RESOLUCION No.304-2022
(08 de noviembre de 2022)

POR MEDIO DE LA CUAL SE ESTABLECE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL ESE.

El Gerente del Hospital Departamental San Rafael De Zarzal E.S.E., Valle del Cauca, en uso de las atribuciones legales y constitucionales, y demás normas concordantes y reglamentarias, y,

CONSIDERANDO

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información son derechos reservados por parte del Hospital Departamental San Rafael Zarzal E.S.E., por medio de la Estrategia de Gobierno en línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC.

RESUELVE:

CAPITULO I
DISPOSICIONES GENERALES

ARTICULO 1. OBJETO. El propósito es identificar políticas que lleven a cabo los acontecimientos generales que los empleados y el área de sistemas de información llevara a cabo en cuestión de copias de seguridad.

ARTICULO 2. AMBITO DE APLICACIÓN. La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por el comité de seguridad de sistemas de información.

ARTICULO 3. DEFINICIONES.

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

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

ARTICULO 4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El comité de seguridad de la información en dirección del HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, 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 defina en el alcance, sus funcionarios, terceros, aprendices, 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 SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- 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 los funcionarios, terceros, aprendices, practicantes y clientes de HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E Garantizar la continuidad del negocio frente a incidentes.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva. Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la "Guía de políticas específicas de seguridad y privacidad de la información" y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E:

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos 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.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E protegerá su información de las amenazas originadas por parte del personal.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E implementará control de acceso a la información, sistemas y recursos de red.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Política de Seguridad y Privacidad de la Información

El siguiente documento es un formato de política de Seguridad y Privacidad de la Información

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de _ HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información. HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E y la ciudadanía en general.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E:

HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos 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.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E protegerá su información de las amenazas originadas por parte del personal.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E implementará control de acceso a la información, sistemas y recursos de red.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

ARTICULO 5. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice por la página institucional.

Importancia de las políticas de seguridad de la información

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

1. **Desarrollo de las políticas**: En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

- **Justificación de la creación de política:** identificación de riesgos de seguridad para la continuidad del negocio.
- **Alcance:** Va dirigido a las áreas de servicio tanto asistenciales como financiera y sus sedes.
- **Roles y Responsabilidades:** Los jefes de área serán los responsables en la ayuda para la implementación, aplicación, seguimiento y autorizaciones de la política.

- **Revisión de la política:** La revisión de la política será evaluada por el comité de seguridad de la información.
- **Aprobación de la Política:** La aprobación de la política será el gerente de la institución.

2. Cumplimiento: Se implementarán las políticas de seguridad con el fin de cumplir con lo establecido por la institución.

3. Comunicación: Se distribuirá por los canales internos y la página web del Hospital Departamental San Rafael de Zarzal E.S.E.

4. Monitoreo: El comité de seguridad de la información se reunirá para monitorear que la política se lleve a cabo.

5. Mantenimiento: Esta política se le realizará mantenimientos o actualizaciones para ajustar los contenidos.

6. Retiro: El comité de seguridad de la información tendrá la potestad para retirar cualquier retiro de política.

ARTICULO 6. POLITICAS ESPECÍFICAS RECOMENDADAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Organización de la seguridad de la información

Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información. Debe tener los siguientes elementos:

- Los que conforman el comité de seguridad son: El subgerente administrativo, Asesor de planeación, Asesor de calidad, Jefe del área de sistemas, Coordinador de calidad
- Objetivos: Aprobar políticas, evaluar estrategias de seguridad, orientar en la toma de decisiones, recomendar iniciativas y revisión de resultados
- Cumplimiento: El comité de seguridad de la información revisara el cumplimiento de las políticas.
- Gestión de activos

Identificación de Activos: el proceso de identificación de los activos de la información se actualizará en la medida que el jefe del área reporte al área de sistema del nuevo activo de la información.

Clasificación de Activos: La Entidad debe determinar la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Entidad, algunos ejemplos: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza de la entidad.

Etiquetado de la Información: Esta política debe determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.

Gestión de medios removibles: Los jefes de área determinan los usos y permisos que tienen los usuarios y/o funcionarios de la Entidad frente a los medios removibles.

Política de control de acceso con usuario y contraseña

Control de acceso con usuario y contraseña: Este proceso dentro de la política sobre control de acceso y contraseñas a redes, aplicaciones, y/o sistemas de información de la entidad, mediante la cual se determina los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas.

El proceso dentro de la política anuncia las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de la entidad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.

Suministro del control de acceso: Este proceso dentro de la política se determina según el área donde se encuentre el usuario (área) se identificará un grupo de permisos para los usuarios para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados.

Gestión de Contraseñas: Este proceso dentro de la política define los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad.

Altas y bajas de los usuarios del sistema de información: Este proceso se define como mecanismo de seguridad e integral del sistema de control de accesos al sistema de información.

La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.

La política deberá incluir mínimo los siguientes aspectos:

Trazabilidad: Este proceso hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.

Retención: Este proceso incluirá el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.

PRIVACIDAD Y CONFIDENCIALIDAD

Este proceso contiene una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente.

INTEGRIDAD

Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

DISPONIBILIDAD DEL SERVICIO E INFORMACIÓ

La Entidad deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

Niveles de disponibilidad: Este proceso debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con clientes, proveedores y/o terceros en función de las necesidades de la Entidad, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos. Ver Plan de continuidad del negocio y de contingencias.

Planes de recuperación: El plan incluye los planes de recuperación que incluyan las necesidades de disponibilidad del negocio. Ver Plan de continuidad del negocio y de contingencias.

Interrupciones: El plan vela por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad del mismo.

Acuerdos de Nivel de servicio: Tener en cuenta los acuerdos de niveles de servicios en las interrupciones del servicio.

Segregación de ambientes: Esta política debe establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.

Gestión de Cambios: La política debe incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

MATRIZ DE ROLES DE LOS SISTEMAS DE INFORMACION:

La definición del equipo responsable de seguridad y privacidad de información dentro de las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

REGISTRO Y AUDITORÍA

Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Esta política deberá contener:

Responsabilidad: Incluir la responsabilidad de la Oficina de Control Interno y similares, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

Almacenamiento de registros: La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.

Normatividad: La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.

Garantía cumplimiento: La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.

Periodicidad: La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

La política debe contemplar para su elaboración los siguientes parámetros:

Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.

- **Visión General:** ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?
- **Definir Responsables:** Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.
- **Actividades:** Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
- **Documentación:** Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.
- **Descripción Del Equipo Que Manejará Los Incidentes:** Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.
- **Aspectos Legales:** Deben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN:

Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.Dicha política debe contener los siguientes parámetros.

- El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.
- ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- La obligación de los usuarios a asistir a los eventos o cursos de capacitación.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- Definir los roles y responsabilidades de quienes diseñarán los programas, quienes los comunicarán.
- Documentación sobre planes de estudio y desarrollo de los programas.
- Compromisos y obligaciones por parte del personal capacitado.
- Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios usuarios como las siguientes:
  - Política De Escritorio Limpio
  - Política De Uso Aceptable
  - Ética Empresarial.

ARTICULO 7: La presente resolución rige a partir de la fecha de su expedición

COMUNIQUESE, NOTIFIQUESE Y CUMPLASE:

Dada en Zarzal Valle del Cauca, a los ocho (08) días del mes de noviembre del dos mil veintidós (2022).

Julián Andrés Correa Trujillo
Gerente

Elaboro: Sandra Rincón – Coordinadora de sistemas
Reviso: Paulo Castillo Ferreira – Asesor de Calidad
Aprobó: Julián Andrés Correa Trujillo – Gerente