CONTENIDO

1. INTRODUCCIÓN

Anditel S.A.S tiene la responsabilidad de implementar un direccionamiento estratégico en materia de Seguridad de la Información, por ello el desarrollo de diferentes políticas enmarcadas en este documento, le permitirá tomar decisiones más ágiles y acertadas frente a sus riesgos y objetivos, permitiendo una gestión oportuna y efectiva de los recursos con que cuenta.

La referencia principal para el desarrollo de una política de Seguridad de la Información orientada al desarrollo de mejores prácticas de gestión, es la Norma NTC-ISO/IEC 27001 de 2013, los modelos y guías de Gobierno en Línea (GEL) generados por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC).

Por lo anterior, Anditel S.A.S define las políticas de seguridad de la información con el fin de atender estos nuevos requisitos orientadas al aseguramiento de la información que se genera en el cumplimiento del objetivo estratégico.

2. OBJETIVOS

2.1. Objetivo General

Preservar la confidencialidad, integridad y disponibilidad de los activos de información de Anditel S.A.S.

2.2 Objetivos Específicos

a) Establecer unas políticas y fundamentos base para la implementación efectiva de controles de seguridad de la información.
b) Definir la conducta esperada en el acceso, manejo de los activos de información.

c) Establecer y comunicar la responsabilidad en el uso de los activos de información que soportan los procesos y sistemas de Anditel S.A.S.

3. ALCANCE

Estas políticas aplican a todos los interesados de Anditel S.A.S y contratistas de acuerdo al nivel de acceso a la información que les haya sido asignado y su aplicación es obligatoria.

3.1 Cumplimiento de Anditel S.A.S.

Las direcciones de Anditel S.A.S proveen evidencia de su compromiso con el desarrollo y la implementación de las políticas de seguridad de la información, así como de su mejora continua, mediante:

- La autorización para que se implementen, actualicen y/o eliminen las políticas de seguridad de la información en Anditel S.A.S.
- Comunicar la importancia de lograr los objetivos de seguridad de la política de seguridad de la información.

3.2 Cumplimiento y manejo de violaciones a las Políticas

Las políticas de seguridad de la información son de obligatorio cumplimiento para cada uno de los trabajadores, contratistas y asesores externos de Anditel S.A.S, cada usuario debe entender su rol y asumir su responsabilidad respecto a los riesgos en seguridad de la información y la protección de los activos de información. Cualquier incumplimiento de estas políticas que comprometa la integridad, confidencialidad y/o disponibilidad de la información puede constituir una falta disciplinaria de acuerdo a lo establecido en la Ley 1273 de 2009. Ley de Delitos Informáticos.

3.3. Administración de la Política y Procedimiento de Cambio

Las políticas de seguridad de la información se deben revisar cada año o en el evento de cambios estructurales que afecten a Anditel S.A.S, con el fin de asegurar que ésta cumpla con los cambios que pudiera presentar el mismo.

La fecha de vigencia será a partir de la aprobación y socialización del presente documento.

Ante la necesidad de una actualización de las políticas, se debe hacer una reunión con los jefes de área de Anditel S.A.S, para efectos de aprobación de los cambios en el presente documento y realizar una divulgación de los cambios realizados a todos los trabajadores, contratistas y asesores externos.

4. DEFINICIONES

Activo: En relación con la Seguridad de la Información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización.

Confidencialidad: Propiedad de la información de no estar a disposición o ser revelada a individuos, Instituciones, o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable para su uso cuando lo requiera una Institución autorizada.

Evento: Circunstancia inesperada o no deseada que se presenta y que indica una posible violación a la Seguridad de la Información y no compromete las operaciones de la organización ni amenaza la Seguridad de la Información.

Incidente de Seguridad de la Información: Circunstancia inesperada o no deseada que se presenta y que posee una probabilidad significativa de

comprometer las operaciones de la organización y amenazar la Seguridad de la Información.

Integridad: Propiedad de exactitud y completitud de la información.

Política: Declaración de alto nivel que describe la posición de la organización sobre un tema específico.

Privacidad: La capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos.

Procedimiento: Forma específica de llevar a cabo una actividad o un proceso.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la Información: La preservación de la confidencialidad, la integridad y la disponibilidad de la información.

TIC: Tecnologías de la Información y las Comunicaciones.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1 Política General de Seguridad de la Información

Anditel S.A.S, dentro del marco de su misión Institucional, reconoce la importancia de identificar y proteger sus activos de información, asegurando su disponibilidad, confidencialidad e integridad, comprometiéndose a establecer, implementar, mantener y mejorar continuamente la Seguridad de la Información enmarcado en el cumplimiento del ordenamiento legal y en concordancia con la misión, visión, objetivos estratégicos y valores de la Institución.

5.2 Principios de las Políticas de Seguridad de la Información

A continuación, se establecen los siguientes principios de seguridad que soportan la Información de Anditel S.A.S:

a) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los trabajadores y demás terceros relacionados con Anditel S.A.S.

b) Anditel S.A.S, protegerá la información generada, procesada o almacenada por los procesos de su operación, su infraestructura tecnológica y activa, del riesgo que se genera de los accesos otorgados a trabajadores, contratistas y asesores externos.

c) Anditel S.A.S, protegerá la información creada, procesada, transmitida o almacenada por sus procesos de operación, con el fin de minimizar impactos operacionales o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

d) Anditel S.A.S, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

e) Anditel S.A.S, controlará la gestión de sus procesos de operación garantizando la seguridad de los recursos tecnológicos y las redes de datos.

f) Anditel S.A.S, verificará el control de acceso a la información, sistemas y recursos de red.

