TABLA DE CONTENIDO

1. OBJETIVO

Definir y comunicar a las partes interesadas las políticas y lineamientos de Seguridad de la Información que deben ser aplicados por parte de todos los colaboradores de Parques Nacionales Naturales de Colombia, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad, tomando como referencia la Norma ISO/IEC 27001:2013 y su anexo A.

2. ALCANCE

Las políticas definidas en el presente documento aplican para todos los procesos de la Entidad, los activos definidos a través del Inventario de Activos de Seguridad de la Información y las partes interesadas que acceden, almacenan, distribuyen y/o eliminan información de Parques Nacionales Naturales de Colombia.

3. DEFINICIONES, ABREVIATURAS O SIGLAS

A continuación, se presenta la definición de algunos términos que se utilizan en el desarrollo del documento:

Activo de Información:	Cualquier elemento que contenga, datos que tienen valor para uno o más procesos de la organización y debe protegerse. (ISO/IEC 27001:2013).
Anexo A en ISO 27001:	Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.
Archivo:	Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión conservados, respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia
Ataque:	Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo (ISO/IEC 27000:2018).
Bluetooth:	Protocolo de comunicaciones que sirve para la transmisión inalámbrica de datos (fotos, música, contactos…) entre diferentes dispositivos que se hallan a corta distancia.
Colaborador:	Con este nombre se hace referencia a la persona que tiene cualquier tipo de vínculo contractual, legal y reglamentario con Parques Nacionales Naturales de Colombia, esto incluye servidores públicos, proveedores, contratistas, estudiantes en práctica, estudiantes en pasantía y cualquier persona a la que le sea asignada una responsabilidad por parte de Parques Nacionales naturales de Colombia.
Computación en la nube:	Modelo mediante el cual se habilita el acceso a recursos de procesamiento y almacenamiento de información a través de una red (habitualmente internet), de manera escalable y flexible, permitiendo el auto aprovisionamiento y administración.

Confidencialidad:	Propiedad de la información que garantiza no estar disponible o ser divulgada a personas, Entidades o procesos no autorizados. (ISO/IEC 27000:2018).
Control:	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de Seguridad de la Información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (MinTIC- Modelo de Seguridad y Privacidad de la Información 2016).
Control de acceso:	Garantizar que el acceso a los activos esté autorizado y restringido según los requisitos de negocio y de seguridad. (ISO/IEC 27000:2018)
CVE (Vulnerabilidades y exposiciones comunes):	Lista de vulnerabilidades y exposiciones de seguridad de la información.
Datos Personales:	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012).
Disponibilidad:	Propiedad de la información que garantiza el ser accesible y usable de acuerdo con lo requerido por una Entidad autorizada. (ISO/IEC 27000:2018).
Equipo de cómputo:	Dispositivo electrónico para procesamiento de información controlado por programas de software.
Etiquetar / Marcar:	Procedimiento mediante el cual se rotula un activo de información físico o digital utilizando una convención que identifica su clasificación para confidencialidad, integridad y disponibilidad. El término “etiquetar”, al cual hace referencia la Norma ISO 27001:2013, se cambia para efectos del presente documento por “marcar”, lo anterior teniendo en cuenta que el Proceso de Gestión Documental adoptó el término “etiquetar” con una connotación diferente.
Evento de Seguridad de la Información:	Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad. (ISO/IEC 27000:2018).
Firewall (cortafuego):	Dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
GPO:	conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo dentro de un dominio organizacional

Incidente de Seguridad de la Información:	Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información-
Indicador:	Medida que proporciona una estimación o evaluación (ISO/IEC 27000:2018).
Integridad:	Propiedad de exactitud y completitud de la información que contienen los activos de información. (ISO/IEC 27000:2018).
IPS:	Sistema de Prevención de Intrusiones, su función es proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva.
OWASP:	Open Web Application Security Project. Está dedicado a la búsqueda y la lucha contra las vulnerabilidades en el software. La **OWASP** Foundation es una organización sin ánimo de lucro que proporciona la infraestructura y apoya a este trabajo.
Parte Interesada:	Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. (ISO/IEC 27000:2018).
Rollback:	Operación que devuelve cambios generados en los sistemas de información.
Servicios:	Servicios de computación y comunicaciones, tales como los de consulta, correo electrónico, mensajería instantánea, videoconferencia, herramientas colaborativas y streaming, entre otros que sean prestados por un tercero.
Sistema de Gestión de Seguridad de la Información - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
VPN:	Virtual Network protocol.
Vulnerabilidad:	Debilidad de un activo o control que puede ser explotado por una o más amenazas.
Wifi:	Mecanismo que permite, de forma inalámbrica, el acceso a Internet de distintos dispositivos al conectarse a una red determinada.
Primera Línea de Defensa:	corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad
Segunda Línea de Defensa:	está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección
Tercera Línea de Defensa:	está conformada por la Oficina de Control Interno, quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa

que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa

4. MARCO LEGAL Y TÉCNICO

ISO 27001:2013: Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización.

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

5. LINEAMIENTOS GENERALES

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, servidores públicos, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con Parques Nacionales Naturales de Colombia, para el correcto cumplimiento de sus funciones y para dar un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual.

Para la implementación de la Política de Seguridad y Privacidad de la Información a manera de lineamientos, directrices y prohibiciones se define un conjunto de políticas para la adopción de los controles relacionados con seguridad de la información y la seguridad digital, los cuales se construyen de acuerdo con las características particulares para Parques Nacionales Naturales de Colombia, sus activos de información, sus procesos y los servicios de información que presta.

Todo el personal de Parques Nacionales Naturales de Colombia y/o Proveedores, tienen la responsabilidad de cumplir con lo establecido en este Manual de Políticas de Seguridad de la Información.

El responsable de Seguridad de la Información tiene como función velar por el cumplimiento de las políticas establecidas, este responsable debe ser designado por la Alta Dirección a través del Manual del Sistema de Gestión Integrado.[1]

La Política General de Seguridad de la Información (Seguridad Digital) se compone de un subsistema que hace parte del Sistema de Gestión Integrado de PNNC aprobado mediante resolución 0186 del 16 de junio de 2020.

[1] https://senda.parquesnacionales.gov.co/senda/doc/usrdoc?soa=12&mdl=doc&_sveVrs=1001620240305&&docId=2933&float=t&float=t#

6. DESARROLLO

6.1 POLÍTICA SEGURIDAD DE LA INFORMACIÓN (A[2].6.1)

La Dirección de Parques Nacionales Naturales de Colombia reconoce la importancia de identificar y proteger los activos de información de la entidad. Para ello, evitará la destrucción, divulgación, modificación y utilización no autorizada de dicha información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

La Alta dirección de Parques Nacionales Naturales de Colombia declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

Para Parques Nacionales Naturales de Colombia, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de minimizar un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la entidad según como se define en el alcance, sus servidores públicos, contratistas, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema de Gestión de Seguridad de la Información estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en los tres niveles funcionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en todos los niveles funcionales de Parques Nacionales Naturales de Colombia
- Asegurar la continuidad del negocio de la entidad frente a incidentes.

La Seguridad de la Información se caracteriza como la preservación de:

- **Confidencialidad,** asegurando que solo quienes estén autorizados puedan acceder a la información.
- **Integridad**, asegurando que la información y sus métodos de proceso sean exactos y completos.
- **Disponibilidad**, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura. Estos controles deberán ser establecidos para asegurar los objetivos de seguridad de la entidad.

[2] **A.6.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

Parques Nacionales Naturales de Colombia designará un responsable de la Seguridad de la Información, quien se encargará de la guía, implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información.

La presente Política de Seguridad de la Información debe ser conocida y cumplida por todo el personal de la Institución, independiente del cargo que desempeñe y de su situación contractual.

Esta Política de Seguridad de la Información se integrará a la normativa básica de la Institución, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política, así como de los documentos relacionados a esta.

El director general de Parques Nacionales Naturales de Colombia deberá designar a un servidor público o colaborador con las competencias requeridas para desempeñar el rol de Oficial de Seguridad Digital, quien coordinará la implementación y mantenimiento del Sistema de Gestión de Seguridad de información (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) en la entidad, atendiendo las normas en materia de seguridad digital establecidas por el Ministerio de las Tecnologías de la Información (MINTIC).

Dentro de sus actividades se encuentran las siguientes:

- Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad.
- Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad

7. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

7.1 POLÍTICA DE DISPOSITIVOS MÓVILES CORPORATIVOS

Parques Nacionales Naturales de Colombia, a través del Grupo de Tecnologías de la Información y las Comunicaciones, permite el uso de dispositivos móviles al interior de sus instalaciones siempre y cuando se cumplan los lineamientos, controles y demás aspectos frente al uso de estos en la red de la entidad. Esta política aplica a todos los dispositivos y equipos móviles de los servidores públicos, contratistas o terceros de la entidad que se les haya asignado un dispositivo propiedad de la entidad y que estén autorizados para conectarse a las redes de datos de Parques Nacionales Naturales de Colombia y busca garantizar la seguridad de la información cuando se administre, transmita o almacene información de la entidad en dichos dispositivos.

7.2 POLÍTICA DISPOSITIVOS PROPIOS (BYOD)

Parques Nacionales Naturales de Colombia autorizará el uso de dispositivos BYOD para el tratamiento de información institucional. La entidad determinará mediante sus procedimientos en qué momento se considera viable autorizar el uso de dispositivos personales que no sean propiedad de la entidad para el tratamiento de la información institucional. Parques Nacionales Naturales de Colombia, a través del Grupo de Tecnologías de la Información y las Comunicaciones permite el uso de dispositivos móviles personales al interior de sus instalaciones siempre y cuando se cumplan los lineamientos, controles y demás aspectos frente al uso de estos en la red de la entidad. Esta política define las medidas necesarias para evitar que la información pública reservada o pública clasificada se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos de propiedad de servidores públicos o contratistas. Esta política

aplica a todos los dispositivos electrónicos personales tales como teléfonos inteligentes y tabletas, los computadores portátiles que no pertenecen a Parques Nacionales de Colombia pero que son utilizados por servidores públicos y contratistas para acceder o almacenar información. A estos dispositivos se les conoce comúnmente como BYOD (Bring Your Own Device – Trae tu propio dispositivo).

7.3 POLÍTICA DE TELETRABAJO

Parques Nacionales Naturales de Colombia, a través del Grupo de Gestión Humana, el Grupo de Tecnologías de la Información y las Comunicaciones y demás dependencias que se requieran deberán establecer los lineamientos, controles y demás aspectos frente al teletrabajo y/o trabajo remoto al interior de la entidad.

Esta política debe ser aplicada por todos los servidores públicos que realicen teletrabajo y/o trabajo remoto.

7.4 POLÍTICA DE CONTROL DE ACCESO

Parques Nacionales Naturales de Colombia, a través de los Líderes de los procesos o los responsables de los activos de información deberán establecer controles de acceso sobre los mismos, con el fin de protegerlos contra accesos no autorizados. Esta política debe ser aplicada por todos los servidores públicos, contratistas y terceras partes que por la naturaleza de sus funciones acceden a los activos de información de la entidad.

7.5 POLÍTICA USO CONTROLES CRIPTOGRAFICOS

Parques Nacionales Naturales de Colombia, a través del Grupo de Tecnologías de la Información y las Comunicaciones, establecerá controles criptográficos con el fin de proteger y cifrar la información al momento de almacenamiento y/o transmisión por cualquier medio y proteger la confidencialidad, la autenticidad y/o la integridad de esta.

7.6 POLÍTICA ESCRITORIO Y PANTALLA LIMPIOS

Todos los colaboradores de Parques Nacionales Naturales de Colombia deberán mantener la información objeto de su labor debidamente custodiada y salvaguardada del acceso de personas no autorizadas. El Grupo de Procesos Corporativos deberá dotar con cajoneras o archivos para el almacenamiento de la información sensible o crítica.

Los puestos de trabajo deberán permanecer organizados y la información clasificada como reservada, deberá guardarse bajo llave o en lugares vigilados mientras el colaborador responsable de la misma no esté trabajando con ella.

En cuanto a la información que se maneja en los equipos de Parques Nacionales Naturales de Colombia, los colaboradores deberán conservar la pantalla libre de accesos directos a información de la entidad. Para los equipos propiedad de Parques Nacionales Naturales de Colombia, el Grupo de Tecnologías de la información y las Comunicaciones podrá implementar políticas de directivas de grupo (Group Policy Object - GPO) para el mantenimiento de pantalla limpios, implementando unidades de red centralizadas para el almacenamiento de esta información.

Esta política debe ser aplicada por todos los servidores públicos, contratistas y terceras partes que por la naturaleza de sus funciones acceden a los activos de información de la entidad.

7.7 POLÍTICA RESPALDO DE LA INFORMACIÓN

Todas las áreas/dependencias de Parques Nacionales Naturales de Colombia, debe asegurar que la información con cierto nivel de clasificación, definida en conjunto con el Grupo de Tecnologías de la Información y las Comunicaciones y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la entidad, como servidores, dispositivos de red para almacenamiento de información, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente respaldada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado, así mismo; el Grupo de Tecnologías de la Información y las comunicaciones definirá los lineamientos específicos que apoyaran esta política a través del Sistema de Gestión de Seguridad de la información.

Esta política debe ser aplicada por todos los servidores públicos, contratistas y terceras partes que por la naturaleza de sus funciones acceden a los activos de información de la entidad.

7.8 POLÍTICA TRANSFERENCIA DE INFORMACIÓN

Parques Nacionales Naturales de Colombia, debe garantizar la protección de la información.

Cualquier intercambio de información con entes externos debe quedar formalizado mediante un acuerdo de intercambio de información documento que deben firmar las partes intervinientes.

Cuando un tercero proponga un anexo o documento que contenga condiciones o cláusulas para asegurar el intercambio entre partes, éste podrá sustituir el acuerdo establecido por la entidad siempre y cuando ésta lo acepte.

El Grupo de Tecnologías de la Información y las Comunicaciones deberá establecer las condiciones técnicas que se deben cumplir para el intercambio de información con terceros.

7.9 POLÍTICA DE DESARROLLO SEGURO

Cuando Parques Nacionales Naturales de Colombia, desarrolle software o contrate el desarrollo de software con proveedores, deberá considerar los lineamientos generales para el desarrollo, mantenimiento y adquisición de software, que defina el Grupo de Tecnologías de la Información y las Comunicaciones con el fin de adoptar los controles de seguridad y buenas prácticas en el desarrollo del software.

