RESOLUCIÓN NÚMERO 000683 DEL 17 DIC 2020

"Por la cual se adopta la política de seguridad y privacidad de información"

EL DIRECTOR GENERAL DE LA UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

En uso de las facultades legales y en especial la conferida en el articulo 12 del Decreto 4150 de 2011, Decreto 1293 de 2020 y

CONSIDERANDO

Que, el articulo 12 del Decreto 4150 de 2011 faculta al Director General para implementar, mantener y mejorar el Sistema de Gestión Institucional de la Unidad de Servicios Penitenciarios y Carelarios – USPEC.

Que, el capitulo I sección 2 articulo 2.2.9.1.1.3. del Decreto 1008 de 2018 incluye la seguridad de la Información entre los principios de la Política de Gobierno Digital, igualmente el artículo 2.2.9.1.2.1 define la seguridad de la información como habilitador transversal de la Política de Gobierno Digital que junto con los demás habilitadores permiten el desarrollo de los componentes y logros incluidos en dicha política.

Que, el CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital en la República de Colombia y busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socieconómicas en el entorno digital, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vz impulsará una mayor prosperidad económica del país.

Que el CONPES 3995 del 2020 establece la Política Nacional de Confianza y Seguridad Digital. , a través de los cuales se pretende establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Que, a través de la Resolución 001046 del 2018 se modifica la política de seguridad de información y es necesario derogar teniendo en cuenta los ajustes realizados a la plataforma estratégica de la USPEC, en tal sentido se cambia su nombre por Política general de seguridad y privacidad de información y se modifican los objetivos de seguridad, los roles y responsabilidades de seguridad de información.

Que, el Decreto 1499 de 2017, por el cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, adopta la actualización del Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su título 2, capitulo 1, artículo 2.2.22.3.2 como *"(...) un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".* Así mismo en su capítulo 2, artículo 2.2.22.2.1 se define *"Las Políticas de Gestión y Desempeño Institucional. Las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominan políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes(...) 12. Seguridad Digital".*

Que, en la implementación del Sistema de Gestión de Seguridad de la Información(en adelante SGSI), es preciso establecer el alcance, la Política de Seguridad de la Información, los objetivos y los roles y responsabilidades de Seguridad de la Información, así como las políticas adicionales del Sistema de Gestión de conformidad con la norma NTC-ISO-IEC 27001:2013 a través del presente acto administrativo.

Que en virtud de lo anterior;

RESUELVE:

CAPÍTULO 1
Generalidades de la política

ARTÍCULO 1. Objeto: La presente resolución tiene como objeto adoptar la Política de Seguridad y Privacidad de la Información en la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, así como definir los roles y responsabilidades y demás políticas propias frente a la implementación del Sistema de Gestión de Seguridad de Información.

ARTÍCULO 2. Política General de Seguridad y Privacidad de la Información. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información que se incorpora con la presente resolución y quedará así:

> "La UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS, a través de la implementación del Modelo de Seguridad y privacidad de Información – MSPI, enmarcado en el Sistema de Gestión de Seguridad de Información y consciente de la importancia que representa la seguridad de la información y considerándola como un factor fundamental para la gestión y operación del suministro de bienes y prestación de servicios, la infraestructura y el apoyo logístico y administrativo requeridos para el adecuado funcionamiento de los servicios penitenciarios y carcelarios a cargo del INPEC, se compromete a preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de los riesgos, cumplimiento de los objetivos de seguridad de la información, de los requisitos legales y organizacionales, de las obligaciones contractuales, y de la asignación de los recursos necesarios para mejorar continuamente el Sistema de Gestión de Seguridad de la Información".