g) Anditel S.A.S, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

h) Anditel S.A.S, garantizará a través de una adecuada gestión de los incidentes de seguridad de la información y las debilidades asociadas con los sistemas de información una mejora efectiva de la Seguridad de la Información.

i) Anditel S.A.S, garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

j) Anditel S.A.S, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

5.3 Políticas Específicas de Seguridad de la Información

5.3.1 Política para Dispositivos Móviles

El uso de dispositivos móviles, tales como computadores portátiles (notebooks y laptops), tabletas electrónicas, unidades de almacenamiento externo y teléfonos móviles que contengan información de Anditel S.A.S, y que a su vez se utilicen para el manejo de esta información, deben ser controlados y/o verificados de acuerdo al análisis de riesgo correspondiente, y mitigar el impacto a que se expone la información como su pérdida, alteración y divulgación no autorizada.

a. Normas:

1) Se debe contar con un inventario actualizado de dispositivos móviles utilizados para almacenar o transmitir información de Anditel S.A.S.

2) En los dispositivos móviles que exista información de Anditel S.A.S, se debe restringir la conexión a redes o servicios que no sean explícitamente autorizados por el personal de Seguridad informática de cada unidad.
3) En caso que el dispositivo móvil tenga fines de traslado de información debe contar con controles de cifrado de la información.
4) Si desde el dispositivo móvil se procesa información se debe contar con un software instalado y actualizado contra códigos maliciosos, firewall personal y para prevenir intrusos.
5) Estos dispositivos deben contar con uno o dos factores de autenticación como clave y huella digital.
6) Se deben generar recomendaciones del uso y cuidado de tipo físico cuando el dispositivo se encuentre fuera de las instalaciones de la Institución.
7) Si desde el equipo móvil se requiere conexión remota a los servicios e información de la red de Anditel S.A.S, se debe validar previamente que el dispositivo está libre de infección y cumple con los demás controles de seguridad activos y actualizados.
8) Se deben configurar los dispositivos móviles de tal manera que cualquier aplicación incluyendo los mecanismos de software de seguridad permanezcan actualizados sin que dependan de conexión directa de la infraestructura tecnológica de Anditel S.A.S.
9) Los dispositivos móviles institucionales deben tener activado la función de geolocalización (si aplica) o recuperación por GPS. Se debe contar con un mecanismo que permita localizar y recuperar sus datos.
10) Al realizar la disposición final o reasignación del dispositivo móvil a otra área con un propósito diferente para el cual estaba designado, se deberá realizar un borrado seguro de toda la información almacenada.

11) El acceso al computador portátil debe estar protegido por una contraseña de encendido la cual se define en la BIOS (Basic Input Output System) del equipo (Aplica para equipos no arrendados)
12) El computador portátil debe tener un mecanismo de anclaje con clave y/o llave que permita asegurarlo a otro elemento fijo de tal manera que no pueda ser hurtado del lugar conectado.
13) Los trabajadores que tengan asignados equipos móviles de comunicación y equipos portátiles, deben ser responsables de la reserva de la información almacenada en ellos, para lo cual deben aplicar los mecanismos de seguridad de este documento, que impidan la consulta de información por parte de personas no autorizadas.

5.3.2 Política de Teletrabajo

Anditel S.A.S, requiere accesos remotos en determinados casos en los cuales se debe proteger la información clasificada, por lo tanto, el acceso a la información fuera de la oficina puede ser permitida si se demuestra que la información requerida es necesaria para el cumplimiento de sus funciones, y que existe un control de acceso con autorización previa y controlada por Anditel S.A.S.

a. Normas:

1) El acceso remoto únicamente se podrá realizar desde los equipos institucionales que cumplan con los niveles de seguridad y sobre los cuales se pueda confirmar el cumplimiento de requerimientos de seguridad, antes

de permitir la conexión remota a los servicios o recursos de la infraestructura tecnológica.

2) Los accesos remotos a los sistemas de información de Anditel S.A.S, se deben realizar a través de los protocolos de acceso establecidos previamente.
3) Se debe incluir controles de seguridad física a los equipos desde los cuales se procesa información de Anditel S.A.S, lo anterior para evitar accesos no autorizados por personas ajenas.
4) Se deben realizar copias de respaldo de la información de acuerdo al procedimiento de copias de seguridad para asegurar la continuidad de las funciones realizadas.
5) Todo usuario que requiera conexión remota a los servicios o información de Anditel S.A.S, deberá ser previamente autorizado por quien tenga dentro de sus responsabilidades otorgar esta autorización.
6) La conexión remota a servicios o información de Anditel S.A.S, se deberá realizar a través de canales de comunicación seguros como redes privadas virtuales.
7) La administración remota de los servicios informáticos de Anditel S.A.S, desde equipos conectados desde redes comerciales no está permitida, salvo que se cuente con la autorización debidamente sustentada mediante documento escrito y con un mecanismo de control de acceso seguro autorizado.
8) En caso de pérdida, suplantación o robo de un equipo portátil o cualquier medio de almacenamiento durante el teletrabajo que contenga información relacionada de Anditel S.A.S, se deberá realizar inmediatamente el respectivo reporte y se deberá poner la denuncia ante la autoridad competente.