La única dependencia que puede contratar o desarrollar software (aplicaciones o sistemas de información) en Parques Nacionales Naturales de Colombia es el Grupo de Tecnologías de la Información y las Comunicaciones.

7.10 POLÍTICA DE SEGURIDAD PARA LAS RELACIONES CON PROVEEDORES

Los terceros o proveedores de Parques Nacionales Naturales de Colombia deberán acatar y cumplir con todos las políticas y lineamientos de seguridad de la información que en el marco del desarrollo de la actividad contratada tenga aplicabilidad. Está política aplica a proveedores de servicios de Parques Nacionales Naturales de Colombia y contratistas y busca preservar los niveles de seguridad y privacidad de los activos de información de la entidad, cuando se autorice el acceso o administración por parte de proveedores de servicios o contratos de prestación de servicios.

8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Las numeraciones de las políticas específicas de seguridad de la información conservan su numeración de acuerdo con el anexo A de la norma ISO: 27001:2013.

8.1 ORGANIZACIÓN INTERNA (A.6.1)[3]

- Los roles y responsabilidades para la seguridad de la información son definidos por el Líder del sistema de seguridad de la información y este deberá dar a conocer los roles y responsabilidades a todos los colaboradores de la entidad.
- La información deberá estar bajo la responsabilidad del Líder de proceso de la dependencia/área para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información de la entidad.
- El Líder del sistema de seguridad de la información deberá mantener contacto con las autoridades nacionales e internacionales en materia de seguridad de la información, y los boletines que estas entidades emitan deberán ser publicados en el micrositio de SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN en la intranet de la entidad. Estos deberán ser divulgados a los colaboradores de la entidad.
- El Líder del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN deberá mantener los contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información, que requiera de asesoría externa.
- Todo proyecto que ejecute Parques Nacionales Naturales de Colombia, independientemente de su objeto, naturaleza, tamaño y complejidad debe contar con un documento de identificación y valoración de riesgos, el cual se debe elaborar siguiendo la Metodología Integrada de Administración del Riesgo definida por la entidad, adicionalmente debe incluir los controles, para la planeación y gestión de proyectos.[4]

Parques Nacionales Naturales de Colombia no debe emprender proyectos que tengan asociados riesgos altos no mitigados.

[3] **A.6.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

[4] https://senda.parquesnacionales.gov.co/senda/doc/usrdoc?soa=12&mdl=doc&_sveVrs=1001620240305&&docId=2942&float=t&float=t#

8.2 DISPOSITIVO MÓVILES (A.6.2)[5]

- El Grupo de Tecnologías de la Información y las Comunicaciones, deberá establecer de manera formal un lineamiento para el control y uso de dispositivos móviles (Computadores Portátiles, Tablet, smartphone, cámaras de video digitales, entre otros), que permita orientar a los servidores públicos de la entidad y a terceros que requieran acceder a los servicios de tecnología.
- Para el uso de Mensajería Instantánea como WhatsApp se debe aplicar los lineamientos del gobierno nacional definidos mediante la resolución 15342 de 2002 emitida por el Ministerio de Comercio, Industria y Turismo, Superintendencia de Industria y comercio.[6]
- La conexión y uso de dispositivos móviles en la red de la entidad debe ser autorizada por el Grupo de Tecnologías de la Información y las Comunicaciones.
- La autorización de la conexión de dispositivos móviles debe considerar las restricciones de acceso a la información y los privilegios de uso de información del usuario.
- El Grupo Procesos Corporativos debe tener un control para el ingreso y salida de las instalaciones de la entidad (bitácoras o registro en sistemas de información) para los elementos de TI asignados a los colaboradores (Portátiles, radios, GPS, entre otros).
- El Grupo de Tecnologías de la Información y las Comunicaciones, realizará el cifrado de los discos duros de los computadores/portátiles propiedad de la entidad, para preservar la confidencialidad de la información en caso de hurto o robo de los equipos.
- El Grupo de Tecnologías de la información y las Comunicaciones, deberá suministrar guayas de seguridad para los equipos portátiles institucionales con el fin de evitar el robo de estos.
- En caso de pérdida o robo del dispositivo móvil el servidor público, contratista o tercero responsable de este, deberá comunicarlo inmediatamente a su jefe o Supervisor del Contrato y deberá reportar este hecho como un incidente de seguridad al Coordinador del Grupo de Tecnologías de la Información y las Comunicaciones y al Coordinador del Grupo de Procesos Corporativos, para que sea atendido.
- El Grupo de Tecnologías de la Información y las Comunicaciones, deberá contar con una herramienta que permita hacer borrado seguro de la información de la entidad en caso de pérdida o robo del dispositivo móvil institucional.
- El Grupo Procesos Corporativos debe establecer un procedimiento ante la pérdida de dispositivos móviles asignados a los colaboradores.
- Los smartphones, propiedad de la entidad deberán disponer de sistemas de autenticación de usuarios (Patrón de desbloqueo, código de seguridad, clave o registro biométrico).
- Los colaboradores (servidores públicos y/o contratistas) son responsables de la custodia de los dispositivos móviles y se harán responsables dentro y fuera de las instalaciones de estos, igualmente, de la información almacenada en estos, por tal razón deberá desarrollar mecanismos para el respaldo de información periódicamente, de ser necesario solicitar apoyo al Grupo de Tecnologías de la Información y las Comunicaciones.
- Los computadores portátiles propiedad de los colaboradores no deberán estar incluidos en dominio @pnnc.local, para conectarse a los servicios de la red de datos de la entidad deberán realizar solicitud a la mesa de servicios (GLPI) y cumplir como mínimo con los siguientes lineamientos referentes a seguridad de la información (contar con un sistema operativo licenciado y actualizado, tener un software antivirus licenciado

[5] **A.6.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

[6] https://www.sic.gov.co/sites/default/files/boletin-juridico/Resolución%2015342.pdf

y actualizado y no tener instalado software o herramientas que le permita saltarse los controles de seguridad de la entidad).

- Para el uso de los computadores portátiles de propiedad de los colaboradores, antes de ser conectados a los recursos de información, tecnológicos y servicios de la entidad se debe validar su integridad mediante la herramienta de control de acceso (Network Access Control "NAC") diseñada por el Grupo de Tecnologías de la Información y las Comunicaciones para tal fin.
- Para los dispositivos móviles propiedad de la entidad, el Grupo de Tecnologías de la Información y las Comunicaciones deberá hacer la disposición de herramientas de ofimática, antivirus, medios de almacenamiento virtual (almacenamiento en nube), herramientas de cifrado y las que se requieran siempre y cuando estas hagan parte de la línea base de software de la entidad, igualmente la restricción de instalación de software por parte del usuario final.
- El Grupo de Tecnologías de la Información y las Comunicaciones debe capacitar a los propietarios o responsables de los dispositivos móviles acerca de los cuidados y responsabilidades que tienen sobre cada uno de los componentes de procesamiento electrónico de información. (Portátiles, teléfonos celulares, Smartphone, Tablet, IPad, teléfonos inteligentes, entre otros).
- Todos los dispositivos móviles propiedad de la entidad que almacenen información deben estar protegidos contra software malicioso y ser actualizado regularmente.
- Los dispositivos móviles personales autorizados se deben revisar periódicamente para certificar que están cumpliendo con las políticas de seguridad de la información de la entidad, las revisiones preservarán el derecho fundamental a la intimidad del usuario y las normas sobre Protección de Datos de carácter personal.
- Los dispositivos móviles propiedad de la entidad deberán cumplir con la política de control de acceso, y los colaboradores que deseen configurar sus dispositivos personales deberán acogerse a las políticas de monitoreo del dispositivo móvil, sin que esto incurra en una violación a la privacidad del colaborador.
- Los colaboradores deberán evitar la descarga de contenidos sospechosos o que procedan de fuentes no verificables (tanto a través de correo, como de navegación) en los dispositivos móviles y equipos portátiles entregados por la entidad.
- Los colaboradores que tengan asignado un dispositivo móvil de la entidad serán responsables de hacer buen uso de la información de la entidad que sea almacenada en estos dispositivos teniendo en cuenta que éste es para uso exclusivo de sus funciones.
- Los colaboradores que tengan asignado un dispositivo móvil propiedad de la entidad no están autorizados a cambiar la configuración, desinstalar software, formatear o restaurar de fábrica el equipo asignado. Únicamente debe aceptar y aplicar las actualizaciones requeridas por el equipo.

8.3 PROTECCIÓN DE DISPOSITIVOS (BYOD) (A.6.2.1)[7]

- Los Líderes de los procesos, los Jefes de Oficina, los Coordinadores, los Directores Territoriales deben determinar en qué procesos y/o dependencias y bajo qué circunstancias se autorizará el uso de dispositivos que no pertenecen la entidad (BYOD) para almacenar o procesar información Institucional pública reservada o información pública clasificada, así como la aplicación de las políticas de seguridad requeridas para la información que se almacene y gestione en el dispositivo personal del funcionario o contratista.

[7] **A.6.2.1- Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- Los Líderes de los procesos deben evaluar los riesgos asociados a la divulgación de información pública reservada o información pública clasificada antes de autorizar el uso de los BYOD.
- El servidor público o contratista al que se autorice un BYOD debe garantizar bajo compromiso de confidencialidad que la información pública reservada o información pública clasificada correspondiente a sus labores asignadas será almacenada de forma aislada a la información personal que guarde en su dispositivo.
- Todo dispositivo BYOD autorizado para almacenar información de la entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.
- El Grupo de Tecnologías de la Información y las Comunicaciones, pueden realizar periódicamente revisiones a los equipos BYOD para certificar que están cumpliendo con las políticas de seguridad de la información, las revisiones preservarán el derecho fundamental a la intimidad del usuario del BYOD y las normas sobre Protección de Datos de carácter personal.
- El propietario del dispositivo BYOD debe aplicar todas las medidas de seguridad razonables que estén a su alcance para preservar la integridad, confidencialidad y disponibilidad de la información que se encuentre en su dispositivo personal.
- El propietario del dispositivo deberá informar sin demoras injustificadas al Grupo de Tecnologías de la Información y las Comunicaciones, y a la autoridad competente el robo o pérdida de su dispositivo. La entidad gestionará la pérdida o divulgación de información almacenada en los dispositivos BYOD mediante el procedimiento de gestión de incidentes de seguridad de la información.

8.4 TELETRABAJO (A.6.3)[8]

- Los criterios y condiciones para ejercer la modalidad de teletrabajo o trabajo remoto deberán ser definidos de forma integral por el Grupo de Gestión Humana y el Grupo de Tecnologías de la Información, teniendo como base la normativa legal vigente mediante la formalización y/o actualización de procedimientos que incluyan los aspectos de seguridad de la información.
- Los colaboradores que requieran acceder a los recursos informáticos de la entidad fuera de las instalaciones de Parques Nacionales Naturales de Colombia deberán realizarlo a través de una conexión de red virtual privada (VPN) o por medio de la plataforma de nube de Google Work Space para el manejo adecuado de la información, previa autorización del jefe inmediato o Supervisor de contrato y del Coordinador del Grupo de Tecnologias de la Información y las Comunicaciones.
- Las conexiones de la modalidad de teletrabajo o trabajo remoto deberán ser monitoreadas y supervisadas según el perfil de usuario y/o asignación roles y privilegios, igualmente verificar la desactivación de los accesos una vez el servidor público no tenga vinculación con la entidad.
- Todo acceso a servicios de teletrabajo debe ser autorizado por el Líder del proceso al que pertenece el servidor público que lo solicita considerando las evaluaciones de riesgos de seguridad de la información y riesgos administrativos.
- Antes de su aprobación todo acceso a servicios de teletrabajo debe ser sometido a una evaluación de riesgos de seguridad de la información y de seguridad y salud en el trabajo.

[8] **A.6.3 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- Los responsables de los procesos que autoricen servicios de teletrabajo se apoyaran en el Grupo de Tecnologias de la Información y las Comunicaciones para realizar las evaluaciones de riesgos digitales sobre los accesos solicitados y formular las recomendaciones de controles de seguridad necesarios para la implementación del acceso. En caso de identificar riesgos que no son aceptables se notificará al jefe del Proceso y al Coordinador del Grupo de Tecnologias de la Información y las Comunicaciones y al peticionario del servicio la imposibilidad de activar los servicios de teletrabajo en las condiciones presentadas en la solicitud.
- Para el acceso al teletrabajo se deben tener en cuenta las necesidades técnicas y tecnológicas que garanticen que el servidor público cuente con las herramientas necesarias para poder realizar su trabajo, así como las configuraciones de acceso seguro, los medios y horarios que solicite el responsable del proceso manteniendo en todo momento los principios de eficiencia, eficacia y uso racional de los recursos del Estado.
- Los servicios de teletrabajo deben ser implementados con controles del sistema de gestión de seguridad de la información que garanticen en todo momento que la seguridad de la información de la entidad esté salvaguardada.
- Cualquier dispositivo que se emplee para las actividades de teletrabajo deberá cumplir con los requisitos y controles de seguridad que defina el Grupo de Tecnologias de la Información y las Comunicaciones.
- Las conexiones a servicios de teletrabajo deben permanecer cifradas con los controles de seguridad del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y utilizando conexiones seguras o redes privadas entre el lugar dónde se realiza el teletrabajo y los sistemas de información de la entidad.
- El acceso a los servicios de teletrabajo se debe usar para el cumplimiento de las funciones asignadas y el cumplimiento de la misión y objetivos de la entidad, cualquier uso diferente está expresamente prohibido.
- Los servidores públicos que realizan teletrabajo son responsables de reportar a la mayor brevedad posible la pérdida o hurto de los equipos y dispositivos móviles usados para teletrabajo y que se encuentren bajo su responsabilidad.
- La estación de trabajo del teletrabajador debe cumplir con la reglamentación en cuanto a uso de software legal.
- La estación de trabajo del teletrabajador debe tener activo el firewall y debe contar con software de protección contra código malicioso.
- Los sistemas operativos de los computadores desde donde se realicen actividades de teletrabajo deben estar actualizados y contar con controles que mitiguen las vulnerabilidades de seguridad.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe asignar el acceso únicamente a la información, servicios y sistemas de información necesarios para la realización de las actividades a cargo del servidor público que solicita el acceso al teletrabajo.
- Una vez el colaborador retorne a las instalaciones de la entidad es responsabilidad del jefe inmediato informar al Grupo de Tecnologias de la Información y las Comunicaciones, para que le sean modificados los accesos concedidos.