ARTÍCULO 3. Objetivos de Seguridad de la Información. Para la implementación de la presente política se establecen los siguientes objetivos generales:

- Gestionar los riesgos de seguridad digital, con el fin de implementar controles que permitan proteger los activos de información que soportan la estrategia y operación de la Entidad.
- Capacitar y sensibilizar al personal de la USPEC en temas relacionados con seguridad de la información.
- Gestionar los incidentes de seguridad de la información generando, documentando y aplicando las lecciones aprendidas, con el fin de reducir la probabilidad o el impacto de incidentes futuros.
- Implementar acciones preventivas, correctivas y de mejora generadas como resultado de las auditorías internas y/o externas con el fin de apoyar la mejora continua del sistema de gestión de seguridad de información.

ARTÍCULO 4. Alcance de la política. La Política de Seguridad y Privacidad de la Información aplica a todos los procesos institucionales incluidos los estratégicos, misionales, de apoyo, evaluación y control, así como a todos los funcionarios, contratistas, proveedores y todos los terceros que en ejercicio de sus funciones y las propias de la Entidad tengan acceso o gestionen la información institucional, así como los Entes de Control u otras Entidades que accedan a la misma. La implementación del SGSI en la USPEC se realizará acorde a los lineamientos contenidos en el Modelo de Seguridad y Privacidad de la Información y los requisitos de la Norma ISO 27001 en su versión vigente.

CAPÍTULO 2
Roles y responsabilidades de seguridad de información

ARTÍCULO 5. A continuación se describen tanto los roles como las responsabilidades que se deben asumir al interior de la USPEC para la implementación y mejora continua del Sistema de Gestión de Seguridad de Información.

A. **Dirección General:** Responsable por el direccionamiento estratégico e impulso del Sistema de Gestión de Seguridad de Información. Establece su compromiso, mediante la asignación de recursos, responsabilidades y revisiones internas. Como parte de la gestión de la Dirección General para seguridad de la información deberá establecer los lineamientos para:

a. La asignación de roles y responsabilidades de seguridad de la información.
b. La definición de la política general, objetivos, políticas específicas de seguridad de información y que estos sean compatibles con la planeación estratégica de la Entidad.
c. La asignación de los recursos necesarios para el mantenimiento del SGSI.
d. La revisión del Sistema de Gestión de Seguridad de la Información de la Entidad semestralmente, para asegurarse de su conveniencia, adecuación y eficacia continua. Esta revisión se realizará conforme a la información remitida por el Oficial de Seguridad de Información.
e. La dirección y apoyo a los funcionarios y/o contratistas para contribuir a la eficacia, mejora continua y logro de los resultados previstos dentro del SGSI.
f. El apoyo a otros roles pertinentes de la dirección, para demostrar su liderazgo dentro del SGSI aplicado a sus áreas de responsabilidad.

B. **Oficial de Seguridad de Información:**

a. Liderar el mantenimiento del SGSI velando por el cumplimiento de las políticas de seguridad establecidas en la Entidad, los objetivos y planes del SGSI de forma que se encuentren alineados con los requerimientos de normas y leyes vigentes.
b. Realizar actualizaciones de las metodologías y políticas de Seguridad de la Información.
c. Socializar con funcionarios y contratistas de la Entidad los lineamientos del SGSI.
d. Acompañar a los procesos en la actualización de activos de información, riesgos de seguridad digital y la definición de los planes de tratamiento.
e. Realizar seguimiento a la ejecución de todos los planes que forman parte del SGSI.
f. Definir métodos que permitan identificar las vulnerabilidades en la infraestructura tecnológica de la Entidad.
g. Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a Seguridad de la Información.
h. Asegurar la adecuada gestión de los incidentes de seguridad de la información en la USPEC.
i. Definir las mediciones requeridas para verificar el desempeño del SGSI.
j. Mantener actualizada la declaración de aplicabilidad definiendo la justificación de las inclusiones de los controles implementados o justificación de aquellos que se pueden considerar como exclusión en el SGSI. Esta actualización se llevará a cabo de forma anual, posterior a la actualización del mapa de riesgos de seguridad digital con el fin de incluir los controles implementados en el tratamiento de riesgos.
k. Coordinar las actividades y reuniones del equipo operativo de seguridad de información.
l. Informar semestralmente a la Alta Dirección sobre el desempeño del sistema de gestión de seguridad de información a través del informe de revisión por la Dirección.
m. Revisar que el sistema se encuentre conforme con los requisitos de la Norma ISO 27001:2013 y el MSPI y mantener actualizada la herramienta de diagnóstico del MSPI.
n. Adelantar las gestiones pertinentes para llevar a cabo ejercicios de auditoria al SGSI.