5.3.3 Política de Acceso Lógico y Físico

Anditel S.A.S, define un grupo de controles que deben hacer referencia a todas aquellas directrices mediante las cuales se determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos, lógicos o físicos.

a. Normas de acceso lógico:

1) Dependiendo del nivel de clasificación y criticidad de los activos de información a los cuales se va a brindar acceso se deben establecer mecanismos de autenticación de uno, dos o tres factores.
2) Cuando se solicite tener acceso a algún recurso o servicio informático de Anditel S.A.S se deberá realizar el correspondiente análisis de riesgo con la participación del responsable de la información y de los activos asociados, con el fin de determinar los privilegios a otorgar y definir los mecanismos necesarios para su protección.
3) Se deben establecer los requisitos para la autorización formal de las solicitudes, así como para la revisión periódica de los controles y el retiro de los derechos de acceso a los usuarios.
4) Se debe usar una única identificación de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones.
5) Se debe verificar que el nivel de acceso otorgado sea adecuado para los propósitos y limitado exclusivamente a la información que está autorizado a acceder, y no poner en riesgo la segregación de funciones.
6) Todos los trabajadores de Anditel S.A.S, deben conocer, leer y firmar una declaración escrita de los derechos de acceso otorgados en la cual se

indique que ellos conocen, entienden y aceptan cumplir los controles de acceso a los sistemas de información.

7) El acceso a los sistemas de información se debe retirar o bloquear máximo 36 horas después de ser notificado el retiro del funcionario de la Institución y máximo 24 horas si el funcionario es trasladado.
8) Todos los accesos no autorizados serán considerados como un incidente de seguridad de la información, de acuerdo a la gravedad se llevarán a cabo las cláusulas (disciplinarias, administrativas y penales), definidas previamente.
9) Los privilegios de administración de los equipos de cómputo (servidor, estación de trabajo, portátil, o equipo activo de red), deben ser asignados únicamente a los administradores del sistema designados en la sección de comunicaciones de la unidad correspondiente de Anditel S.A.S, en ningún caso se debe autorizar estos privilegios de acceso al usuario final del equipo.
10) Todos los trabajadores deben gestionar sus contraseñas, inicialmente se les suministrará de manera segura una contraseña temporal, la cual se debe forzar a cambiar inmediatamente realice el siguiente ingreso al sistema.
11) Las contraseñas predeterminadas o por defecto se deben cambiar inmediatamente después de la instalación de los sistemas o del software.
12) Si un usuario tiene acceso a diferentes sistemas de información, se deben emplear contraseñas diferentes, siempre y cuando esta no se encuentre asociada al Directorio activo de Anditel S.A.S.
13) Toda contraseña es personal e intransferible, y cada usuario es responsable de las acciones que se ejecuten con el usuario que se le ha asignado.
14) En caso de que exista sospecha o certeza de que alguna contraseña se ha comprometido, esta debe ser cambiada y documentada de manera inmediata.
15) La gestión de las contraseñas incluye construir contraseñas teniendo en cuenta los siguientes lineamientos de manera obligatoria:

- Deben estar compuestas mínimo de diez (10) caracteres que deben ser combinados (mayúsculas, minúsculas, números y caracteres especiales).
- No deben ser idénticas o similares a contraseñas que hayan usado previamente o que usen en otros sistemas de información.
- La contraseña tendrá una vigencia máxima de 30 días, finalizando este periodo el usuario deberá realizar el cambio correspondiente.
- No deben ser fáciles de inferir o adivinar.
- No deben ser susceptibles a ataques de diccionario, es decir, que no incluya palabras que podrían ser encontradas en un diccionario.

b. Normas de Acceso Físico:

1) La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas, alrededor de las instalaciones de Anditel S.A.S y de las instalaciones de procesamiento de información.
2) Para la selección de controles de las áreas protegidas se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre.
3) El cableado de energía eléctrica y comunicaciones que transportan datos o brinda apoyo a los servicios de información deben estar aislados y protegerse contra intercepción o daños.
4) Se debe garantizar la seguridad física del centro de datos incluyendo, entre otros, el sistema eléctrico, el sistema de protección contra incendios y el control de temperatura.

5) Todas las puertas que utilicen sistema de control de acceso, deben permanecer cerradas, y es responsabilidad de todos los trabajadores y terceros autorizados evitar que las puertas se dejen abiertas.
6) Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado en cada una de las unidades de Anditel S.A.S, mientras permanezcan dentro de sus instalaciones.
7) Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas seguras (Centros de Datos – secciones de sistemas de información y comunicaciones), de Anditel S.A.S.
8) Es responsabilidad de todos los trabajadores y terceros acatar las normas de seguridad y mecanismos de control de acceso a las instalaciones de las unidades de Anditel S.A.S.
9) En las áreas restringidas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:
    - No se deben consumir alimentos ni bebidas.
    - No se deben ingresar elementos inflamables.
    - No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.
    - No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
    - No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
    - No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

5.3.4 Política de Controles Criptográficos

Con el fin de proteger la confidencialidad e integridad de la información, Anditel S.A.S, deberá definir los controles y responsables del cifrado de la información, así como también de las claves de cifrado estas deberán ser utilizadas, protegidas y gestionadas a lo largo de su ciclo de vida únicamente por los responsables designados.

a. Normas:

1) La información digital clasificada como Restringido, Confidencial y Secreto se debe almacenar y transmitir bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad, no obstante, en caso de no poderse aplicar un mecanismo de cifrado seguro, el responsable del cifrado deberá asignar clave de apertura a los archivos digitales que contengan este tipo de información.
2) Se debe asegurar que todo sistema de información o aplicativo que requiera realizar transmisión de información clasificada como Restringido, Confidencial y Secreto, cuente con mecanismos de cifrado de datos.
3) Se debe verificar desarrollar y establecer mecanismos para el manejo y la administración de llaves de cifrado; y estándares para la aplicación de controles criptográficos.
4) Se deben implementar controles respecto de la administración de claves, recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y reemplazo de las claves de cifrado.