9. SEGURIDAD DE LOS RECURSOS HUMANOS (A.7)[9]

9.1. ANTES DE SER CONTRATADO (A.7.1)[10]

- El Grupo de Gestión Humana deberá definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación de la entidad y los que dicte la Función Pública.
- El Grupo de Contratos deberá definir una lista de verificación que contenga los aspectos necesarios para la revisión de los antecedentes, certificaciones académicas y laborales entre otras del personal a contratar por prestación de servicios de acuerdo con lo que dicta la Ley y la reglamentación vigente.
- Los procesos de selección de personal de planta y procesos contractuales deberán contener la autorización para el tratamiento de los datos personales de acuerdo con la Política de tratamiento de datos personales de la entidad y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- Los documentos de verificación deberán reposar en la historia laboral o carpeta contractual del colaborador.
- El Grupo de Gestión Humana y el Grupo de Contratos, deberán establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.

9.2. DURANTE LA VINCULACIÓN DEL SERVIDOR PÚBLICO O EJECUCIÓN DEL CONTRATO (A.7.2)[11]

- El Grupo de Contratos deberá definir los términos y condiciones del contrato, en los cuales se establecerán las obligaciones del contratista en materia de seguridad de la información, las leyes de propiedad intelectual, de protección de datos personales, de transparencia y acceso a la información pública.
- El Grupo de Gestión Humana y el Grupo de Contratos, deberán dar a conocer a los colaboradores los términos y condiciones de empleo o contrato y especificar los roles y las responsabilidades u obligaciones en materia de la seguridad de la información y aclarar que estas se extienden más allá de los límites de la Entidad y del horario normal de trabajo o de ejecución del objeto contractual.
- El Grupo de Contratos deberá incluir en el pliego de condiciones o estudios previos para la contratación de terceras partes, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad de la información que dicte Parques Nacionales Naturales de Colombia.
- El Grupo de Gestión Humana y el Grupo de Contratos, deberán hacer firmar un documento de compromiso de confidencialidad de la información que contenga como mínimo el cumplimiento de las políticas institucionales y normatividad vigente a todos los servidores públicos de la entidad, cualquiera sea su situación contractual, la dependencia a la cual pertenezca y las tareas que desempeñe, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.
- El Grupo de Gestión Humana y el Grupo de Contratos, juntamente con el Grupo de Tecnologias de la Información y las Comunicaciones darán a conocer el manual de políticas de seguridad de la información a los colaboradores de la entidad.

---

[9] **A.7 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

[10] **A.7.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

[11] **A.7.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- Una vez formalizado el proceso de vinculación, el Grupo de Gestión Humana y el Grupo de Contratos o a quien el ordenador del gasto delegue la supervisión, solicitará la creación de la cuenta de usuario y apertura del inventario de vinculación del personal.
- El Grupo de Gestión Humana, el Grupo de Contratos, el Supervisor del Contrato o el jefe inmediato deberá informar a la mesa de servicios (GLPI) sobre las novedades del colaborador y la acción a tomar (bloqueo o desbloqueo) de los recursos tecnológicos.
- Parques Nacionales Naturales de Colombia deberá incluir dentro de los programas de inducción y/o reinducción, sesiones de capacitación y sensibilización del sistema de gestión de seguridad de la información para los servidores públicos y contratistas.
- El Grupo de Tecnologias de la Información y las Comunicaciones, diseñará e implementará en el plan de uso y apropiación estrategias de cultura y apropiación referentes a seguridad de la información.
- Todos los servidores públicos, contratistas y terceros de la entidad, deberán almacenar la información de la operación, únicamente en los repositorios autorizados por la entidad.

PROCESO DISCIPLINARIO POR INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- El incumplimiento de las políticas de seguridad de la información de la entidad por parte de los servidores públicos, contratistas y terceros de Parques Nacionales Naturales de Colombia podrá incurrir en sanciones disciplinarias o legales según corresponda.
- El Oficina de Control Disciplinario Interno debe aplicar las normas y leyes para investigar y sancionar disciplinariamente los casos en que se presenten usos de información y tecnología que violen los términos y condiciones de la política de seguridad de la información de la entidad y los acuerdos firmados por los servidores públicos.
- Con la implementación de políticas de seguridad de la información Parques Nacionales Naturales de Colombia da cumplimiento a las disposiciones legales y regulatorias emitidas por los diferentes organismos estatales, a fin de contar con una metodología de gestión de riesgos como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad de los procesos de la entidad.
- Todos los servidores públicos de la entidad (de carrera administrativa, de libre nombramiento y remoción, provisionales, contratistas, proveedores, terceros, entre otros) que tengan acceso a los sistemas de información, recursos informáticos y demás activos de información de la entidad, deben cumplir con la política de seguridad de información de Parques Nacionales Naturales de Colombia.
- El incumplimiento de las políticas y procedimientos de seguridad, para los servidores públicos constituye falta disciplinaria conforme a lo señalado en los numerales 4 y 5 del artículo 34 y numerales 16 y 43 del artículo 48 de la ley 734 de 2002.

Artículo 34 Son deberes de todo servidor público:

> “4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función en forma exclusiva para los fines a que están afectos.”

"5. Custodiar y cuidar la documentación que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."

Artículo 48. Son faltas gravísimas las siguientes: "16. Atentar con cualquier propósito, contra la inviolabilidad de la correspondencia y demás formas de comunicación, u obtener información o recaudar prueba con desconocimiento de los derechos y garantías constitucionales y legales"

"43. Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos y en los que se almacene o guarde la misma, o permita el acceso a ella a personas no autorizadas."

- El Oficina de Control Disciplinario Interno es el único competente para realizar una investigación disciplinaria según (art.76 Ley 734 de 2002). Las faltas y sanciones son las establecidas en la ley 734 de 2002, conforme al procedimiento constituido para el efecto.

9.3. TERMINACIÓN Y/O CAMBIO DE EMPLEO (A.7.3)[12]

- El supervisor del contrato o a quien delegue deberá recoger y custodiar la información de la entidad bajo la responsabilidad de los contratistas en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- El jefe inmediato o a quien delegue deberá recoger y custodiar la información de la entidad bajo la responsabilidad de los servidores públicos en el caso de retiro, investigación, inhabilidades, o cambio de funciones.
- El Grupo de Gestión Humana y el Grupo de Contratos o a quienes se deleguen deberán informar al Grupo de Tecnologias de la Información y las Comunicaciones a través de la mesa de servicios (GLPI), cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador o cambio de rol; una vez notificada la novedad al Grupo de Tecnologias de la Información y las Comunicaciones deberá proceder a la inactivación de los accesos del colaborador, teniendo en cuenta los siguientes parámetros:
    - Si el buzón pertenece a una cuenta de correo genérica o de servicio (ejemplo: info@parquesnacionales.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar nuevo responsable para evitar accesos no autorizados.
    - En caso de que el buzón sea objeto de investigación por parte de las autoridades competentes se les entregará en cadena de custodia una copia del buzón garantizando su integridad. Se deben inactivar los accesos biométricos de los sistemas de control de acceso.
    - Emitir comunicado a los proveedores y demás personal con el que el colaborador tenga contacto, indicándole que esa persona ya no labora en la entidad e indicar quién asumirá sus funciones o responsabilidades.
- Adicionalmente en desvinculación:
    - Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con Parques Nacionales Naturales de Colombia.

[12] **A.7.3 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y no se podrán emitir correos ni notificaciones desde estos buzones.
- Se deben inactivar todos los accesos a los sistemas de información.
- Se debe solicitar la devolución del carné o cualquier distintivo de autenticación o prenda de vestir, que lo acredite como colaborador de la entidad.

- El Grupo de Gestión Humana y el Grupo de Contratos, deberá comunicar a los servidores públicos y contratistas, las responsabilidades respecto a seguridad de la información que se derivan de la terminación o cambio de empleo.
- El funcionario, contratista y/o proveedor deberán entregar todos los activos de información según como lo determina el procedimiento de terminación del empleo, así mismo el proceso de entrega del cargo o separación temporal del mismo, y los informes de supervisión de contrato según el caso que aplique.
- La Oficina Asesora de Planeación a través del Sistema de Gestión Integrado establecerá un procedimiento o instructivo para la finalización de contratos de prestación de servicios, que permita determinar los criterios para la entrega de información y equipos a la hora de culminar los contratos.

10. GESTIÓN ACTIVOS (A.8)[13]

10.1 RESPONSABILIDADES (A.8.1)[14]

- Toda información sea física o digital generada, almacenada o transformada por los servidores públicos, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de Parques Nacionales Naturales de Colombia
- El Líder del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN o a quien este delegue deberá aplicar y mantener actualizada la documentación para el levantamiento y actualización de los activos de información de la entidad.
- La identificación, clasificación y valoración de activos de la entidad, deberá ser realizada por los Líderes de proceso, en el formato de registro de activos de información, de acuerdo con lo definido en la guía para la gestión de activos de información de la entidad. Este proceso deberá actualizarse anualmente o previo a los cambios normativos vigentes.
- Los Líderes de los procesos o a quienes estos deleguen con el apoyo del Grupo de Tecnologias de la Información y las Comunicaciones deberán mantener un inventario de sus activos de información de forma anual y serán actualizados según el evento en que se requiera.
- Los Líderes de los procesos de la entidad, serán los propietarios de los activos de información identificados para sus procesos.
- Los Líderes de los procesos deben establecer los controles de acceso para cada uno de los activos de información.

[13] **A.8 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

[14] **A.8.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- El Líder del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN o a quien este delegue, deberá remitir el consolidado del levantamiento de activos de información, al Profesional que lidera la estrategia de la ley de transparencia y acceso a la información pública y la estrategia de Gobierno Digital o a quien haga sus veces, con el objetivo de ser analizada, realimentada, actualizada y publicada de acuerdo con la normativa vigente colombiana.
- Los servidores públicos, contratistas y usuarios de los activos de información y de la información de la entidad deben:
    - Aceptar y cumplir las políticas de seguridad de la información establecidas en la entidad.
    - Proteger contra pérdida, modificaciones y acceso no autorizados a los activos de información de la entidad.
    - Comprender y aceptar sus responsabilidades frente al acceso a los diferentes sistemas de información que se tienen o administran en la entidad.
- Los Líderes de proceso de la entidad deberán realizar la respectiva aceptación de los activos de información del proceso a su cargo, con el fin de establecer posteriormente los riesgos de seguridad digital a los que estos se vean expuestos.
- El Grupo de Tecnologias de la Información y las Comunicaciones, debe establecer lineamientos para el uso y acceso a los recursos de tecnología de la entidad “correo electrónico, internet, Google Work Space, entre otros”.
- En caso de que un colaborador deba hacer uso de equipos ajenos a la entidad, estos deberán cumplir con la legalidad del software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red de la entidad una vez esté avalado por el Grupo de Tecnologias de la Información y las Comunicaciones.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la entidad es el que cuenta con el dominio @parquesnacionales.gov.co.
- Parques Nacionales Naturales de Colombia se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus servidores públicos o contratistas, además podrá realizar copias de seguridad en cualquier momento, así como limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en el mismo por solicitud expresa del Director, Ordenador del Gasto, Jefes de Oficina, Directores, Subdirectores y Coordinadores de Grupo de Tecnologias de la Información y las Comunicaciones.
- Con el fin de mitigar la suplantación de la identidad de correos electrónicos, se prohíbe suministrar acceso directo a los buzones de correo asignado a cada colaborador. En caso de ser necesario realizar la gestión del correo institucional, se debe solicitar a la mesa de servicios (GLPI) listando los colaboradores que tendrán los permisos para escribir correos en nombre del colaborador solicitante.
- No se permite el almacenamiento en los equipos de cómputo y medios de almacenamiento propiedad de la entidad, el almacenamiento de archivos de multimedia (Audio, video, Imágenes), programas ejecutables, o cualquier tipo de archivo que no sea de carácter institucional.
- Únicamente se permitirá el acceso a las aplicaciones y sistemas de información autorizados por la entidad, de esta manera evitar la ejecución de software no licenciado el cual atente contra los derechos de autor y propiedad intelectual según como lo regula la ley.
- El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los servidores públicos y contratistas determinadas por los jefes o Coordinadores de área o dependencia.
- Para la consulta de documentos adjuntados en el software de gestión documental, se establecerán privilegios de acceso a los servidores públicos y/o contratistas de acuerdo con el desarrollo de sus funciones y

competencias. Dichos privilegios serán establecidos por el jefe, coordinador o director del área, quien comunicará al Grupo encargado de la administración del software el listado con los servidores públicos y sus privilegios.

- Parques Nacionales Naturales de Colombia debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los servidores públicos y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente.
- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la entidad es responsabilidad del Grupo de Tecnologias de la Información y las Comunicaciones, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación del software deben ser los proporcionados por la entidad a través de esta oficina.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la entidad, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el Grupo de Tecnologias de la Información y las Comunicaciones.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la entidad; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por el Grupo de Tecnologias de la Información y las Comunicaciones.
- Los colaboradores y terceras partes deberán devolver todos los activos de información de la entidad que se encuentren en su poder a la terminación de su empleo, contrato, convenio o acuerdo.
- Para el traslado de equipos de cómputo al almacén o a otros colaboradores, o baja de los inventarios por cualquier motivo, se deberá realizar un respaldo de la información que en él se encuentre a través de la mesa de servicios. Cuando el dispositivo se vaya a dar de baja el Grupo de Tecnologias de la Información y las Comunicaciones debe realizar el borrado seguro de la información que contengan medios de almacenamiento con el fin de propender que la información de la entidad contenida en estos medios no se pueda recuperar.
- Cuando se realice el traslado de equipos de cómputo a otros colaboradores, se deberá instalar de nuevo el sistema operativo y los programas de la línea base.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será el Grupo de Tecnologias de la Información y las Comunicaciones, sin embargo, cuando deba realizarse desde y hacia el almacén será el Grupo de Procesos Corporativos, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la entidad.