C. **Responsables de proceso:** Director, Jefe de Oficina o Líder encargado de proceso, quienes deberán asumir y ejecutar las siguientes responsabilidades:

a. Asignar los integrantes para la conformación del Equipo Operativo SGSI del(los) proceso(s) a cargo.
b. Difundir las políticas, procedimientos y demás documentos relacionados con el SGSI en su respectivo proceso.
c. Mantener actualizado el inventario de activos de información de su proceso de acuerdo a la metodología establecida por la entidad y velar por la ejecución de los controles requeridos para asegurar la confidencialidad, integridad y disponibilidad de los mismos.
d. Liderar la gestión para llevar a cabo la actualización de riesgos de seguridad digital al interior de su proceso según la metodología establecida por la Entidad.

e. Definir el plan de tratamiento de riesgos de seguridad digital, aprobarlo y velar por su cumplimiento.
f. Gestionar los recursos necesarios para la mitigación de riesgos de seguridad digital a través de la implementación de controles definidos en los planes de tratamiento de riesgos.
g. Asegurar la disponibilidad de los Funcionarios y Contratistas de su proceso para la asistencia a actividades de formación y sensibilización que permitan el fortalecimiento de la cultura en Seguridad de la Información.
h. Gestionar la definición y ejecución de planes de mejoramiento requeridos para apoyar la mejora continua del SGSI.
i. Aprobar los planes, procedimientos y demás documentación necesaria para el mantenimiento del SGSI acorde a su proceso.
j. Las demás responsabilidades asignadas en los procedimientos, instructivos, guías y demás documentación del SGSI.

D. **Equipo Operativo de Seguridad de Información:** Este equipo está integrado por delegados de cada proceso institucional y dentro de sus responsabilidades se encuentran las siguientes:

a. Apoyar la actualización del inventario de activos de su proceso teniendo en cuenta la metodología definida por la Entidad.
b. Apoyar la actualización de riesgos de seguridad digital y la formulación de su respectivo plan de tratamiento de riesgos.
c. Apoyar a los responsables de la implementación del plan de tratamiento de riesgos de su proceso en la ejecución de controles según lo requerido.
d. Realizar seguimiento al interior de su proceso al plan de tratamiento de riesgos definido para mitigar los riesgos de seguridad digital y los demás planes relacionados con el cumplimento de lineamientos de seguridad de información.
e. Participar en las actividades de formación y sensibilización organizadas por el Sistema de Gestión de Seguridad de Información.
f. Apoyar la definición de los planes de mejoramiento requeridos para evidenciar la mejora continua del SGSI.
g. Difundir al interior de su proceso las políticas, procedimientos y demás documentos que hacen parte del SGSI.

El Equipo Operativo de Seguridad de la Información se reunirá de acuerdo con las necesidades del Sistema de Gestión de Seguridad de Información y por solicitud del Oficial de Seguridad de Información.

E. **Funcionarios y Contratistas:**

a. Apoyar el mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, de acuerdo con las políticas, metodologías, procesos, procedimientos y los demás lineamientos establecidos para tal fin.
b. Aceptar y dar cumplimiento a las políticas y demás lineamientos de seguridad de la información
c. Ejecutar los controles que al interior de su proceso y la Entidad se requieran para la adecuada protección de los activos que se encuentran bajo su gestión.
d. Reportar eventos y/o incidentes de seguridad de la información de acuerdo al procedimiento establecido por la Entidad.
e. Clasificar, etiquetar y manejar la información de acuerdo con los procedimientos y políticas establecidas por la Entidad.
f. Participar activamente en las actividades de sensibilización, formación y toma de conciencia desarrolladas por la Entidad.