   Se deben utilizar los siguientes algoritmos de cifrado y tamaños de clave:

CIFRADO SIMÉTRICO	
ALGORITMO	**LONGITUD DE CLAVE**
AES	256 Bits

CIFRADO ASIMÉTRICO		
CASO DE USO	**ALGORITMO**	**LONGITUD DE CLAVE**
Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 - 4096 Bits
Para certificados de sitio seguro.	RSA	2048 - 4096 Bits
Para certificados de usuario (personas físicas o jurídicas).	RSA	2048 - 4096 Bits

5) Los algoritmos y longitudes de clave mencionados anteriormente a la fecha de la generación de esta política se consideran seguros. Se recomienda verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.
6) Todos los documentos electrónicos que requieran asegurar la integridad y autenticidad de la información deben incluir una firma digital o electrónica.

El área técnica debe asesorar al responsable de la información para realizar la firma digital o electrónica.

7) Al utilizar firmas y certificados digitales, se debe considerar la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.
8) Todas las llaves serán protegidas contra modificación y destrucción; y las llaves secretas o privadas serán protegidas contra copia o divulgación no autorizada.
9) Se proporcionará una protección adecuada a la infraestructura utilizada para generar, almacenar y archivar llaves, considerándola crítica o de alto riesgo.
10) Cuando las llaves son comprometidas o cuando un funcionario se desvincula de Anditel S.A.S, se deben revocar los certificados o firmas digitales.
11) Se debe registrar y auditar las actividades relacionadas a la administración de llaves.
12) A fin de reducir la probabilidad de compromiso, las llaves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por un lapso de tiempo definido, no mayor a 12 meses.
13) Cuando se utilice criptografía simétrica, se debe asegurar que la metodología para el envío de la llave sea segura y que está solo sea conocida por el emisor y el receptor.

5.3.5 Política para Recursos Humanos

Toda vinculación laboral realizada por Anditel S.A.S, se debe regir de acuerdo a los manuales, procedimientos, las leyes Colombianas. Adicionalmente, Anditel

S.A.S, proporcionará los recursos necesarios para la formación, capacitación y/o concienciación en seguridad de la información de los empleados, contratistas y terceros con acceso a información.

a. Normas:

1) Se debe establecer un plan de capacitación y formación en seguridad de la información, en cual se incluyan todos los aspectos de seguridad de la información como:
   1.1) Gestión de activos seguridad de la información
   1.2) Gestión de riesgos de seguridad de la información
   1.3) Gestión de incidentes de seguridad de la información
   1.4) Gestión de contraseñas seguras
   1.5) Buenas prácticas en seguridad de la información
   1.6) Cumplimiento de lineamientos de seguridad de la información
2) Las capacitaciones deben ir dirigidas a todo el personal activo de Anditel S.A.S, lo cual permitirá fortalecer el conocimiento y crear una cultura de seguridad de la información.
3) Se debe establecer un plan de concienciación anual con actividades lúdicas que permitan que los trabajadores tengan una educación constante en seguridad de la información a través de los diferentes medios de comunicación con pantallas de los equipos, carteleras digitales, correos electrónicos, entre otros.
4) Incluir los temas de seguridad de la información en los planes de inducción y reinducción de la empresa, es importante tener registros de las personas que recibieron la inducción.
5) La asistencia a las sesiones de capacitación y sensibilización en seguridad de la información son de carácter obligatorio.

6) Se debe realizar evaluación de conocimientos en seguridad de la información al personal capacitado y sensibilizado, es importante medir la efectividad de las actividades de cultura en seguridad de la información.
7) Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por las necesidades institucionales.
8) Los trabajadores son responsables por la custodia y las acciones que se realicen sobre los activos informáticos que le han asignado, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.
9) Se deben definir compromisos y obligaciones por parte del personal que es capacitado en temas de seguridad de la información.
10) No se debe dejar en las impresoras documentos expuestos que contengan información sensible, ya que se puede comprometer su confidencialidad.
11) Para la vinculación de personal a la empresa se deben realizar el diligenciamiento de los documentos requeridos por Anditel los cuales serán de carácter obligatorio sin excepción alguna.

5.3.6 Política de Respaldo de la Información

Anditel S.A.S, debe realizar copias de respaldo de la información dando prioridad a la clasificada con mayores niveles de importancia y criticidad.

a. Normas:

1) Los medios de copias de seguridad se deben almacenar en custodia externa, asegurando que tenga implementado mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.

2) Se deben realizar pruebas de restauración de la información, de acuerdo a un plan de restauración de copias de respaldo establecido, para asegurar que se puede depender de ellos para uso de emergencia en caso necesario.
3) Definir los tiempos de retención y de protección en instalaciones adecuadas que proveen la debida seguridad física y ambiental, permitiendo minimizar el impacto en las funciones de Anditel S.A.S, en caso de presentarse una falla o desastre y poder contar con la información necesaria en el momento oportuno para responder con los tiempos de restauración de los servicios.
4) Se debe contar con registros exactos y completos de las copias de respaldo.
5) Definir la frecuencia y tipo de copias de respaldo a realizar.
6) Las pruebas de restauración se deberían hacer en medios de prueba dedicados, no sobrescribiendo el medio original, para evitar que se cause un daño o pérdida de la información.
7) El personal encargado de realizar las copias de respaldo y pruebas de restauración deberá contar con las competencias e idoneidad, además de los estudios de credibilidad, confiabilidad y actualización.

5.3.7 Política de Transferencia de Información

Anditel S.A.S, debe implementar procedimientos y controles para el uso adecuado de las redes y medios de comunicación de la Institución, evitando que los sistemas de información sean vulnerados y dejar en riesgo la confidencialidad, integridad y disponibilidad de la información durante la transferencia de información entre trabajadores y terceros.

a. Normas:

1) Los responsables de la información a transferir deben asegurar que la clasificación de ésta se encuentre actualizada teniendo en cuenta las

propiedades de seguridad: confidencialidad, integridad y disponibilidad, con el fin de permitir el acceso únicamente a los autorizados.