10.2 CLASIFICACIÓN DE LA INFORMACIÓN (A.8.2)[15]

El Grupo de Tecnologias de la Información y las Comunicaciones deberá apoyar al Grupo de Atención al Ciudadano los cuales desarrollarán los lineamientos para la clasificación de la información teniendo en cuenta lo siguiente:

[15] **A.8.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- Los propietarios de la información son los encargados de realizar la clasificación de la información.
- Parques Nacionales Naturales de Colombia definirá los niveles adecuados para clasificar su información de acuerdo con su sensibilidad donde se valorarán confidencialidad, integridad y disponibilidad de la información. Estos niveles deberán ser oficializados y divulgados a todos los colaboradores.
- Los propietarios y custodios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.
- Los colaboradores y terceras partes deberán acatar los lineamientos que se definan frente a almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.
- La información física y digital de la entidad deberá tener un periodo de almacenamiento que puede ser dado por requerimientos legales o misionales; este periodo deberá ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información deberá ser eliminada o transferida adecuadamente.
- Parques Nacionales Naturales de Colombia, a través del Grupo de Atención al Ciudadano, deberá establecer los mecanismos necesarios para proteger la información catalogada como Información pública reservada, teniendo en cuenta el medio en que se encuentre.
- La información pública clasificada y pública reservada deberá protegerse incluso en los ambientes de pruebas.
- Los servidores públicos y contratistas de la entidad no deben divulgar información pública clasificada o pública reservada de la entidad a personas no autorizadas o a entes externos, a menos que se realice por el canal oficialmente establecido y con la aprobación previa del líder de proceso al cual pertenece el activo de información.
- La información de la entidad no debe ser divulgada sin contar con los permisos correspondientes, además, ningún funcionario, contratista o proveedor debe copiarla o extraerla en el momento en que se retire de la entidad o durante su permanencia.
- Los terceros, proveedores u operadores tecnológicos que accedan a la información de la entidad, no deben hacer copias de la información suministrada por la entidad, ni podrán transferirla a otro equipo a través de la red, sin la autorización del dueño de la información.
- Los servidores públicos y/o contratistas a los que se haya asignado un equipo de cómputo en la entidad, no debe almacenar información, como música, videos y fotos que no sean de carácter estrictamente institucional.

10.3 MANEJO DE MEDIOS (A.8.3)[16]

- El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, memorias flash, USBs, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de la entidad, estará autorizado para aquellos servidores públicos cuyo perfil del cargo y funciones lo requiera.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe definir un procedimiento para el uso de medios removibles e implementar los controles necesarios para su uso.
- Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la entidad que este contiene.

[16] **A.8.3 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- En ninguna circunstancia se dejarán desatendidos los medios de almacenamiento o copias de seguridad de los sistemas de información.
- Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la red de la entidad.
- Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.
- Se prohíbe el uso de medios removibles en lugares de acceso al público que contengan información reservada o clasificada de la entidad.
- El Grupo Procesos Corporativos deberá crear un procedimiento para la disposición final de residuos de aparatos electrónicos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá propender porque el procedimiento de almacenamiento de información (Backus) cuente con las condiciones para asegurar la confidencialidad, integridad y disponibilidad de la información en custodia.
- Los medios y equipos donde se almacena y procesa información deben mantenerse con las medidas de protección físicas, lógicas y condiciones dadas por los fabricantes, que permitan un adecuado funcionamiento.
- El uso de medios removibles será restringido, en caso de requerir su uso deberá ser solicitado por la parte interesada de manera formal a través de la mesa de servicio (GLPI), posteriormente autorizado por el Grupo de Tecnologias de la Información y las Comunicaciones teniendo en cuenta lo siguiente:
    - Definir en qué condiciones o casos se permitirá el uso (procedimiento guía o instructivo).
    - El Grupo de Tecnologias de la Información y las Comunicaciones deberá mantener un registro de los dispositivos y/o medios removibles autorizados.
    - El uso de medios removibles deberá emplear métodos para el cifrado de información, para ello el Grupo de Tecnologias de la Información y las Comunicaciones deberá indicar los medios de cifrado, esto con el fin de evitar la pérdida y fuga de información institucional de carácter clasificada o reservada.
- Los medios que requieran ser eliminados, dar de baja o ser reasignados deberán someterse a un proceso de borrado seguro y demás mecanismos que puedan considerarse, con el fin de evitar la recuperación de la información que alguna vez estuvo contenida en estos medios.
- Los equipos que se regresen al almacén para asignarse a otro colaborador o para dar de baja, se les deberá ejecutar el procedimiento de borrado seguro o en caso de no poder realizar el borrado seguro validar el procedimiento para la disposición final de residuos de aparatos electrónicos RAEE.
- Es requisito realizar el respaldo o copia de la información contenida en el equipo, previa ejecución del procedimiento de borrado seguro.
- Cuando se requiera transferir un medio de almacenamiento de información de la entidad a otras entidades se deberá establecer un acuerdo entre las partes. Dichos acuerdos deberán dirigirse a la transferencia segura de información de interés entre la entidad y las partes.
- El transporte para los medios de almacenamiento deberá contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información.
- Toda información propiedad de la entidad de tipo clasificada y/o reservada, almacenada en los diferentes medios y que requieran ser transportados a otras locaciones ajenas a la entidad, deberá cumplir con los lineamientos de seguridad establecidos por el Grupo de Tecnologias de la Información y las Comunicaciones.

11. CONTROL DE ACCESO (A.9)[17]

11.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO (A.9.1)[18]

- Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información Parques Nacionales Naturales de Colombia suministrará a los usuarios las credenciales respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados; estas credenciales de acceso son de uso personal e intransferible.
- Es responsabilidad de los colaboradores o terceras partes de la entidad el manejo que se les dé a las credenciales de acceso asignadas, así como el uso que se le dé a la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- Los colaboradores o terceras partes que realicen actividades administrativas sobre la plataforma tecnológica de la entidad deberán realizarlas en las instalaciones de la entidad y no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del Supervisor del contrato o del jefe en caso del servidor público.
- La conexión remota a la red de área local de la entidad deberá establecerse a través de una conexión VPN suministrada por la entidad, la cual deberá ser aprobada, registrada y auditada por el Grupo de Tecnologias de la Información y las Comunicaciones.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar revisiones e inactivaciones de las conexiones VPN cada treinta (30) días o de acuerdo con las solicitudes de desactivación generadas en la mesa de servicio (GLPI).
- Las conexiones remotas deberán utilizar los métodos establecidos de autenticación para el control de acceso de los usuarios.
    - El Grupo de Tecnologias de la Información y las Comunicaciones deberá implantar controles para el acceso por redes inalámbricas.
    - El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer una adecuada segregación de redes, separando los entornos de red de usuarios de los entornos de red de servicios.
    - El control de acceso a los datos, información y servicios se deberá basar en el principio del menor privilegio y la necesidad de conocer, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.
    - El Grupo de Tecnologias de la Información y las Comunicaciones deberá verificar periódicamente los controles de acceso para los usuarios de la entidad y los provistos a terceras partes, con el fin de revisar que dichos usuarios tengan los permisos únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
    - Los colaboradores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la entidad, deberán contar con el formato solicitud servicios de gestión de los usuarios debidamente autorizados.[19]

[17] **A.9 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

[18] **A.9.1 Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

[19] https://senda.parquesnacionales.gov.co/senda//base/attachment;jsessionid=106302192DE4594263C43FCB37FE9241?soa=1&attId=1104

- Los equipos personales de los colaboradores que se conecten a las redes de datos de la entidad deberán cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- No se podrá utilizar ningún tipo de utilitario para conexión remota a la red interna de la entidad, únicamente se deberá utilizar el autorizado por el Grupo de Tecnologias de la Información y las Comunicaciones.
- El Grupo de Tecnologias de la Información y las Comunicaciones es el responsable de asignar los accesos a plataformas, usuarios y segmentos de red de acuerdo con los procesos formales de autorización.
- La autorización para el acceso a los sistemas de información debe ser definida y aprobada por el área propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los servidores públicos y terceros e implementada por el Grupo de Tecnologias de la Información y las Comunicaciones.
- En caso de conexiones de tipo remoto deben existir mecanismos robustos de autenticación y transmisión segura de datos. Este servicio debe ser restringido solo a usuarios autorizados y específicamente a los recursos que requiera para el cumplimiento de las funciones en Parques Nacionales Naturales de Colombia, aplicando el principio de “el acceso mínimo permitido”.
- La conexión remota a las redes de Parques Nacionales Naturales de Colombia sólo podrá hacerse mediante la infraestructura provista y por los servicios definidos por el Grupo de Tecnologias de la Información y las Comunicaciones. Está prohibido el uso de módems en computadores de usuarios para obtener el acceso remoto a la red, así como cualquier otro medio no autorizado por el Grupo de Tecnologias de la Información y las Comunicaciones.
- Si Parques Nacionales Naturales de Colombia requiere proporcionar acceso remoto a terceros, deberá contar con sistemas de autenticación de nodos, habilitar controles de red para restringir el uso de servicios no necesarios y limitar los accesos por fecha y hora.
- Todas las conexiones remotas que requieran acceso a la red interna de la entidad deben pasar forzosamente por un Firewall, el cual proporcione a las redes internas un nivel de seguridad acorde a la sensibilidad de los sistemas, aplicaciones e información disponible en ellas.
- El Grupo de Tecnologias de la Información y las Comunicaciones es responsable de la administración de redes, debe contar con un procedimiento formal para la autorización de conexiones remotas a los usuarios, el cual incluya por lo menos:
    - Plena identificación del usuario.
    - Justificación del acceso.
    - Sistema e información a la cual requiere acceso.
    - Solicitud formal escrita con la justificación del jefe o coordinador del Área del usuario solicitante dirigida al Grupo de Tecnologias de la Información y las Comunicaciones.
- En función de la justificación del usuario para obtener acceso remoto, el Grupo de Tecnologias de la Información y las Comunicaciones debe determinar el tipo y nivel de acceso que le otorgará, así como establecer un procedimiento de monitoreo periódico de las conexiones y actividades de los usuarios para identificar posibles anomalías en las conexiones o cuentas con inactividad mayor a 2 meses que requieran ser eliminadas.
- Deben existir al menos 3 tipos de acceso remoto:
    - Acceso general: Acceso a correo electrónico corporativo, internet y portal corporativo (intranet) sin aplicaciones.

- Acceso particular: El mismo acceso que general, más los permisos necesarios para ingresar al sistema o aplicaciones que se justifique y autorice.
- Acceso a administradores de sistemas: Acceso a los sistemas e infraestructura asignada según sus funciones o actividades.

- El acceso remoto a terceros no estará permitido a menos que exista una legítima necesidad justificada para otorgarles el servicio. El usuario externo tendrá que cumplir con un procedimiento formal de autorización con el Grupo de Tecnologias de la Información y las Comunicaciones.
- Las aplicaciones o sistemas de información nuevos que sean desarrollados al interior de la entidad o por terceros deberán cumplir como mínimo con los siguientes requisitos de seguridad:
  - La autenticación de los usuarios debe hacerse a través del directorio activo.
  - Los desarrolladores deberán establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y en su lugar, se deben generar mensajes generales de falla.
  - Los desarrolladores deberán asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deberán deshabilitar la funcionalidad de recordar campos de contraseña.
  - Los desarrolladores deberán asegurar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
  - Los desarrolladores deberán asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deberán tener un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales después de su utilización
  - Toda aplicación debe controlar el tiempo de inactividad en las sesiones, las cuales deberán cerrarse después de un período de inactividad definido máximo 5 minutos y se deberán usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones misionales de alto riesgo.

11.2 GESTIÓN DE ACCESO DE USUARIOS (A.9.2)[20]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir un procedimiento para el registro y la cancelación de usuarios en Parques Nacionales Naturales de Colombia, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.
- Se deberá definir un estándar para la definición de los usuarios en caso de presentarse homónimos.
- Se deberán deshabilitar las credenciales de acceso a los colaboradores que no tengan ningún vínculo con la entidad.
- El acceso a la información de la entidad es otorgado sólo a usuarios autorizados, teniendo en cuenta lo requerido para la realización de sus labores relacionadas con su responsabilidad o tipo de servicio con los privilegios asignados.
- No se deberá configurar el acceso a los recursos tecnológicos a usuarios que no hayan formalizado el proceso de ingreso a la entidad.
- Todo usuario que quiera acceder a servicios o información de la plataforma tecnológica de la entidad deberá autenticarse.

[20] **A.9.2 Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional.

- Los usuarios deberán cumplir con los lineamientos para la creación y uso de contraseñas.
- El uso de credenciales de usuarios administradores de sistemas operativos, consolas de administración y bases de datos tales como: “root”, “adm”, “admin”, “administrador”, “SQLAdmin”, “administrator” y “system”, entre otros, deberán ser controladas, monitoreadas y vigiladas por el coordinador del Grupo de Tecnologias de la Información y las Comunicaciones.
- Todos los colaboradores y terceras partes deberán cumplir las condiciones de acceso y mantener de forma confidencial las contraseñas con la finalidad de preservar el no repudio.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá otorgar los privilegios para la administración de recursos tecnológicos, servicios de red y sistemas de información únicamente a aquellos colaboradores que cumplan dichas funciones.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá otorgar cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información, diferentes a los nativos y deberán ser cuentas únicas asociadas al usuario de dominio.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deberá permitir el acceso a los colaboradores autorizados.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware y las bases de datos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá mantener un listado actualizado en donde se identifiquen los derechos de acceso privilegiado asociados con cada sistema o proceso, sistema operativo, sistema de gestión de bases de datos, y cada aplicación de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá generar registros de auditoría que contengan eventos relacionados de seguridad, teniendo en cuenta criterios tales como nombre de usuario, fechas y hora de evento, tipo de modificación sobre el objeto. Se deberá realizar un respaldo de esta información facilitando la revisión y el análisis de estos
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar auditorías a las carpetas y subcarpetas mínimo cada seis (6) meses, con el fin de establecer controles que permitan validar que solo cuenten con los permisos de acceso los usuarios autorizados. Esta información deberá ser suministrada a cada Líder de proceso.
- El Grupo de Tecnologias de la Información y las Comunicaciones, deberá tener un listado de las cuentas de servicio que se configuren en el directorio activo y debe establecer un responsable para cada una de ellas.
- La contraseña para la autenticación se deberá suministrar a los usuarios de manera segura, y el sistema deberá solicitar el cambio inmediato de la misma al ingresa.
- Se deberán establecer mecanismos para verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal.
- La información secreta para la autenticación por defecto del fabricante se deberá modificar después de la instalación de los dispositivos o del software.
- Toda aplicación o sistema de información el Grupo de Tecnologias de la Información y las Comunicaciones, deberá generar reportes de uso de cada uno con el fin de identificar la periodicidad de uso de cada uno de los usuarios.
- El Grupo de Tecnologias de la Información y las Comunicaciones, deberá revisar los derechos de acceso de los usuarios administradores por lo menos una vez al año.
- El retiro de los privilegios de acceso se deberá hacer inmediatamente se realice la solicitud de desactivación de los usuarios.