CAPÍTULO 3
POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE INFORMACIÓN

ARTÍCULO 6. Política de seguridad de los recursos humanos. El Grupo de Administración de Personal a cargo de la Dirección Administrativa y Financiera establecerá los lineamientos de seguridad que se deben cumplir durante los procesos de vinculación de personal, la ejecución del trabajo y en la terminación del vínculo laboral o cuando se presenten cambios de roles o funciones. Así mismo, el Grupo de Talento Humano será el responsable de llevar a cabo el proceso de inducción y reinducción en seguridad de información para el personal adscrito a la Entidad.

Parágrafo: Con el mismo propósito, la Dirección de Gestión Contractual establecerá en las minutas de contrato los lineamientos de seguridad de información a través de las cláusulas y obligaciones contractuales las cuales serán divulgadas y verificadas para su cumplimiento por cada supervisor de contrato.

ARTÍCULO 7. Política para dispositivos móviles. El Grupo Administrativo a cargo de la Dirección Administrativa y Financiera y la Oficina de Tecnología establecen los lineamientos y buenas prácticas para proteger la información de la USPEC almacenada y /o gestionada a través de dispositivos móviles.

ARTÍCULO 8. Política de gestión de activos. La Oficina Asesora Jurídica, el Grupo de Gestión Documental y la Oficina de Tecnología mantendrán actualizados los lineamientos para la adecuada valoración, clasificación y gestión de activos de la USPEC a través del Manual de Clasificación de Activos, con el fin de suministrar la protección adecuada de activos de la Entidad de acuerdo con la legislación y estándares vigentes.

ARTÍCULO 9. Política de control de acceso. A través de esta política se definen las responsabilidades de seguridad que los usuarios deben aplicar para minimizar riesgos de accesos no autorizados a servicios tecnológicos, sistemas de información o aplicaciones administradas tanto por la Oficina de Tecnología como por las demás dependencias responsables. En el caso de los servicios o sistemas de información externos a los cuales los funcionarios y contratistas deben acceder como cumplimiento de sus funciones u obligaciones contractuales, se deberán tener en cuenta los lineamientos de la Entidad responsable, pero así mismo la dependencia de la USPEC a cargo de su registro deberá mantener un registro de usuarios habilitados y deshabilitados del mismo y asegurar las gestiones correspondientes para la actualización de usuarios cuando haya lugar.

ARTÍCULO 10. Política de seguridad física y del entorno. El Grupo Administrativo en cabeza de la Dirección Administrativa y Financiera debe establecer junto con las áreas responsables los lineamientos y controles de acceso físico para acceder a las zonas seguras de la Entidad, así como a las demás instalaciones de la USPEC, con el fin de permitir el acceso únicamente a personal autorizado. Adicionalmente a través de esta política se debe asignar la protección contra amenazas externas y ambientales, ubicación y protección de los equipos, retiro de los activos de las instalaciones y de la seguridad de los mismos fuera de las instalaciones.

Parágrafo: Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones de la USPEC deben estar debidamente identificados a través del carné asignado por la Entidad y portarlo siempre en un lugar visible. En el caso de los funcionarios y contratistas deben emplear la tarjeta de acceso para ingresar y salir del edificio. Estos documentos de identificación son de carácter personal e intransferible.

ARTÍCULO 11. Política sobre el uso de controles criptográficos. La Oficina de Tecnología establecerá las herramientas a través de las cuales se puede llevar a cabo la encriptación de información institucional de carácter reservado o clasificado con el fin de mantener sus criterios de confidencialidad previamente establecidos por la dependencia responsable de la información al momento de realizar transferencias de la misma.