2) Únicamente se entrega información a receptores autorizados quienes garanticen por escrito la reserva legal y protección de la información que se les vaya a suministrar.
3) Cuando proceda, la Unidad responsable de proporcionar respuesta legal a un requerimiento de información clasificada, deberá verificar previamente entre otros temas y sin limitarse a:

   3.1) La solicitud se ajuste a la normatividad aplicable vigente.

   3.2) La respuesta identifique el nivel de clasificación, correspondiente a la naturaleza del documento o la información que se ponga en conocimiento del receptor autorizado

   3.3) La respuesta debe reflejar adecuadamente la valoración de la información, el uso de términos condicionales y dubitativos, que garantice entre otros la reserva, el debido proceso, el buen nombre y el derecho a la intimidad.

   3.4) La respuesta cumpla con los protocolos de seguridad, acceso y reserva.

   3.5) Con el fin de asegurar la trazabilidad de la respuesta esta debe quedar debidamente registrada.
4) Los emisores deben verificar el nombre de los destinatarios previo al envío de los correos electrónicos que contengan datos clasificados como confidenciales. Esto permite reducir al máximo el riesgo de fuga de información o transferencia de información clasificada a destinatarios no autorizados.
5) Se prohíbe en el correo electrónico institucional el envío de archivos que contengan extensiones ejecutables (exe, bat, etc).
6) Todo empleado y tercero debe firmar un acuerdo de confidencialidad, el cual debe contener un compromiso de no divulgación de la información

clasificada a la que tenga acceso como parte del desarrollo de las funciones.

7) El acuerdo de confidencialidad debe indicar la vigencia del mismo, el cual debe mantenerse por la vigencia que considere Anditel S.A.S, luego de terminada la vinculación con la empresa.

5.3.8 Política de Desarrollo Seguro

Anditel S.A.S, definirá un conjunto de lineamientos para garantizar la seguridad de la información durante la adquisición, desarrollo y mantenimiento de los sistemas de información.

a. Normas:

1) Se deben identificar y acordar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software, y se deben justificar, acordar y documentar. Estos requisitos se deben aplicar en el desarrollo de nuevos sistemas de información o en las mejoras a los sistemas de información existentes en la empresa.
2) Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.
3) El cambio de versión de las aplicaciones implementadas en el ambiente de producción se debe hacer de acuerdo a lo definido en el procedimiento de Gestión de Cambios; además, debe contar con controles de seguridad, para esto se debe hacer una copia de respaldo en caso que se deba realizar rollback o marcha atrás, para mantener la disponibilidad e integridad de los datos y de los sistemas de información.
4) Se deben realizar pruebas de seguridad en un ambiente controlado con el fin de identificar vulnerabilidades, las cuales deben ser resueltas antes del paso a producción.
5) Los ambientes de desarrollo, pruebas y producción, deben estar separados.

6) El paso de software de un ambiente a otro debe ser controlado y gestionado de acuerdo a lo definido en el procedimiento de Control de Cambios.
7) Los usuarios deben utilizar perfiles diferentes en el ambiente de desarrollo, pruebas y producción; además, asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente.
8) El ambiente de prueba debe simular el ambiente de producción.
9) En caso de requerirse hacer copia de la información del ambiente de producción al ambiente de pruebas, se podrá realizar únicamente si la información se encuentra enmascarada u ofuscada, con el fin de que no se llegue a comprometer.
10) El desarrollo de contratos de mantenimiento deberá contar con la asignación de un supervisor permanente, encargado de controlar que se cumplan los estándares de seguridad tanto en la parte física como lógica de los sistemas. Ningún mantenimiento podrá ser realizado por personal que no tenga los respectivos estudios de Credibilidad y Confiabilidad, certificados por Anditel.
11) Se debe dar cumplimiento a lo establecido en el "Procedimiento Gestión de Cambio".
12) Los sistemas de información y aplicaciones están sujetas a evaluaciones de seguridad basadas en los siguientes criterios:

    12.1) El paso a producción de una nueva aplicación estará sujeto a una evaluación de seguridad (análisis de vulnerabilidades y ethical hacking) completa previa a la aprobación de la documentación de control de cambios y entrada en ambiente de producción.
    12.2) Una aplicación web estará sujeta a una evaluación completa después de la cual, las vulnerabilidades encontradas serán remediadas de acuerdo a los requerimientos de la política de seguridad.

12.3) Las versiones nuevas y la liberación de parches estarán sujetas a un nivel de evaluación apropiado basado en el riesgo de los cambios en la funcionalidad de cada aplicación.

12.4) Todas las aplicaciones web que se publiquen a nivel interno o en internet deben accederse por medio de un nombre. No se permitirá la publicación de una aplicación web utilizando una dirección IP interna o externa.

12.5) La URL de ingreso a las aplicaciones web no debe incluir puertos, estos deben enmascararse en el servidor web.

12.6) La actualización del sistema operativo e instalación de parches estará sujeta a una evaluación por parte de los desarrolladores o el proveedor de la aplicación y los administradores de la plataforma tecnológica de Anditel S.A.S.

12.7) Todas las aplicaciones o sistemas de información que requieran el acceso a una base de datos, debe garantizar el acceso mediante el principio de menor privilegio. Esto significa que el usuario a través del cual se accede a la base de datos debe tener los permisos mínimos necesarios para que la aplicación o sistema de información funcione correctamente.

