha oficina durante su visita al centro de cómputo o los centros de cableado.
- El ingreso de los visitantes al centro de cómputo y a los centros de cableado debe quedar registrado en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Queda estrictamente prohibido sustraer equipos o materiales propiedad del centro de cómputo sin previa autorización por la oficina encargada.
- Se debe mantener un inventario físico de los equipos y accesorios existentes.
- Se prohíbe ingresar alimentos de cualquier tipo al centro de cómputo.
- Los administradores del centro de cómputo debe llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.

25. Intercambio de información con terceras partes.

Sobre el intercambio de información se deben implementar las siguientes prácticas para mantener la seguridad de la información y del software que se intercambian dentro del Instituto o con cualquier entidad externa.

- Las Oficinas o dependencias del Instituto deben aplicar acuerdos de confidencialidad para el intercambio de la información o software entre el Instituto y partes externas según sea el caso.
- Cuando se realicen acuerdos de Intercambio de información y software entre organizaciones o entidades, se especificará el grado de sensibilidad de la información del Instituto Nacional Penitenciario y Carcelario y las consideraciones de seguridad sobre la misma.
- La firma de los acuerdos de confidencialidad entre las partes, debe garantizar la total reserva de la información, así como los alcances frente al tratamiento y divulgación de la información.
- El Grupo Gestión Documental debe 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.
- La Información disponible al público debe estar protegida para evitar la modificación no autorizada, y así conservar su integridad.
- 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.

26. 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.

- 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.
- 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.

Los usuarios deben:

- Recibir y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de los mismos.
- Dar aviso al Grupo de Presupuesto de la Dirección Gestión Corporativa en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- 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.
- Devolver el Token asignado a la Dirección del establecimiento cuando el vínculo laboral con el Instituto del funcionario se dé por terminado o haya cambio de cargo, el cual será requerido para legalizar la finalización del vínculo con el Instituto.
- 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.
- 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 funcionarios del Instituto. En caso de que suceda algún evento irregular con los Token los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

- 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.
- 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
- No abra el Token. Éste es un dispositivo de seguridad y al intentar abrirlo lo dañará de manera permanente.
- Cierre la sesión cuando termine de hacer sus transacciones.
- 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.

27. Uso de dispositivos móviles Institucionales

Para garantizar y adoptar medidas de seguridad de la información cuando se utilicen dispositivos móviles Institucionales.

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

Los usuarios deben:

- Utilizar los minutos o tiempo al aire asignados a los dispositivos móviles exclusivamente para uso Institucional.
- Realizar la devolución de los dispositivos móviles institucionales asignados en estado operativo al grupo de Bienes Muebles e Inmuebles cuando el vínculo laboral con el Instituto se dé por terminado o haya cambio de cargo.

Los usuarios deben evitar:

- 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
- Hacer uso de redes inalámbricas de uso público
- Almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
- La instalación de programas o software en los dispositivos móviles desde fuentes desconocidas.

28. Sincronización de relojes

- Los relojes de los sistemas de procesamiento de información dentro de la Institución o del dominio de seguridad deben estar sincronizados 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.

29. Acceso a Sistemas Operativos

- Con el fin de evitar el acceso no autorizado a los sistemas operativos, la Oficina Sistemas de Información debe asegurar que las contraseñas que traen por defecto los sistemas operativos no sean utilizados, incluyen el firewall y las bases de datos.

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

Implemente las siguientes normas y buenas prácticas para garantizar que la seguridad sea parte integral de los desarrollos, adquisiciones y mantenimiento de los sistemas de información de esta manera se previene pérdida, modificaciones o uso inadecuado de los mismos sistemas de aplicación.

El Grupo Administración de la Información:

- 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. Como también debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.
- 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.
- 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).
- 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.

La Oficina de Sistemas de Información:

- Será la única dependencia con la capacidad de avalar y/o adquirir software de acuerdo a los requerimientos de las demás direcciones, establecimientos o regionales. 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.
- Certifica que todo sistema de información adquiridos o desarrollados utilicen herramientas licenciadas.
- 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

Los programadores deben :

- 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.
- Proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Suministrar opciones de cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión.
- 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.

- Evitar divulgar la información de la estructura de directorios de los sistemas de información construidos sin previa autorización.

Otros:

- El software proporcionado o desarrollado por el Instituto no puede ser copiado o suministrado a terceros sin previa autorización.
- Toda contraseña de aplicativos desarrollados o adquiridos con terceros deben ser protegidas contra copia o divulgación no autorizada mediante almacenamiento cifrado en las bases de datos.
- Todo software que se vaya a adquirir y/o conectar a la plataforma tecnológica del Instituto, por cualquier dependencia o proyecto del INPEC, deberá ser gestionado 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.

31. Cumplimiento

Los diferentes aspectos contemplados en esta guía son de obligatorio cumplimiento para los funcionarios, visitantes, contratistas y terceros colaboradores del Instituto.

Los Directores, Subdirectores, Jefes de Oficina, Directores Regionales, Directores de Establecimientos, deben garantizar y verificar la aplicación de las recomendaciones y buenas prácticas de seguridad de la información en sus áreas/dependencias/oficinas.

Anexo

PA-TI-G02-F01 V01 Acuerdo de Confidencialidad y Compromiso con la Seguridad de la Información

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 funcionarios, contratistas y/o proveedores que tengan acceso a información sensible, contemplando así la necesidad de protección de la información del Instituto.

Elaboró		Revisó		Aprobó	
Nombre:	María Cristina Reyes Castillo	**Nombre:**	Juan Manuel Riaño Vargas	**Nombre:**	Adriana Cetina Hernández
Cargo:	Auxiliar Administrativo	**Cargo:**	Jefe Oficina Asesora de Planeación	**Cargo:**	Jefe Oficina Sistemas de Información
Fecha:	14/Ago/2018	**Fecha:**	16/Ago/2018	**Fecha:**	17/Ago/2018

	Nombre:	Angelica María Patiño García	
	Cargo:	Profesional Especializado	
	Fecha:	15/Ago/2018	