Parágrafo: Las dependencias que requieran transferir información reservada o confidencialidad deberán informar a la Oficina de Tecnología con el fin de brindar orientación frente al proceso de encriptación.

ARTÍCULO 12. Política teletrabajo o trabajo remoto. Esta política define las condiciones, directrices, acuerdos y restricciones que deben implementarse en las diferentes modalidades de teletrabajo de la USPEC y el uso seguro de las herramientas tecnológicas suministradas para cumplir este propósito, las cuales se encuentran alineadas con la legislación colombiana vigente.

ARTÍCULO 13. Política de escritorio y pantalla limpios. Esta política establece los lineamientos para prevenir el acceso no autorizado, pérdida y/o daño de la información institucional, que se encuentra a cargo del personal que labora en la USPEC, almacenada en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral.

ARTÍCULO 14. Política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. Para el manejo de llaves criptográficas (token) en la Entidad, se deben aplicar las siguientes medidas:

1. El uso de estos dispositivos está asociado a nombre propio de cada usuario, por lo tanto, no deben ser usados por personal ajeno, con el fin de contribuir con la integridad de la información.
2. Las contraseñas o passwords que se usen como mecanismo de identificación adicional al token deben cumplir con los requisitos de contraseñas seguras establecidos por la Oficina de Tecnología.
3. Las contraseñas o passwords utilizadas con estos dispositivos no se deben compartir y se debe garantizar que estas no sean conocidas por otras personas o sean divulgadas.
4. Cuando estos dispositivos se averíen y/o deban ser reemplazados, se debe garantizar la destrucción segura de los antiguos dispositivos, con el fin de evitar que puedan ser usados de manera ilegal o fraudulenta.
5. Siempre guardar estos dispositivos en lugares seguros, resguardados y en lo posible monitoreados, para evitar que sean accedidos y/o usados sin autorización, incluso cuando no se encuentren en uso.
6. En caso de pérdida o robo, o uso no autorizado debe ser reportado como un evento de seguridad de información a través de los canales establecidos para tal fin por la Oficina de Tecnología. Lo anterior con el fin de gestionar la revocación de los certificados o llaves privadas de cifrado y así evitar que se vulneren los accesos, la información o datos sensibles que se puedan gestionar con estos dispositivos.
7. Las llaves de cifrado deben ser renovadas como mínimo 1 vez al año o en lo posible, se deben realizar acuerdos con los proveedores para que éstas sean actualizadas cada 6 meses.
8. Es indispensable que se usen siempre desde equipos propios de la USPEC, con el fin de asegurar que no sean vulnerados en equipos con malware o que se encuentren en riesgo de ser infectado con tales amenazas.

ARTÍCULO 15. Política de copias de respaldo. La Oficina de Tecnología define los lineamientos y directrices que deben seguirse al interior de la Entidad para la realización de respaldo de la información del correo institucional y el backup de la Entidad, para asegurar que pueda efectuarse una recuperación adecuada en el momento que se requiera. Adicionalmente el Grupo de Gestión Documental definirá en conjunto con las dependencias, los tiempos de retención de la información a cargo de cada una de ellas con el propósito de establecer los TIEMPOS de conservación.

ARTÍCULO 16. Política de transferencia de información. La Oficina de Tecnología establece los lineamientos para la transferencia de información institucional catalogada como reservada o confidencial. Los responsables del proceso son los encargados de autorizar las transferencias de la información sensible que tienen a su cargo y el receptor de la información es el responsable de aplicar los controles pertinentes de seguridad de información con el fin de mantener la confidencialidad e integridad de la misma.