5.3.9 Política para Relaciones con Asesores Externos y Contratistas

Anditel S.A.S, debe identificar requisitos de seguridad para proteger la información, e incluirlos dentro de los acuerdos con proveedores, por medio de un análisis que permita identificar los riesgos de seguridad de la información asociados para implementar planes de acción dependiendo del tipo de actividad con asesor externo y contratista.

a. Normas:

1) Se debe tener en cuenta la documentación relacionada con los servicios, infraestructura de TI, sistemas de información y activos a los cuales tendrá acceso los asesores externos y contratistas, esto deberá ser controlado teniendo en cuenta los permisos de acuerdo al trabajo a realizar y los acuerdos firmados, los cuales deben tener requisitos mínimos de seguridad, que se deben hacer cumplir haciendo seguimiento por medio de mecanismos establecidos.
2) Anditel S.A.S, debe incluir dentro de los acuerdos a firmar con el asesor externo y contratista, todos los controles de seguridad aplicables.
3) Cuando exista la necesidad de otorgar acceso de terceras partes a los activos de información de Anditel S.A.S, deberá realizarse siempre con la participación del responsable de la información, además de realizar una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros, los siguientes aspectos:
   3.1) El tipo de acceso requerido (físico, lógico y a qué recurso).
   3.2) Los motivos para los cuales solicita el acceso.
   3.3) El valor de la información.
   3.4) Los controles empleados por el proveedor.

4) En ningún caso se otorgará acceso a terceros a la información de Anditel S.A.S, a las instalaciones de procesamiento u áreas restringidas, hasta tanto se hayan implementado los controles apropiados y se haya realizado el correspondiente estudio de credibilidad y confiabilidad y firmado un acuerdo que definan las condiciones para la conexión o el acceso.
5) El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al responsable de dicho activo. Éste junto con los encargados

de la infraestructura tecnológica, aprobará y autorizará el acceso y uso de la información.

6) Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y ambientes de computadores, contemplarán como mínimo los siguientes aspectos:
   - 6.1) Forma en los que se cumplirán los requisitos legales aplicables.
   - 6.2) Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
   - 6.3) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
   - 6.4) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.
   - 6.5) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
   - 6.6) Niveles de seguridad física que se asignará al equipamiento tercerizado.
   - 6.7) Derecho a la auditoría por parte de Anditel S.A.S.
7) Todos los trabajadores y terceros deben firmar la cláusula y acuerdo de confidencialidad que deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y a los recursos a personas o Instituciones externas.
8) Se deben formalizar los niveles de acuerdo de servicio y los acuerdos de intercambio de información con cada proveedor dentro del contrato realizado, de acuerdo a los lineamientos establecidos por Anditel S.A.S.

9) Los encargados de la infraestructura tecnológica deben verificar las condiciones de comunicación segura, cifrado y transmisión de información, desde y hacia los terceros.
10) Los supervisores de contratos con terceros deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.
11) El Oficial de seguridad de la información o quien haga sus veces debe validar y verificar en las actividades realizadas por proveedores el cumplimiento de los lineamientos de seguridad de la información. Se debe tener un registro de la actividad.
12) Anditel S.A.S, debe verificar que toda modificación o actualización a la infraestructura de tecnologías de la información por parte de terceros esté debidamente diligenciada y autorizada siguiendo los lineamientos establecidos en el procedimiento de Gestión de Cambios.
13) Anditel S.A.S, debe verificar que toda información a que tenga acceso el tercero con motivo de las actividades desarrolladas para la empresa, deberá tener unos niveles básicos de protección. El tercero deberá comprometerse a:
    13.1) Firmar compromiso de reserva sobre la información de Anditel S.A.S a la que tenga acceso.
    13.2) Tomar medidas adecuadas (cifrado, encapsulado, entre otras.), para mantener la confidencialidad de la información que sea transmitida o resida en sus computadores o dispositivos que contengan información de Anditel S.A.S.
    13.3) Una vez finalizado el contrato, el proveedor deberá borrar de manera segura de sus dispositivos móviles (formateo a bajo nivel), toda la información que pueda tener de Anditel S.A.S.

13.4) El contratista debe informar al Oficial de Seguridad de la Información o quien haga sus veces acerca de los datos de las personas nuevas y los sistemas y carpetas de red a las que requieren acceso. Además, de informar al supervisor del contrato, acerca del personal que se retira para deshabilitar los accesos.

5.3.10 Política de Gestión de Activos

Anditel S.A.S, debe identificar todos los activos de información y mantener un inventario actualizado, exacto, consistente y documentado con todos los aspectos relevantes de cada uno, clasificándolos teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información, para identificar su valor y criticidad, además, cada activo debe tener un responsable que garantice los niveles de seguridad que correspondan según sea el caso.

a. Normas:

1) Los empleados y contratistas al servicio de Anditel S.A.S, se deben comprometer a identificar, priorizar, clasificar, etiquetar, disponer, devolver y gestionar los activos de información que se encuentren para su uso y bajo su responsabilidad.
2) Todos los activos de información deben tener asignado un custodio que tiene la responsabilidad de mantener los controles de seguridad adecuados para su protección.
3) Los responsables de la información son los encargados de identificar y clasificar la información, de acuerdo con el grado de sensibilidad y criticidad, además son los encargados de documentar y actualizar la clasificación efectuada y definir las funciones que deberán tener permisos de acceso a la información.

4) La información de Anditel S.A.S, debe enmarcarse dentro de los niveles de clasificación de seguridad de la información, los cuales gozan de reserva legal:

4.1) Secreto: Es el nivel de clasificación que se debe dar a todos los documentos que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior de la empresa.