- Es responsabilidad de los directores, subdirectores, jefes de Oficina, coordinadores, jefes de áreas protegidas o Supervisores de los contratos dar a conocer al Grupo de Tecnologias de la Información y las Comunicaciones el retiro, suspensión o cualquier novedad administrativa que se presente con los usuarios de la entidad, esta novedad se deberá reportar a través de la mesa de servicios (GLPI).
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá configurar estaciones de acceso privilegiado para cada uno de los administradores de la plataforma tecnológica.

11.3 RESPONSABILIDADES DE LOS USUARIOS (A.9.3)[21]

- El Grupo de Tecnologias de la información y las Comunicaciones establece los siguientes lineamientos para la asignación de información de autenticación secreta teniendo en cuenta lo siguiente:
    - Los usuarios son responsables del uso de las contraseñas de acceso que se le asignen para la utilización de los equipos o servicios tecnológicos de la entidad.
    - El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta o su jefe inmediato.
    - Las contraseñas deberán:
        - Poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
        - La contraseña deberá tener como mínimo ocho (8) caracteres alfanuméricos.
        - La contraseña no deberá contener el nombre de usuario, el nombre real o la sigla PNNC.
        - No se deberán usar contraseñas con los nombres de los hijos, esposo, mascotas, fechas de aniversarios, cumpleaños, etc.
        - La contraseña deberá ser diferente de otras contraseñas anteriores proporcionadas, es decir las ultimas diez (10) suministradas al dominio no se deberán repetir.
        - No se deberán usar las mismas contraseñas de la autenticación para uso personal.
        - Las contraseñas deberán estar compuestas por: letras en mayúsculas “A, B, C…”, letras en minúsculas “a, b, c…”, números “0, 1, 2, 3…”, símbolos especiales “@, #, $, %, &, (),¡, ¡, ¿, ¿, <>…” y espacios en cualquier orden.
        - Las contraseñas deberán cambiarse obligatoriamente cada 60 días o cuando lo establezca el Grupo de Tecnologias de la Información y las Comunicaciones.
        - Después de cinco (5) intentos no exitosos de ingreso de la contraseña el usuario deberá ser bloqueado de manera inmediata y deberá esperar un tiempo determinado para volver a intentar, o solicitar el desbloqueo a través de la Mesa de Servicios.
        - La contraseña deberá cambiarse si se ha detectado anomalía en la cuenta de usuario.
        - La contraseña no deberá ser visible en la pantalla, al momento de ser ingresada.
        - No deberán ser reveladas a ninguna persona.
        - Las contraseñas no se deberán registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado por el Grupo de Tecnologias de la Información y las Comunicaciones.

[21] **A.9.3 Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

11.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES (A.9.4)[22]

- Todo servidor público o contratista de la entidad, cualquiera sea su forma de vinculación, la dependencia a la cual pertenezca y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. El Grupo de Tecnologias de la Información y las Comunicaciones debe mantener un directorio completo y actualizado de tales perfiles.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe establecer el método de autenticación de usuarios a adoptar por la entidad. El método que se escoja debe garantizar que el repositorio de cuentas de usuario, perfiles y contraseñas para la autenticación de usuarios se encuentre protegido de cualquier intento de acceso indebido o corrupción y cuente con logs de seguridad requeridos para las auditorías. Adicionalmente determinará cuales son los perfiles de usuarios que deben existir en la entidad y los atributos que debe tener cada uno de los diferentes perfiles para el control de accesos a los sistemas de información, bases de datos y servicios de información, donde se definan los niveles de acceso de los usuarios estándar del sistema comunes a cada categoría de puestos de trabajo y los administradores, asegurando que no comprometan la segregación de funciones; estos perfiles de usuarios deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir los lineamientos para la restricción de acceso a la información teniendo en cuenta lo siguiente:
    - Deberá implementar controles para que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
    - Deberá establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, deberá implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
    - Deberá proporcionar repositorios de archivos fuente de los sistemas de información; estos deberán contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
    - Los desarrolladores deberán establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cuál fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
    - Los desarrolladores deberán asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deberán deshabilitar la funcionalidad de recordar campos de contraseñas.
    - Los desarrolladores deberán asegurar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
    - Los desarrolladores deberán asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deberán tener un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales después de su utilización.
    - El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deberán estar restringidos y estrictamente controlados.

[22] **A.9.4 Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- Las sesiones inactivas deberán cerrarse después de un período de inactividad definido y se deberán usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones misionales de alto riesgo.
- Toda la autenticación de aplicaciones o sistemas de información debe usar el método de autenticación definido por el Grupo de Tecnologias de la Información y las Comunicaciones.

- El Grupo de Tecnologias de la Información y las Comunicaciones debe elaborar, mantener y publicar los documentos de servicios de red que ofrece la entidad a sus servidores públicos, contratistas y terceros.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.
- El acceso a aplicativos, sistemas de cómputo y los datos es responsabilidad exclusiva del funcionario propietario de los activos de información, según la matriz del inventario de activos de información.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe hacer mantenimiento continuo al directorio activo o al sistema empleado para la autenticación de usuarios con el objeto de desactivar las cuentas de usuarios que se desvincularon de la entidad y verificar que las cuentas existentes corresponden a usuarios activos o vigentes en la entidad y su información está actualizada. Modificar los derechos de acceso de los usuarios que cambiaron de área y sus tareas. Cancelar cuentas de usuario redundantes. Inhabilitar cuentas que no hayan sido utilizadas por más de 30 días y estas no serán reactivadas hasta que la identidad del usuario haya sido verificada. Eliminar cuentas inactivas por más de 60 días. En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- Las contraseñas de administrador de las aplicaciones o soluciones de software que se producen, procesan, gestionan, o almacenan información de misión crítica de la entidad, deben ser conservadas por la Alta Dirección y/o el Grupo de Tecnologias de la Información y las Comunicaciones, estas deben ser cambiadas en intervalos regulares de tiempo, máximo de 60 días y/o en caso que el personal responsable de las mismas cambie de cargo o de dependencia. De igual manera las claves de administrador de servidores, equipos de comunicaciones y de seguridad deben ser conservadas por la Alta Dirección y el Grupo de Tecnologias de la Información y las Comunicaciones, en el momento en que sea cambiada alguna de las contraseñas de estos equipos inmediatamente debe ser dada a conocer a estas dependencias. Adicionalmente las contraseñas de administrador de los equipos de escritorio adscritos al grupo de apoyo tecnológico deben ser conservadas por el Coordinador de este grupo y deben ser cambiadas en intervalos regulares de tiempo, máximo de 60 días y en todo caso cuando el funcionario adscrito al cargo cambie.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de contraseñas de usuario.
- Como requisito para la terminación de la relación laboral o contractual de servidores públicos y contratistas de la entidad, el Grupo de Tecnologias de la Información y las Comunicaciones debe expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de cada uno de los recursos de tecnologías de la información de la entidad a que tenía acceso el funcionario o contratista.
- Los sistemas de información o aplicaciones deberán cumplir con:
  - Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se deberá bloquear la sesión, sin cerrar las sesiones de aplicación o de red.
  - No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
  - No suministrar mensajes de ayuda, durante el proceso de autenticación.
  - Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
  - Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos hasta un máximo de tres (3) intentos.
  - No mostrar las contraseñas digitadas con anterioridad.

- No transmitir la contraseña en texto claro.

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información.
- El acceso al código fuente del programa es limitado, solamente los ingenieros desarrolladores y de soporte autorizados por el Grupo de Tecnologias de la Información y las Comunicaciones o por los dueños de los activos de información pueden tener acceso.

12. CRIPTOGRAFÍA (A.10)[23]

12.1 CONTROLES CRIPTOGRÁFICOS (A.10.1)[24]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberán utilizar controles criptográficos en los siguientes casos:
  - Para la protección de claves de acceso a sistemas, datos y servicios.
  - Para la información digital o electrónica reservada y clasificada.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá verificar que todo sistema de información que requiera realizar transmisión de información clasificada como reservada o restringida, cuente con mecanismos de cifrado de datos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá utilizar controles criptográficos para la transmisión de información clasificada, fuera del ámbito de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.

[23] **A.10 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[24] **A.10.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

13. SEGURIDAD FÍSICA Y DEL ENTORNO (A.11)[25]

13.1 ÁREAS SEGURAS (A.11.1)[26]

- El perímetro de las áreas que contienen la información y sus instalaciones de procesamiento sensible o crítico deberán estar protegidos de accesos no permitidos.
- Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.
- Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación.
- El perímetro de seguridad debe contar con vigilancia mediante Circuito Cerrado de Televisión (CCTV) y debe ser monitoreado por el personal de vigilancia de la entidad.
- El Grupo de Procesos Corporativos deberá señalizar las áreas de acceso restringido.
- El Grupo de Procesos Corporativos deberá establecer un sistema de control de acceso a las instalaciones de la entidad, así como a las áreas demarcadas con acceso restringido dentro y fuera de las instalaciones principales de la entidad.
- Las áreas de acceso restringido deben estar monitoreadas en su acceso por Circuito Cerrado de Televisión (CCTV).
- El Grupo de Procesos Corporativos o a quien éste designe, será responsable de administrar el ingreso y salida del personal a los centros de cableado y al centro de datos de la sede de Parques Nacionales Naturales de Colombia.
- El Grupo de Procesos Corporativos o a quien este delegue autorizará el ingreso a personal ajeno a la entidad a los centros de cableado para fines laborales, este deberá estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno a la entidad durante el tiempo que permanezca en las instalaciones.
- Todo el personal que ingrese al centro de datos o a los centros de cableado deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso y deberá diligenciar una bitácora en la cual se debe registrar la fecha y hora de su ingreso y salida, motivo de la visita, nombres, cédula, quien le autoriza el ingreso y/o si ingresa o retira elementos de estas áreas, y demás información que el Grupo de Procesos Corporativos determine apropiadas.
- El Grupo de Procesos Corporativos deberá controlar que los centros de cableado permanezcan siempre con las puertas de acceso cerradas y con controles de seguridad que mitiguen el acceso a personal no autorizado.
- El Grupo de Tecnologias de la Información y las Comunicaciones será responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado.
- El Grupo Procesos Corporativos deberá mantener en buen estado la infraestructura física de los centros de cableado y del centro de datos, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar una revisión periódica del estado de los centros de cableado e informar cualquier anomalía presentada de la siguiente manera: daños en el rack y equipos activos de red al Grupo de Tecnologias de la Información y las Comunicaciones y daños

[25] **A.11 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[26] **A.11.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros) al Grupo de Procesos Corporativos.

- El Grupo de Procesos Corporativos y el Grupo de Tecnologias de la Información y las Comunicaciones, son los responsables del cumplimiento del protocolo de aseo en los centros de cableado y centro de datos.
- El Grupo de Tecnologias de la Información y las Comunicaciones será responsable de mantener organizado e identificado el cableado en los racks de los centros cableado y centro de datos.
- El Grupo de Tecnologias de la Información y las Comunicaciones será responsable de la identificación y señalización necesaria de los centros de cableado y centro de datos.
- El Grupo de Procesos Corporativos deberá implementar y administrar los circuitos cerrados de televisión (CCTV) para los centros de cableado y centro de datos.
- El Grupo de Procesos Corporativos deberá respaldar los videos generados por las cámaras de vigilancia ubicadas en los centros de cableado y el centro de datos de acuerdo con las políticas de respaldo de la información de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones, deberá mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos y centros de cableado.
- El Grupo de Procesos Corporativos deberá controlar y monitorear a través de circuitos cerrados de televisión (CCTV) el ingreso a las áreas seguras.
- El Grupo de Procesos Corporativos deberá establecer circuito cerrado de televisión (CCTV), que cubra el acceso al área y al funcionario que utilice los equipos financieros de pago.
- El Grupo de Procesos Corporativos deberá implementar controles que permitan hacer seguimiento a variables de humedad y temperatura al centro de datos y a los centros de cableado.
- El Grupo de Tecnologias de la Información y las Comunicaciones, deberá monitorear las variables de temperatura y humedad de los centros de cableado o data center y cuando estos se vean afectados por daño o falta de mantenimiento, se deberá reportar al Grupo de Procesos Corporativos dichas eventualidades para que estos equipos sean cambiados o se haga el mantenimiento necesario para su debido funcionamiento.
- El Grupo Procesos Corporativos deberá realizar revisiones periódicas de las oficinas que estén vacías asegurando que estén cerradas con llave.
- El Grupo de Procesos Corporativos deberá restringir al interior de la entidad el uso de equipos fotográficos, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello por parte del área encargada.
- El trabajo en áreas seguras debe estar monitoreado por circuitos cerrados de televisión (CCTV), teniendo en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.
- El Grupo de Procesos Corporativos deberá establecer lineamientos para los controles de área de despacho y carga teniendo en cuenta lo siguiente:
    - Las áreas de cargue y descargue deberán estar señalizadas.
    - Los puntos de acceso como el área de entrega y las zonas de carga deberán ser controladas y monitoreadas mediante circuitos cerrados de televisión (CCTV).
    - El material que ingresa se deberá inspeccionar y examinar para determinar la presencia de materiales peligrosos.

13.2 EQUIPOS (A.11.2)[27]

- El Grupo de Procesos Corporativos deberá establecer lineamientos para los controles de ubicación y protección de los equipos teniendo en cuenta lo siguiente:
    - Los equipos de cómputo e impresoras deberán estar situados y protegidos para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
    - Todos los equipos portátiles deben estar protegidos por guaya de seguridad.
    - Establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información.
- El Grupo de Control Interno podrá auditar los registros de acceso a las diferentes dependencias del nivel central, direcciones territoriales y áreas protegidas. La entidad debe implementar el uso de un control de acceso biométrico, Lector de Proximidad, a las áreas restringidas para evitar la presencia de desconocidos no escoltados por personal autorizado.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe establecer lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deberán conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deberán conectarse a la red eléctrica no regulada.
- El Grupo de Tecnologias de la Información y las Comunicaciones con el acompañamiento del Grupo de Procesos Corporativos deberán implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento.
- El Grupo de Procesos Corporativos deberá suministrar plantas eléctricas a las sedes de la entidad y el Grupo de Tecnologias de la Información y las Comunicaciones las UPS, y garantizar su manteamiento preventivo y correctivo.
- El cableado que transporta datos y de suministro de energía deberán estar protegidos contra la interceptación, interferencia o daños.
- Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencia.
- Deberán tener en cuenta las consideraciones técnicas de las normas vigentes y el reglamento técnico de instalaciones eléctricas RETIE.
- Los cuartos de cableado solo podrán tener los elementos activos para su funcionamiento y no utilizarse como almacén para guardar cajas, mesas u otros equipos que no estén en uso.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir mecanismos de soporte y mantenimiento a los equipos.
- Las actividades de mantenimiento tanto preventivo como correctivo deberán registrarse.
- Solo el personal autorizado deberá llevar a cabo el mantenimiento o las reparaciones a los equipos tecnológicos de la entidad.
- En caso de presentarse una falla o problema de hardware o software en una estación de trabajo o equipo portátil de propiedad de la entidad, el usuario responsable del mismo deberá informarlo al Grupo de Tecnologias de la Información y las Comunicaciones, para una asistencia especializada, y por ningún motivo deberá intentar resolver el problema.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas.