ARTÍCULO 17. Política de desarrollo seguro. La Oficina de Tecnología establece los requerimientos de seguridad que se deben tener en cuenta durante el ciclo de vida del software, independientemente que se genere un proceso de adquisición, desarrollo o mantenimiento de un sistema de información. Así mismo el Oficial de Seguridad ejecutará pruebas de seguridad de información con el fin de validar si el sistema de información cumple con los parámetros establecidos para asegurar la confidencialidad, integridad y disponibilidad de la información.

Cualquier software que opere en la Unidad de Servicios Penitenciarios y Carcelarios deberá reportarse y entregarse a la Oficina de Tecnología cumpliendo con los lineamientos técnicos y estándar de desarrollo de software establecidos por la OTEC, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente de seguridad de información.

ARTÍCULO 18. Política de seguridad de la información para las relaciones con proveedores. La Dirección de Gestión Contractual establece a través de las minutas de contrato los lineamientos de seguridad de la información que deben implementarse con los terceros que cuenten con privilegios para acceder, procesar y almacenar información de la USPEC. Es responsabilidad del supervisor de contrato divulgar las políticas y demás lineamientos de seguridad de información a los proveedores que tiene a su cargo.

ARTÍCULO 19. Política de Gestión de Incidentes. La Oficina de Tecnología establecerá los lineamientos para la gestión de los incidentes de seguridad de información en la Entidad, así mismo se encargará de asignar el personal responsable para su tratamiento, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados. Todo el personal de la USPEC podrá reportar incidentes de seguridad a través de los canales establecidos para tal fin.

ARTÍCULO 19. Todas las políticas identificadas en este capítulo se deberán reglamentar de manera detallada en la Declaración de aplicabilidad y la documentación propia del Sistema de Gestión de Seguridad de Información.

ARTÍCULO 20. Actualización del alcance, política, objetivos, roles y responsabilidades de seguridad de la información. La Política de Seguridad y Privacidad de la Información se revisará anualmente, o antes si se presentan situaciones que puedan llegar a afectar la seguridad de la información en la Entidad. Esta gestión está a cargo del Oficial de Seguridad de Información o quien haga sus veces y será aprobada por el Director General de la USPEC.

ARTÍCULO 21. Incumplimiento de las políticas y lineamientos de seguridad de información. El incumplimiento de las políticas mencionadas en la presente resolución, así como la violación de los procedimientos o lineamientos establecidos en temas de seguridad de información y de las leyes, decretos y demás normas que soporten estas políticas, se establecerá como un incidente de seguridad de información y se gestionará de acuerdo con los lineamientos establecidos por la Oficina de Tecnología. Adicionalmente conllevará a en el caso de funcionarios a la notificación de la situación que se evidencia a su jefe inmediato y en caso requerido se procederá a iniciar el proceso disciplinario teniendo en cuenta lo establecido en el procedimiento A2PRO2 Procesos disciplinarios de la Entidad.

En el caso de contratistas se enviará notificación al interventor y/o supervisor del contrato y copia a la Dirección de Gestión Contractual para que de acuerdo con sus competencias generen las investigaciones a que haya lugar. En el caso de terceros, esto conlleva una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista y en caso de manipulación indebida podrá tener efectos penales, de igual manera se notificará a los interventores y/o supervisores de contrato.

ARTÍCULO 22. La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C. a los 17 DIC 2020

ANDRES ERNESTO DÍAZ HERNÁNDEZ
Director General de la Unidad de Servicios Penitenciarios y Carcelarios

Elaboró: Fernando Arturo Vargas Herrera - Técnico Operativo / Diana Paola Cárdenas Huertas - Profesional Universitario / Mayra Alexandra Agudelo Carvajal - Profesional Especializado
Revisó: Piedad Cecilia Montero Villegas Jefe Oficina de Tecnología
Control de Legalidad: Jorge Mauricio Salinas Gutiérrez – Coordinador Grupo de Acciones Constitucionales, Conceptos y Control de Legalidad
Ruta: No aplica.
Ubicación archivo físico: Carpeta seguridad de información