4.2) Confidencial: Es el nivel de clasificación que se debe dar a todos los documentos que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades.

5) Los documentos de Anditel S.A.S que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.

6) Los activos de información deben tener un uso aceptable siguiendo las siguientes indicaciones definidas, así:

6.1) Protección de la confidencialidad, integridad y disponibilidad:

6.1.1 De acuerdo con la clasificación del activo frente a la confidencialidad, integridad y disponibilidad, el empleado o contratista debe verificar que el acceso es coherente con su rol; en caso contrario debe abstenerse de hacerlo e informar del hecho a su Jefe Inmediato y al encargado de la Seguridad de la Información para que se tomen las medidas pertinentes.

6.1.2) Todos los empleados y contratistas están obligados a reportar accesos o modificaciones no autorizados o uso indebido de un activo.

6.2) Uso de la información digital y física:

6.2.1) Los responsables de los activos de información deben asegurar que el acceso a éstos se realice dependiendo su nivel de clasificación.

6.2.2) Los responsables de los activos de información deben asegurar que éstos se encuentren actualizados cuando exista un cambio en el proceso en cuanto a su medio de almacenamiento, ubicación, responsable y custodio.

6.3) Correo electrónico:

6.3.1) No es permitido utilizar cuentas personales o comerciales para transmitir cualquier tipo de activo de información de Anditel S.A.S.

6.3.2) La cuenta de correo electrónico empresarial asignada a un empleado o contratista, es para uso exclusivo de las actividades de sus funciones y es su responsabilidad velar por la seguridad del acceso.

6.4) Recursos compartidos:

6.4.1) La Dirección de Protección de Datos y Archivos establecerá los protocolos para la creación, uso y control de los recursos

compartidos que se requieran, a su vez brindará los permisos de lectura y escritura y las medidas de protección necesarias.

5.3.11 Política de Gestión de Incidentes de Seguridad de la Información

Anditel S.A.S, establece responsabilidades, controles y un procedimiento de gestión de incidentes de seguridad de la información que permitirá asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

a. Normas:

1) Los empleados y contratistas deberán reportar al Oficial de Seguridad de la Información o quien haga sus veces el evento o incidente de seguridad de la información una vez se identifique cualquier situación que ponga en riesgo la confidencialidad, integridad o disponibilidad de la misma. En caso de ser necesario el Oficial reportará siguiendo el protocolo y conducto regular dependiendo la criticidad del evento presentado.
2) Se debe reportar a la unidad designada por Anditel S.A.S, los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y documentar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.
3) Los responsables de los activos de información, trabajadores y terceros deben reportar los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
4) Se debe documentar todo el procedimiento de la gestión de incidentes de seguridad de la información.
5) Todo evento de seguridad de la información que se identifique por medio del monitoreo y revisión de los registros logs y que ponga en riesgo la

confidencialidad, integridad y disponibilidad de la infraestructura tecnológica deberá ser reportado.

5.3.12 Política para Organización de la Seguridad de la Información

Es importante tener claridad que los responsables de la Seguridad de la Información son todos los empleados, contratistas y terceros con acceso a la información de Anditel S.A.S.

Para velar por el cumplimento de los lineamientos de seguridad de la información, las unidades de Anditel S.A.S definirán un Comité de Seguridad de la Información como responsable de la revisión y aprobación de los documentos relacionados con el Sistema de Seguridad de la Información.

a. Normas:

1) Los individuos nombrados en los cargos de seguridad de la información deben contar con las competencias académicas requeridas.

5.3.13 Política de No Repudio

Anditel S.A.S definirá los controles requeridos para garantizar el No repudio de la Información a través de la trazabilidad, retención, auditoría y el intercambio electrónico de información gestionada por los empleados, contratistas o terceros.

a. Normas:

1) Para los procesos que se requieran se deben implementar mecanismos de seguridad en los que no exista la posibilidad de desafiar la validez de una acción por parte de quien la generó.

2) Algunos mecanismos a implementar deberán ser certificados o contar con un tercero en que todos confíen y que permita avalar la integridad y el origen de los datos.
3) Se deben contar con registros y herramientas que permita hacer trazabilidad de las acciones de creación, origen, recepción, entrega de información y otros, que servirán de evidencia para poder garantizar el no repudio.
4) Estos registros se deben proteger contra pérdida o modificación de tal manera que se garantice su disponibilidad e integridad.
5) Los servicios de intercambio electrónico de información deben incorporar mecanismos que sean garantía de no repudio.

5.3.14 Política de Privacidad y Confidencialidad

Anditel S.A.S adoptará una Política de Tratamiento y Protección de Datos Personales que deben ser aplicados, conforme a la Ley 1581 de 2012, Ley de Protección de Datos Personales.

a. Normas:

1) Todo empleado y tercero vinculado a Anditel S.A.S, deberá realizar los estudios de Credibilidad y Confiabilidad previo a la suscripción del contrato de vinculación y cada vez que lo requiera la empresa.
2) El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente, Ley 1581 de 2012, Ley de Protección de Datos Personales.

5.3.15 Política de Integridad

La política de Integridad se refiere al manejo integral de la información tanto interna como externa, conocida o administrada por empleados y terceros relacionados con Anditel S.A.S.

a. Normas:
   1) Toda información verbal, física o electrónica debe ser procesada y entregada exclusivamente a las personas autorizadas a través de los medios autorizados sin modificaciones ni alteraciones.
   2) En el caso de vinculación contractual, el compromiso de administración y manejo íntegro e integral de la información interna y externa debe hacer parte de las cláusulas del respectivo contrato, bajo la denominación de cláusula de integridad de la información.
   3) La integridad de la información transmitida a través de canales de comunicación y que se clasifique como Restringida, Confidencial y Secreta, se garantizará mediante el uso de mecanismos descritos en la Política “Controles criptográficos”.