[27] **A.11.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- Los equipos que requieran salir de las instalaciones de la entidad para reparación o mantenimiento deberán estar debidamente autorizados y se deberán verificar que en dichos elementos no cuenten con información catalogada como (Clasificada – Reservada). En caso de contener información reservada o clasificada, se deberá realizar respaldo de la información y borrado seguro.
- El Grupo de Procesos Corporativos deberá registrar cuando los equipos de cómputo ingresan y se retiran de las instalaciones de la entidad.
- El Grupo de Procesos Corporativos deberá llevar un control en el almacén de los equipos cuando se asignan y cuando se hace su devolución.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá garantizar que los equipos de cómputo que salgan de las instalaciones de la entidad deben estar cifrados.
- Todo equipo de cómputo que se quiera retirar de las instalaciones de la entidad deberá ser autorizado por el jefe inmediato e informado a servicio de Seguridad para que se permita su salida.
- El ingreso y salida de servidores y de dispositivos de comunicaciones de las instalaciones de la entidad debe estar debidamente autorizado por el Grupo de Tecnologias de la Información y las Comunicaciones y el Grupo de Procesos Corporativos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá garantizar que cuando un dispositivo vaya a ser reasignado o retirado de servicio, deberá garantizarse la eliminación de toda información mediante borrado seguro teniendo en cuenta que previo a esta actividad deberá realizar copia de seguridad de esta.
- Los Colaboradores de la entidad, durante su ausencia no deberán conservar sobre el escritorio información propia de la entidad como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.
- Los Colaboradores de la entidad, deberán bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el computador y cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- Los Colaboradores de la entidad que impriman documentos con clasificación (Clasificada –Reservada), estos deberán ser retirados de la impresora inmediatamente y no se deberán dejar en el escritorio sin custodia.
- No se deberá reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deberán ser destruidos y no deberán estar como papel reciclable.
- Los documentos impresos con clasificación (Clasificada – Reservada), no deberán publicarse.
- Los lugares de trabajo de los Colaboradores de la entidad y terceras partes que prestan sus servicios a la entidad y cuyas funciones no obliguen a la atención directa de ciudadanos deberán localizarse preferiblemente en ubicaciones físicas que no queden expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.
- Todos los computadores de la entidad deberán tener configurado y en operación un protector de pantalla con tiempo máximo de tres (3) minutos para que se active cuando el equipo no esté en uso.
- Los equipos críticos de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe asegurar que la infraestructura de servicios de Tecnologias de la información esté cubierta por mantenimiento y soporte adecuados de hardware y software.
- Los servidores públicos y contratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de la entidad no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

- Las estaciones de trabajo, equipos portátiles y demás recursos informáticos como impresoras, fotocopiadoras, máquinas de fax y video proyectores, entre otros, de propiedad de la entidad no deben ser utilizados para actividades personales o ajenas a la entidad.
- Las estaciones de trabajo, equipos portátiles y demás recursos informáticos de la entidad deben ser operados solamente por personal autorizado y/o el responsable de estos.
- La protección física de las estaciones de trabajo, equipos portátiles y demás recursos informáticos corresponde a los responsables o custodios de estos y es su deber, notificar cualquier eventualidad que ocurra sobre dichos equipos al Grupo de Tecnologias de la Información y las Comunicaciones.
- Los equipos que hacen parte de la infraestructura tecnológica de la entidad tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, así como estaciones de trabajo y dispositivos de almacenamiento (digitales o no digitales), copias de respaldo, y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se deben adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de peligros ambientales y amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.
- Cuando un servidor público inicie o termine su vinculación laboral con la entidad, sea trasladado entre áreas, sedes, o por alguna otra circunstancia deje de utilizar el computador de escritorio o el recurso informático suministrado con carácter permanente, deberá entregar dicho recurso formalmente al Grupo de Tecnologias de la Información y las Comunicaciones o, en su defecto, a su jefe inmediato.
- El alistamiento de las estaciones de trabajo y equipos portátiles es responsabilidad del Grupo de Tecnologias de la Información y las Comunicaciones, así como la eliminación segura de la información de estos.
- El Grupo de Tecnologias de la Información y las Comunicaciones, debe procurar que todos los recursos informáticos tales como servidores, dispositivos de comunicación, estaciones de trabajo, equipos portátiles e impresoras, entre otros, que sean propiedad de la entidad se encuentren continuamente actualizados en aras de conservar e incrementar la calidad del servicio que prestan, mediante la mejora de su desempeño y obtener mayor estabilidad y protección ante amenazas.

14. SEGURIDAD DE LAS OPERACIONES (A.12)[28]

14.1.PROCEDIMIENTO DE OPERACIONES Y RESPONSABILIDADES (A.12.1)[29]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá poner a disposición de todos los colaboradores los procedimientos de operación.
- La configuración de servidores, equipos activos, enrutadores, switches, firewall, sistemas de detección y protección de intrusos y otros dispositivos de seguridad de red; debe ser documentada para cada equipo o

[28] **A.12 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[29] **A.12.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

dispositivo, respaldada por copia de seguridad y mantenida por el Grupo de Tecnologias de la Información y las Comunicaciones.

- Toda modificación en la configuración de los servidores, equipos activos y demás equipos de red debe ser documentada y junto con el respaldo de la nueva configuración inmediatamente actualizada a los responsables de conservar dicha información.
- Todo equipo de Tecnologias de la Información debe ser revisado, registrado y aprobado por el Grupo de Tecnologias de la Información y las Comunicaciones antes de conectarse a cualquier nodo de la red de comunicaciones y datos de la entidad. Dicho Grupo debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe establecer un procedimiento que permita asegurar la gestión de cambios normales y de emergencia a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar los responsables y tareas en la gestión de cambios.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe establecer un comité de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá documentar la gestión de capacidad la cual le permita:
    - Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.
    - Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.
    - Documentar los datos de rendimiento y capacidad de la plataforma tecnológica de la entidad.
    - Documentar los acuerdos de niveles de servicio.
    - Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.
    - Realizar las recomendaciones de mejora de la infraestructura de tecnología.
    - Definir los indicadores de rendimiento correspondientes a la gestión de capacidad.
    - Definir indicadores de rendimiento correspondientes a la gestión de capacidad.
    - Deberá asignar un responsable de la gestión de capacidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer cuotas de almacenamiento para cada recurso compartido, adicional a esto se deberá definir umbrales que permitan notificar al administrador del servicio de almacenamiento y al administrador de carpeta que el espacio asignado ya está llegando a su límite. Cada cuota está sujeta a las necesidades de cada área y a la proyección de crecimiento de cada una de ellas.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá restringir excepto en las dependencias que por el desarrollo de sus funciones sean necesarios almacenamiento de tipo de archivos como:
    - Audio (.avi, .mpeg, .mp3, .mid o .midi, .wav, .wma, .cda, .ogg, .ogm, .aac, .ac3, flac, .mp4, .aym)
    - Video (.avi,.mpeg, .mov, .wmv, .rm, .flv)
    - Archivos ejecutables (.exe, .bat, .com, bin)
    - Archivos de páginas web (html, xml,jsp,asp)
    - Archivos de sistema (.acm,.dll,.ocx,.sys,.vxd)
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá crear grupos de seguridad en el directorio activo con rol de lectura y escritura, de acuerdo con las necesidades solicitadas por cada dependencia. Se deberá configurar los grupos de seguridad en cada una de las carpetas de primer nivel.

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá generar reportes trimestrales en cada una de sus soluciones, evidenciando que tipos de archivos se encuentran alojados, archivos por propietarios, archivos duplicados, archivos grandes, archivos no usados recientemente, para determinar acciones que eviten posibles fallas en la solución de almacenamiento de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar la separación de ambientes de desarrollo, pruebas y producción, los cuales deberán estar separados de manera física y lógica.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir y documentar los lineamientos a seguir para la transferencia entre ambientes.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá utilizar datos que no sean sensibles para la entidad, en los ambientes de prueba.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá permitir que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

14.2. PROTECCIÓN CONTRA CÓDIGO MALICIOSO (A.12.2)[30]

- Parques Nacionales Naturales de Colombia debe contar con las herramientas de seguridad tales como antivirus, antiSpam, antispyware, seguridad perimetral y otras aplicaciones que permitan brindar la adecuada protección contra código malicioso, malware, phishing, ransomware, entre otros con el fin de evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar campañas de concienciación de usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá dictar los lineamientos para la instalación de software antivirus que brinde protección contra códigos maliciosos en todos los recursos informáticos de la entidad y asegurar que estas herramientas no puedan ser deshabilitadas, así como mantenerlas actualizadas permanentes.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar la actualización continua de la base de firmas y parches correspondiente del software de antivirus y actualizaciones de sistema operativo.
- Todo mensaje sospechoso de procedencia desconocida deberá ser inmediatamente reportado al Grupo de Tecnologias de la Información y las Comunicaciones a través de la mesa de servicios, tomando las medidas de control necesarias.
- Los servidores públicos y/o contratistas que detecten alguna infección por software malicioso deben reportar al Grupo de Tecnologias de la Información y las Comunicaciones, mediante la mesa de servicio.
- Los servidores públicos y/o contratistas tendrán prohibido, la desinstalación y/o desactivación de software y herramientas de seguridad aprobadas por el Grupo de Tecnologias de la Información y las Comunicaciones.
- Los servidores públicos y/o contratistas tienen prohibido, escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica de la entidad.

[30] **A.12.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

14.3. COPIAS DE RESPALDO (A.12.3)[31]

- Parques Nacionales Naturales de Colombia debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el Grupo de Tecnologias de la Información y las Comunicaciones y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la entidad, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente respaldada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones establecerá procedimientos o un plan de copia de seguridad de la entidad donde se establezca esquemas de qué, cuándo, con qué periodicidad, cual es la criticidad explícitos de respaldo, número de copias y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de esta. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información respaldada.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar y mantener copias de seguridad de la información digital solicitadas por los directores, subdirectores, coordinadores y/o jefes de oficina.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir la custodia y almacenamiento de las copias.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá tener un inventario y bitácora de las copias que se realizan y de las copias que se restauran.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá dar los lineamientos para la realización de las copias de seguridad de:
    - Bases de datos en producción.
    - Software de aplicaciones.
    - Sistemas operativos.
    - Software base de la entidad.
    - Cuentas de correo electrónico con valor estratégico para la entidad (Director, Jefes, Directores, Subdirectores, Coordinadores, Asesores, Administradores de Sistemas, entre otros).
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá generar mecanismos que mantengan la integridad y confidencialidad de las copias de seguridad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.
- Los colaboradores son responsables de la información que resida en el computador asignado y serán los encargados de mantener copia de sus archivos más sensibles entregando al supervisor del contrato o jefe inmediato en custodia al finalizar la vinculación. En caso de que los colaboradores requieran la ejecución de un respaldo de información, lo pueden solicitar al Grupo de Tecnologias de la Información y las Comunicaciones a través de la mesa de servicios (GLPI).

[31] **A.12.3 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- Las copias de seguridad de la información (back-up), deberán ser almacenadas dentro y fuera de la entidad (Nube), como medida preventiva para asegurar la recuperación total de los datos. En caso de tener una sola copia debe ser llevada fuera de la sede o sitio del procesamiento de datos. El traslado de los medios y/o dispositivos debe ser realizado por personal debidamente autorizado, teniendo en cuentas las medidas de seguridad.

14.4. REGISTRO Y SEGUIMIENTO (A.12.4)[32]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar monitoreo periódico sobre los aplicativos y velar por la generación de los registros de auditoría (log´s).
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá salvaguardar los registros de auditoría que se generen de cada sistema.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá monitorear las excepciones o los eventos de la seguridad de información.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y la misión de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

14.5. CONTROL DE SOFTWARE OPERACIONAL (A.12.5)[33]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá usar controles para proteger todo el software implementado y la documentación del sistema.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá conservar las versiones anteriores del software de aplicación como una medida de contingencia, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores.
- Las actualizaciones del software, de las aplicaciones y librerías las deben realizar únicamente colaboradores que tengan los roles, privilegios y el conocimiento en cada una de las aplicaciones.
- Los servidores de aplicación únicamente deben alojar los códigos ejecutables aprobados de las mismas, de ninguna manera se debe alojar el código fuente o de desarrollo ni los compiladores.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer estrategias de retroceso (rollback) antes de implementar los cambios.

---

[32] **A.12.4 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[33] **A.12.5 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

14.6 GESTIÓN DE VULNERABILIDADES (A.12.6)[34]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá:
  - Realizar de manera periódica revisión de vulnerabilidades técnicas por medio de pruebas de penetración, a los sistemas de información críticos y misionales.
  - Documentar, informar, gestionar y corregir, los hallazgos de las vulnerabilidades adoptando las acciones preventivas y correctivas necesarias para minimizar el nivel de riesgo y reducir el impacto.
  - Definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, las pruebas de gestión, la aplicación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.
  - Si está disponible una actualización de una fuente legítima, se deberán valorar los riesgos asociados con la instalación de la actualización y se deberán probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar.
- Todas las instalaciones de software que se realicen sobre equipos de la entidad deben ser aprobadas por el Grupo de Tecnologias de la Información y las Comunicaciones, de acuerdo con los procedimientos elaborados para tal fin por dicha oficina.
- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la Ley 23 de 1982 y relacionadas. El Grupo de Tecnologias de la Información y las Comunicaciones debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad.
- Corresponde al Grupo de Tecnologias de la Información y las Comunicaciones mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los servidores, estaciones de trabajo y demás equipos de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole derechos de autor.
- El Grupo de Tecnologias de la Información y las Comunicaciones podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo.
- Sólo está permitido el uso de software licenciado por la entidad y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por el Grupo de Tecnologias de la Información y las Comunicaciones. Las aplicaciones desarrolladas al interior de la entidad, en desarrollo de su misión, deberán ser reportadas al Grupo de Tecnologias de la Información y las Comunicaciones, para su administración.
- El Grupo de Tecnologias de la Información y las Comunicaciones es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros o utilizado para fines personales.