5.3.16 Política de Registro y Verificación

Esta política de Registro y Verificación define lo pertinente a las verificaciones que se realizan a los procesos del alcance del Sistema de Gestión de Seguridad de la Información e indica temas del registro y conservación de las evidencias de las actividades y acciones que afectan los activos de información.

a. Normas:
   1) El Área de Evaluación y Seguimiento debe planificar, establecer, implementar y mantener un programa de verificación interna que incluya la frecuencia, los

métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes.

2) Las acciones correctivas deben ser apropiadas a causa de las no conformidades encontradas.
3) El Área de Evaluación y Seguimiento debe asegurar que los resultados de las verificaciones se informen al siguiente nivel, y que se conserva información documentada como evidencia de la implementación del programa de verificación.
4) El Área de Evaluación y Seguimiento debe definir un plan de verificación y un equipo que lo ejecute, el cual debe cumplir con las capacidades, habilidades y conocimientos para su ejecución.
5) Los programas de verificación deben tener en cuenta la importancia de los procesos involucrados y los resultados de las verificaciones previas.
6) Los registros de verificación deben incluir toda la información de registro y monitoreo de eventos de seguridad, estos registros se deben almacenar por lo menos por un periodo de tres años.
7) Las verificaciones se deben realizar acorde a la normatividad y requerimientos legales aplicables a la naturaleza de Anditel S.A.S.
8) Se deben desarrollar planes de verificación interna para evaluar los niveles de aplicabilidad de la seguridad de la información en todos sus ámbitos, tanto digitales como físicos.
9) Se debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de los lineamientos y procedimientos del SGSI; así como recomendar lo pertinente sobre las deficiencias detectadas.
10) Cuando ocurra una no conformidad como resultado de la verificación, Anditel S.A.S debe reaccionar de manera oportuna y tomar las acciones para controlarla y corregirla.

5.3.17 Política de Ubicación y protección de los equipos

El Data Center debe estar ubicado de forma tal que personas no autorizadas no puedan visualizar los trabajos técnicos que se realizan al interior del mismo.

El acceso físico a los Datacenter debe ser controlado por la sección de Sistemas de Información y Comunicaciones a todo nivel.

Se debe realizar seguimiento a las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) que pueden llegar a afectar adversamente el Datacenter y se deben documentar los seguimientos.

5.3.18 Política de Equipo desatendido, escritorio limpio y pantalla limpia

Los empleados y contratistas de Anditel S.A.S, deberán conservar su escritorio libre de información propia de la empresa que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo deben bloquear el equipo y tener en cuenta las siguientes normas:

a. Normas:
   1) Al imprimir documentos con niveles de clasificación, éstos deben ser retirados de la impresora inmediatamente.
   2) Los computadores cargarán por defecto el fondo de pantalla, este no podrá ser modificado y deberá permanecer activo.
   3) Los empleados de Anditel S.A.S, deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo.
   4) Los empleados son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia.

5) Se prohíbe el almacenamiento de información personal en los computadores empresariales.
6) El escritorio lógico debe estar libre de información clasificada.
7) Toda la documentación física (impresa), debe estar guardada en los cajones bajo llave en los escritorios de trabajo.

5.3.19 Política de Registro y Supervisión

1) Registro de Eventos

1.1) Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de Anditel S.A.S, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

2) Protección de la Información de Registro.

2.1) El área de IT con el fin de proteger la información de registro de modificación no autorizada por parte de usuarios no autorizados, administradores u operadores de los sistemas de información implementará mecanismos de copiado de logs en “tiempo real” a un sistema por fuera del control de administradores y operadores de los sistemas.

3) Sincronización de Relojes.

3.1) Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes

equipos de cómputo, servidores y sistemas de información utilizados por Anditel S.A.S, deben estar sincronizados.

5.3.20 Política de Seguridad en las Comunicaciones

1) Gestión de la Seguridad en las Redes.

1.1) El área de IT, debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de las redes, los servicios en red y la información por allí transmitida.

1.2) El área de IT, define e implementa los mecanismos de separación de las redes de la empresa, con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio, dominio de servidor), por dependencias (por ejemplo, área de talento humano, área de servicios administrativos, área de gestión financiera, área de tecnología e información) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples dependencias).

1.3) El área de IT, debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes.

1.4) El acceso remoto a las redes de la empresa se controla mediante conexiones VPN.

6. REFERENCIAS

- ✔ Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos, 2013-12-11, ICONTEC Internacional.
- ✔ Norma Técnica Colombiana NTC-ISO-IEC 27002:2013, Guía de Implementación Sistemas de Gestión de la Seguridad de la Información, 2013-12-11, ICONTEC Internacional.
- ✔ ISO/IEC 27000:2016, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, 2016-02-15, International Organization for Standardization.

Santiago Jaramillo Villegas
Presidente
Bogotá D.C., 15 de mayo de 2024

CONTROL DE DOCUMENTOS

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: Hembert Iregui	Nombre: Carlos Elorza	Nombre: Ingrid Gaitán
Cargo: Gerente Sistemas de Información	Cargo: Gerente de Proyectos	Cargo: Directora Administrativa y Financiera
Fecha: 15-05-2024	Fecha: 15-05-2024	Fecha: 15-05-2024

CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIO REALIZADO	RESPONSABLE
15-05-2024	1	Emisión del documento	Ingrid Gaitán
18-09-2024	2	Manejo de áreas/departamentos en lugar de oficinas	Hembert Iregui