14.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE LA INFORMACIÓN (A.12.7)[35]

[34] **A.12.6 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[35] **A.14.7 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- El Grupo de Tecnologias de la Información y las Comunicaciones, como segunda línea de defensa y líder de la política de seguridad digital, planificará actividades que involucren auditorías de los sistemas críticos en producción, limitando el acceso al sistema de información y a los datos de solo de lectura (en caso de acceso diferente al de solo lectura se deberá acordar previamente), determinando tareas, responsables y estas se deberán realizar fuera del horario laboral.
- El Grupo de Tecnologias de la Información y las Comunicaciones, como segunda línea y líder de la política de seguridad digital, deberá mantener los documentos, dispositivos y medios utilizados para las auditorías de los sistemas de información custodiados de accesos no autorizados.
- El Grupo de Control Interno como tercera línea de defensa realizará evaluaciones independientes a los sistemas de información y al SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN de la entidad, de acuerdo con lo establecido en su Plan Anual de Auditorías y conforme a las necesidades y expectativas de la Alta Dirección
- Todas las dependencias de Parques Nacionales Naturales de Colombia, direcciones territoriales y áreas protegidas como primera línea de defensa deberán acatar las políticas contempladas en el siguiente manual e informar al Grupo de Tecnologías de la Información y las Comunicaciones en caso de detectar posibles desviaciones o vulneraciones en sus áreas.

15. SEGURIDAD DE LAS COMUNICACIONES (A.13)[36]

15.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES (A.13.1)[37]

- La plataforma tecnológica de la entidad que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El Grupo de Tecnologias de la Información y las Comunicaciones es el encargado de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar segmentación de redes para colaboradores y visitantes de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- El Grupo de Tecnologias de la Información y las Comunicaciones es el responsable de mantener disponible toda la infraestructura de red que soportan los servicios tecnológicos de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe establecer los procedimientos, guías y demás documentación que permita la gestión de los dispositivos de red de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá disponer de una zona desmilitarizada o DMZ, entre la red interna de la entidad y la red externa (internet) con el objetivo delimitar

[36] **A.13- Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[37] **A.13-1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

conexiones desde la red interna hacia internet y limitar las conexiones desde internet hacia la red interna de la entidad con los siguientes criterios:
    - El tráfico de la red externa a la DMZ está limitado.
    - El tráfico de la red externa a la red interna deberá estar restringido y monitoreado.
    - El tráfico de la red interna a la DMZ está limitado.
    - El tráfico de la red interna a la red externa está limitado
- La DMZ deberá implementar controles para ofrecer servicios que se necesitan desde internet.
- Estos servicios deberán ser monitoreados con el fin de prevenir ataques.
- La arquitectura de la DMZ deberá estar aislada de la red interna de la entidad de forma que no permita el acceso no autorizado a la red interna, por lo que se deberán diseñar redes perimetrales con los siguientes objetivos:
    - No se pueden hacer consultas directas a la red interna de la entidad desde redes externas e internet.
    - Se deberá realizar la segmentación de redes y listas de acceso a los servicios de la entidad, tales como servidores, administración, invitados, Etc.
    - El acceso a la red de datos de la entidad y a los sistemas de información soportados por la misma, es de carácter restringido. Se concederán permisos con base a "la necesidad de conocer" y el "acceso mínimo requerido".
    - La conexión a la red wifi institucional para servidores públicos deberá ser administrada desde el Grupo de Tecnologias de la Información y las Comunicaciones mediante un SSID (Service Set Identifier) único a nivel de las sedes de la entidad, la autenticación deberá ser con usuario y contraseña de directorio activo.
    - La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas diferentes y será administrada por el Grupo de Tecnologias de la Información y las Comunicaciones; la contraseña deberá cambiar mensualmente y solo estará disponible en el horario laboral definido por la entidad
- Los colaboradores que requieran acceder a los recursos informáticos de la entidad fuera de las instalaciones de la entidad deberán realizarlo a través de una conexión de red virtual privada (VPN), previa autorización del jefe inmediato o Supervisor de contrato y del Coordinador del Grupo de Tecnologias de la Información y las Comunicaciones
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá realizar revisiones e inactivaciones de las conexiones VPN cada treinta (30) días o de acuerdo con las solicitudes de desactivación generadas en la mesa de servicio (GLPI).
- Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

15.2 TRANSFERENCIA DE INFORMACIÓN (A.13.2)[38]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones de la entidad.

[38] **A.13-2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer procedimientos para la detección de software malicioso y protección contra éste.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá contar con los lineamientos para proteger la información transferida con respecto a la interceptación, copiado, modificación, enrutado y destrucción de esta.
- El intercambio de información digital pública clasificada y pública reservada, debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y que cumpla con la política de controles criptográficos, esto debe quedar registrado en los convenios o acuerdos de intercambio de información que firmen las partes.
- El Grupo de Procesos Corporativos establecerá lineamientos sobre retención, disposición y transferencia de la información física de la entidad, de acuerdo con la legislación y reglamentaciones locales y nacionales.
- El Grupo de Tecnologias de la Información y las Comunicaciones y la Oficina Asesora Jurídica deberán establecer un acuerdo para la transferencia de información entre la entidad y las partes externas.
- Todo intercambio de información electrónica perteneciente a la entidad con terceros debe ser respaldado con un acuerdo (convenio o contrato), incluyendo una cláusula de confidencialidad y no divulgación de la información proporcionada.
- Para el transporte de medios físicos de información sensible, se debe generar una bitácora de entrega de estos medios y recepción de estos.
- Para la apertura de ese sello se debe generar un registro y garantizar que no se reutilice el sello.
- Se deben transportar estos medios en un recipiente que proteja al activo de amenazas
- ambientales.
- Toda información enviada desde la entidad a través de correos electrónicos deberá incluir en su pie de página la siguiente advertencia:
  "Este mensaje y cualquier archivo que se adjunte al mismo es confidencial y podría contener información clasificada y reservada de la entidad, para el uso exclusivo de su destinatario. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo al remitente y borrar el mensaje recibido inmediatamente".
- Solo se puede realizar intercambio de información de la entidad entre su personal cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus actividades.
- Se deberán identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
- Para el caso de contratistas y proveedores, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la entidad a personas o entidades externas.
- Todo servidor público de la entidad es responsable de proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.
- Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

- Los acuerdos de confidencialidad deben aceptarse por los contratistas y proveedores como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

16. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS (A.14)[39]

16.1 REQUISITOS DE SEGURIDAD PARA LOS SISTEMAS DE INFORMACIÓN (A.14.1)[40]

El Grupo de Tecnologias de la Información y las Comunicaciones deberá cumplir con los siguientes lineamientos de seguridad:

- El Grupo de Tecnologias de la Información y las Comunicaciones debe elegir, elaborar, mantener y difundir un documento que describa las "Características y metodología para el desarrollo y adquisición de sistemas de información en la entidad", debe especificar los requisitos de seguridad y el framework que debe utilizar la entidad, para contratar la adquisición, desarrollo o mejoras de sus sistemas de información o soluciones de software, los cuales debe cumplir el contratista o casa de software para el suministro de la solución. El documento debe incluir un conjunto estandarizado de requerimientos de seguridad, conceptos, buenas prácticas, criterios, procesos, plantillas y demás características que sirvan para adquirir o contratar los desarrollos de las soluciones de software en un ambiente de mitigación del riesgo y aseguramiento de la calidad.
- Todo proyecto de adquisición o compra de software debe contar con un documento de identificación y valoración de riesgos del proyecto aprobado por el Grupo de Tecnologias de la Información y las Comunicaciones. La entidad no debe emprender procesos de adquisición, desarrollo o mantenimiento de aplicativos o soluciones de software que tengan asociados riesgos altos no mitigados.
- Los aplicativos o soluciones de software adquiridos a través de terceras partes deben certificar por escrito el cumplimiento de los requisitos y estándares de calidad en el proceso de desarrollo.
- El desarrollo de software deberá incluir los siguientes puntos:
    - Acuerdos de licencias, propiedad del código fuente y derechos conferidos.
    - Requerimientos con respecto a la calidad del código fuente y la existencia de garantías.
    - Procedimientos de certificación y verificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos en los términos de referencia.
    - Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.
- En caso de desarrollos propios al interior de la entidad, estos se deben separar en ambientes de desarrollo, prueba y producción, en diferentes procesadores y dominios.
- Todo sistema de información y/o aplicación que se vaya a desarrollar debe estar integrado al directorio activo como fuente de autenticación al mismo.
- El Grupo de Tecnologias de la Información y las Comunicaciones debe asegurar que:

[39] **A.14 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[40] **A.14.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- En el desarrollo o adquisición de sistemas de información se definen todos los requerimientos necesarios para su buen funcionamiento.
- Existe integración de los sistemas de información con los que cuenta la organización.
- Se ejecuten todas las pruebas necesarias antes de la puesta en funcionamiento (producción) a cualquier solución que se implemente.
- Se documenten los sistemas de información y/o aplicaciones y que se realicen las actualizaciones correspondientes cuando éstas son modificadas. Toda adquisición, desarrollo o modificación de sistemas de información y/o aplicación deberán incluir el suministro y/o actualización de la documentación correspondiente del sistema o módulo:
  - Especificaciones funcionales.
  - Especificaciones de seguridad.
  - Manual de Instalación y configuración.
  - Manual de administración, operación y mantenimiento.
  - Manual de usuario.

- La seguridad de la información sea parte integral en el ciclo de vida de las aplicaciones.
- Se entreguen los medios (programa fuente, programas objeto, licencias y manuales), de los sistemas de información para ser inventariados, contar con las garantías y licenciamientos como resultado de la adquisición o desarrollo realizado.
- Se deberán realizar 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.
- Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- El Grupo de Tecnologias de la Información y las Comunicaciones será la única dependencia autorizada para realizar copia de seguridad del software original.
- El software proporcionado por el Grupo de Tecnologias de la Información y las Comunicaciones no puede ser copiado o suministrado a terceros.
- Cualquier desarrollo deberá implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.
- Toda aplicación o sistema de información que deba exponerse en internet debe contar con un certificado digital válido.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones de la entidad.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la entidad, teniendo en cuenta los siguientes criterios
  - Mantener privacidad en las partes involucradas.
  - Cifrar las comunicaciones cuando sea necesario.
  - Los protocolos de comunicación estén asegurados.
  - La información almacenada de las transacciones no se encuentre pública.

16.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO DE SOFTWARE Y SOPORTE (A.14.2)[41]

- El Grupo de Tecnologias de la Información y las Comunicaciones cuando realice o contrate desarrollos de aplicaciones o sistemas de información deberá tener en cuenta como mínimo los siguientes aspectos:
  - Orientar sobre buenas prácticas de seguridad en el desarrollo del software.
  - Requisitos de seguridad en el control de versiones.
  - Capacidad de los desarrolladores para encontrar y resolver vulnerabilidades.
  - Reutilización de código.
  - Mantener un rastro de auditoría de los cambios.
- Cuando el Grupo de Tecnologias de la Información y las Comunicaciones desarrolle o realice mejoras a las aplicaciones o sistemas de información deberán definir controles para que los cambios realizados sean documentados, teniendo en cuenta la integridad de los sistemas y/o aplicaciones desde las primeras etapas de diseño y a través de los mantenimientos posteriores.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir un proceso formal para inclusión y cambios importantes de los sistemas de información y/o aplicaciones involucrando pruebas, control de calidad e implementación cuando se realicen actualizaciones o nuevos desarrollos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá guardar en un repositorio, las versiones anteriores de cada sistema de información que esté actualizado.
- Todo cambio a nivel de aplicación y/o sistema de información debe notificarse con tiempo al dueño del activo permitiendo realizar pruebas y revisiones apropiadas antes de su implementación.
- Todo cambio que se realice a un sistema de información o a una aplicación siempre debe hacerse en un ambiente de desarrollo nunca sobre el ambiente de producción.
- Todos los colaboradores de la entidad deberán evitar realizar modificaciones a los paquetes de software, en la medida de lo posible se deberán usar directamente los dados por el proveedor; limitándose únicamente a cambios necesarios, cuando se hagan, se deberán tener en cuenta los siguientes aspectos:
  - El riesgo en que se puede ver involucrado el sistema de información.
  - Verificar si se requiere consentimiento del vendedor.
  - Verificar la posibilidad que el vendedor realice dichos cambios.
  - El impacto en dado caso que el mantenimiento futuro recaiga en manos de la entidad oficina.
  - La compatibilidad con otro software en uso.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá conservar el software original cuando se hayan realizado cambios en los paquetes de este.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir ambientes de desarrollo seguro, teniendo en cuenta los siguientes aspectos:
  - El carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
  - Requisitos externos como reglamentaciones o políticas.
  - Controles de Seguridad ya establecidos por la entidad.
  - Separación entre diferentes ambientes de desarrollo.
  - Control de acceso al ambiente de desarrollo.
  - Seguimiento de los cambios en el ambiente y los códigos almacenados allí.

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir controles para que los sistemas adquiridos externamente cumplan con los siguientes aspectos:

[41] **A.14.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- Acuerdos de licenciamiento, propiedad de códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
- Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
- Evidencia del uso de umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
- Evidencia de pruebas para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.
- Evidencia de pruebas para proteger contra la presencia de vulnerabilidades conocidas.
- Derecho contractual con relación a procesos y controles de desarrollo de auditorías.
- Documentación del ambiente de construcción usado para crear entregables.

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá contemplar en los cambios y en los nuevos sistemas de información, pruebas asociadas a seguridad de la información.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá contar en sus pruebas de aceptación la verificación de los requisitos de seguridad de la información.
- Para los sistemas adquiridos o desarrollos contratados con terceros, el proveedor debe entregar resultados de pruebas de vulnerabilidad, los cuales no deben tener vulnerabilidades críticas ni altas ni medias. Para los desarrollos internos se deben realizar pruebas de vulnerabilidad y se debe recibir a producción si no hay vulnerabilidades críticas ni altas ni medias.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir controles para que los cambios en los sistemas de información de la entidad sean documentados, teniendo en cuenta la integridad de los sistemas desde las primeras etapas de diseño y a través de los mantenimientos posteriores.

16.3 DATOS DE PRUEBA (A.14.3)[42]

- En la fase de pruebas de los sistemas de información desarrollados o adquiridos, se deben utilizar datos despersonalizados (es decir, no datos de producción).
- Si se utilizan datos de producción, estos deben ser entregados a un servidor público responsable de los mismos, quien debe firmar el compromiso de confidencialidad y no divulgación de la información sobre los datos recibidos para pruebas. Una vez terminadas las pruebas estos deben ser borrados de manera segura.
- En cumplimiento de los requisitos legales de privacidad y seguridad de la información, los datos de prueba no deben contener información que permitan la identificación de la persona natural o jurídica a la que pertenezca la información.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá evitar durante la ejecución de pruebas en ambientes de desarrollo el uso de datos que contengan información personal o información sensible de la entidad que este contenida en el ambiente de producción de las aplicaciones.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá tener en cuenta controles de acceso a los ambientes de producción y de prueba.

[42] **A.14.3 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

17. RELACIONES CON PROVEEDORES (A.15)[43]

17.1 SEGURIDAD DE LA INFORMACIÓN CON LOS PROVEEDORES (A.15.1)[44]

- El Grupo de Contratos deberá establecer lineamientos para el cumplimiento de las obligaciones contractuales del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN con terceros o proveedores.
- El Grupo de Contratos deberá establecer en el momento de suscribirse contratos profesionales de apoyo a la gestión que se desarrollen dentro de la entidad, los riesgos asociados a la seguridad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información de la entidad.
- El Grupo de Contratos deberá establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.
- Cada dependencia de la entidad que establezca relación con proveedores y su cadena de suministro, solicitará capacitación periódica al Grupo de Tecnologias de la Información y las Comunicaciones referente a seguridad de la información con el fin de dar a conocer las políticas que tiene la entidad.
- Todos los proveedores, usuarios externos y servidores públicos de entidades externas deben estar autorizados por un servidor púbico de la entidad quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de Tecnología de la Información institucionales.

17.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES (A.15.2)[45]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica de la entidad.
- Las cuentas de proveedores y usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo con la naturaleza del usuario.
- Los proveedores y usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI de la entidad.

[43] **A.15 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[44] **A.15.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[45] **A.15.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

18. GESTIÓN DE INCIDENTES DE SEGURIDAD (A.16)[46]

18.1 GESTIÓN DE INCIDENTES Y MEJORAS (A.16.1)[47]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir los lineamientos para:
  - Responsables de la gestión de incidentes de seguridad de la información.
  - Los canales para que los colaboradores de la entidad puedan reportar los incidentes de seguridad de la información.
  - Para la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
  - Para la recolección de evidencia de incidentes de seguridad de la información.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes establecidos en los lineamientos para la gestión de incidentes.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá proporcionar los medios para el aprendizaje a la entidad de los incidentes de seguridad de la información.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá dar a conocer a los colaboradores de la entidad, los lineamientos establecidos para la gestión de incidentes de seguridad de la información.
- Los servidores públicos de la entidad deben reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad de la información a través de su Jefe de dependencia al Líder del sistema de gestión de seguridad de la información “Coordinador TIC”, quienes deben garantizar las herramientas informáticas para que formalmente se realicen tales reportes.
- Parques Nacionales Naturales de Colombia a través del Grupo de Tecnologias de la Información y las Comunicaciones podrá monitorear el tráfico en la red para administrar eficientemente los servicios de red, el ancho de banda, anticiparse a posibles amenazas y velar por el cumplimiento de las políticas de seguridad de la información.
- Los siguientes pueden ser considerados incidentes de seguridad de la información:
  - Fraude y robo de activos de información o de cómputo.
  - Divulgación, manipulación, destrucción o modificación no autorizada de la información de la entidad.
  - Interrupción de procesos y sistemas críticos de la entidad.
  - Fallas en la seguridad de los sistemas de información.
  - Fallas en la seguridad física de las instalaciones.
  - Acceso no autorizado a los recursos de la entidad.
  - Uso indebido de los privilegios dentro de un sistema.
  - Propagación de virus cibernéticos o código malicioso.
  - Intrusiones externas a la red (hackeo).
  - Instalación de software no autorizado, entre otros.
- Es responsabilidad de todos los servidores públicos y contratistas de la entidad reportar cualquier tipo de incidente relacionado con la información y/o los recursos informáticos a la mayor brevedad posible.
- Cualquier intento de interferencia, obstrucción o de disuadir a quien reporta una posible violación de seguridad, está prohibido y será motivo de una acción disciplinaria. De igual manera cualquier retaliación o amenaza contra la persona que realiza la investigación.

[46] **A.16 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[47] **A.16.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- Toda falla aparente de cualquier sistema de información o software debe ser reportada al Grupo de Tecnologias de la Información y las Comunicaciones, en caso de tratarse de un sistema de información adquirido a terceros debe reportarse la falla al proveedor del software.
- Los reportes de los incidentes deberán ser lo más completo posibles, aportando la mayor cantidad de evidencias a fin de facilitar la atención de este. Opcionalmente los servidores públicos podrán mantener el anonimato durante su reporte o denuncia.
- Todos los reportes deberán ser manejados con estricta confidencialidad.
- Queda prohibido divulgar cualquier información sobre un incidente de seguridad de la información a personal externo, a menos que por disposiciones legales la entidad se vea obligado a hacerlo. de ser así, deberá ser bajo la aprobación de la Alta Dirección y el Comité Institucional de Gestión y Desempeño.
- El servidor público o contratista que por negligencia no reporte a tiempo un incidente de seguridad o que aproveche deficiencias de seguridad y haga mal uso de la información, será investigado por el Oficina de Control Disciplinario Interno para establecer las sanciones disciplinarias a que haya lugar.
- Los incidentes de seguridad de la información que estén relacionados con requerimientos legales o regulatorios deberán ser reportados a autoridades externas por personal autorizado de la entidad.
- Después de recibida la notificación de un incidente de seguridad o vulnerabilidad de la información, el gestor de incidentes es responsable de asegurar que el propietario del activo de información y todas las personas involucradas con el incidente, estén informadas.
- Todos los incidentes de seguridad deben ser evaluados de acuerdo con su circunstancia particular; esto puede requerir o no la acción de varias áreas de la entidad. Cuando lo requiera la gravedad del incidente de seguridad el Oficina de Control Disciplinario Interno iniciará un proceso disciplinario para establecer las sanciones disciplinarias a partir de la falta cometida.
- Los incidentes de seguridad de la información deben ser investigados por personal calificado.
- Es necesario identificar las causas y planear como prevenir su reincidencia.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá crear bases de datos de incidentes con sus respectivas soluciones para que permitan reducir el tiempo de respuesta en caso de ocurrencia de nuevos incidentes.

19. ASPECTOS DE SEGURIDAD EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (A.17)[48]

19.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN (A.17.1)[49]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir los lineamientos de seguridad de la información que se deben seguir prestando mientras la entidad opere bajo estrategias del plan de continuidad del negocio.
- GTIC deberá generar un plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP).
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá diseñar una herramienta para el análisis de impacto al negocio tecnológico de la entidad, por medio del cual se identifiquen los servicios críticos de tecnología de la entidad.

[48] **A.17 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[49] **A.17.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá diseñar estrategias de recuperación de los servicios críticos de tecnología.
- Cada servicio tecnológico identificado como crítico o esencial deberá contar con planes de contingencia.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá identificar los escenarios y las estrategias del plan de recuperación tecnológica Planes de Recuperación de Desastres (DRP) de los servicios esenciales de tecnología identificados.
- Todas las estrategias de recuperación de tecnología deben contemplar los requisitos de seguridad de la información descritos en el presente manual.
- El plan de recuperación tecnológica y los planes de contingencia de los servicios de tecnología deberán ser aprobados como mínimo una vez al año.
- Los procesos que sean desarrollados por terceros deberán disponer de planes de contingencia y se deberá analizar su cobertura.
- Se debe definir un equipo para la planeación de pruebas, los procesos que estarán involucrados, la infraestructura tecnológica y/u operativa requerida, el plan de rollback y las actividades a realizar. Los participantes de los equipos deberán recibir sensibilización con respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.
- Se debe establecer un programa de pruebas, teniendo en cuenta los requerimientos técnicos necesarios. Las pruebas deberán ejecutarse de manera que simule las condiciones de un evento y no se afecte la operación.
- Se deben documentar las pruebas y se deben generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan de recuperación tecnológica.
- Se deben ejecutar procedimientos de control de cambios según las acciones preventivas y correctivas que se generaron a partir de las pruebas, para asegurar que el Plan de recuperación tecnología se mantenga actualizado y mejorado.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá y someter a aprobación por parte del comité institucional de gestión y desempeño todos los planes.

19.2 CONTINGENCIAS (A.17.2)[50]

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá contar con sistemas redundantes para los servicios críticos de la entidad con el fin de garantizar la disponibilidad de estos.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.

20. CUMPLIMIENTO (A.18)[51]

20.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES (A.18.1)[52]

---

[51] **A.18 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

[52] **A.18.1 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

- El Grupo de Tecnologias de la Información y las Comunicaciones deberá identificar, documentar y actualizar la legislación referente a seguridad de la información en el normograma de este.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá definir controles con el objetivo de proteger adecuadamente la propiedad intelectual tanto propia como la de terceros, tales como derechos de autor de software, licencias y código fuente.
- El Grupo de Tecnologias de la Información y las Comunicaciones deberá generar conciencia a los colaboradores de la entidad sobre los derechos de propiedad intelectual, no copiar total ni parcialmente libros, artículo u otros documentos diferentes de los permitidos por la ley de derechos de autor.
- El Grupo de Gestión Documental y el Grupo de Tecnologias de la Información y las Comunicaciones deberán definir y establecer:
    - Directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital.
    - Deberá establecer e implementar controles para proteger los registros contra pérdida, destrucción y falsificación de información física y digital.
    - Deberá establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.
- Parques Nacionales Naturales de Colombia deberá tomar todas las precauciones para conservar la confidencialidad y la integridad de todos los datos de carácter personal que la entidad conserve de servidores públicos, contratistas o terceros, almacenados o archivados en cualquier medio, entre otros están: cualquier información numérica, alfabética, gráfica, fotográfica, audiovisual o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Se deben adoptar los controles necesarios como lo exigen la Ley 1581 de 2012 y el Decreto 1377 de 2013, para prevenir incidentes de seguridad relacionados con la información personal que conserve la entidad en cualquier forma de almacenamiento.
- Todos los servidores públicos y contratistas deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones. La entidad redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los servidores públicos y contratistas que tengan acceso a información clasificada o reservada. La copia firmada del compromiso será retenida en forma segura por la entidad.
- Mediante este instrumento el subscriptor se comprometerá a utilizar la información solamente para el uso específico al que está destinada y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del responsable del activo de que se trate. El “Compromiso de Confidencialidad” deberá especificar que determinadas actividades pueden ser objeto de control y monitoreo.
- Parques Nacionales Naturales de Colombia requiere que la propiedad de su información se mantenga. Por regla general toda obra (incluido el software), patente, modelo de utilidad, diseño industrial, marca, logotipo, base de datos, etc., relacionados con los procesos de la entidad, que se desarrollen de manera colectiva y/o individual, bajo las políticas y directrices institucionales, son propiedad de la entidad, su uso es considerado restringido para los fines de la misión y deberá ser protegido de otro descubrimiento o uso que menoscabe la reputación de la entidad.

En consecuencia:

Los servidores públicos y contratistas están obligados a poner en conocimiento de sus jefes tales elementos de desarrollo, realizado con recursos de la entidad y a transferir de manera solemne, cuando por ley se requiera, todos los derechos que se deriven de los mismos a favor de la entidad.

Las personas contratadas por la entidad para la prestación de servicios de desarrollo de software, deberán garantizar la propiedad de los derechos patrimoniales sobre el software contratado en cabeza de la entidad.

Para estos efectos los contratos deberán:

- Ser por escrito entre autor y la entidad y en ellos se pactará la remuneración.
- Indicar que se elaboran por cuenta y riesgo de la entidad.
- Todos los desarrollos serán de propiedad de la entidad y este conservará todos los derechos incluyendo los de autor sobre estos desarrollos.
- Establecer el plan señalado por la entidad determinando condiciones de necesidad, características y atributos de la obra, y estableciendo los lineamientos de tiempo, modo y lugar para su desarrollo.

20.1 REVISIONES (A.18.2)[53]

- Los Líderes de los procesos deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión en auditorías.
- Los líderes de los procesos deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se tomarán las acciones necesarias.
- El Grupo de Tecnologias de la Información y las Comunicaciones, como segunda de defensa y líder de la política de seguridad digital realizará auditorías internas periódicas para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.
- La Oficina de Control Interno, como tercera línea de defensa, realizará la evaluación independiente al Sistema de Gestión de Seguridad de la Información, a partir de los resultados de las auditorías adelantadas por la segunda línea de defensa (Líder de Política) y conforme a lo establecido en el Plan Anual de Auditoría.

[53] **A.18.2 - Anexo A en ISO 27001**: Documento normativo que sirve como guía para la implementación de los controles específicos de seguridad de la información, estos están dirigidos a la mejora organizacional

21. CONTROL DE CAMBIOS

FECHA VERSIÓN (presente en el encabezado del documento)	**VERSIÓN**	**MOTIVO DE LA ACTUALIZACIÓN**
08/05/2024	01	Se crea el documento en el Sistema de Gestión Integrado.

CONTROL DE REVISIÓN Y APROBACIÓN		
Elaboró o Actualización	Nombre	Fernando Bolívar Buitrago, Alan Aguia, Andrés Camilo López, Farley Guzmán, Oscar Prada, Víctor Linero, Víctor Rodríguez, Giovanny Gutiérrez, Sandra Milena Gómez.
	Cargo	Profesionales Contratistas GTICs
Revisó	Nombre	Carlos Arturo Sáenz Barón Adriana Lorena Bernal Gloria Pereira y Pedro Pardo Lagos
	Cargo	Coordinador Grupo de Tecnologías de la Información y las Comunicaciones Contratista GTICs Contratistas OAP – Equipo Calidad
Aprobó	Nombre	Carlos Arturo Sáenz Barón
	Cargo	Coordinador Grupo de Tecnologías de la Información y las Comunicaciones