MANUAL DE SEGURIDAD DE LA INFORMACIÓN

En desarrollo del principio de seguridad establecido en la Ley 1581 de 2012, **ALMACÉN SANITARIO EJE CAFETERO S.A.S** adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

1. OBJETIVO

Constituir los lineamientos y medidas necesarias para evitar posibles afectaciones a la seguridad de los datos. Además de establecer el procedimiento en caso de que las medidas de seguridad fallen.

2. ALCANCE

Aplica para los colaboradores, contratistas y proveedores de **ALMACÉN SANITARIO EJE CAFETERO S.A.S.**

3. DEFINICIONES

- **BASE DE DATOS:** Conjunto organizado de datos utilizados por los Sistemas de Información para el funcionamiento de sus aplicaciones y que son objeto de tratamiento por las diferentes Unidades de Negocio.

- **CONTROL DE ACCESOS:** Procesos que garantizan que solo las personas que necesitan acceso a ciertos activos disponen de dicho acceso y la necesidad se determina acorde a los requisitos del negocio y la seguridad.

- **CUSTODIO DE LA INFORMACIÓN:** Es cualquier empleador o tercero autorizado que tiene la obligación de salvaguardar, mantener, recuperar y soportar la información de la entidad.

- **DATO PERSONAL:** Cualquier información vinculada a personas naturales, la información personal tal como: Nombre, apellido, teléfono, estado civil, número de identificación, correo electrónico, domicilio, fecha de nacimiento, edad, nacionalidad.

- **DATOS SENSIBLES:** La información vinculada a personas naturales que afectan su intimidad o pueden generar discriminación tal como: origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos, datos relativos a la salud, vida sexual y los datos biométricos.

- **DATOS PÚBLICOS:** Es la información personal que está contenida en registros públicos, documentos públicos, boletines oficiales y sentencias judiciales no sometida a reserva tal como el estado civil, profesión u oficio.

- **DATOS CONFIDENCIALES RESTRINGIDOS:** Información con datos sensibles que puede ser conocida únicamente por cierto número de colaboradores de **ALMACÉN SANITARIO EJE CAFETERO S.A.S.**

- **ENCARGADO DEL TRATAMIENTO:** Es la persona física o jurídica, autoridad pública o privada, que por sí misma o en asocio con otros perteneciente a **ALMACÉN SANITARIO EJE CAFETERO S.A.S,** realice el tratamiento de datos personales por cuenta del responsable.

- **PRINCIPIO DE SEGURIDAD:** la información sujeta a tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad.

- **PRINCIPIO DE CONFIDENCIALIDAD: ALMACEN SANITARIO EJE CAFETERO S.A.S** está obligado a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley.

- **RESPONSABLE DEL TRATAMIENTO:** Es la persona física o jurídica, autoridad pública o privada, que por sí misma o en asocio con otros perteneciente a **ALMACÉN SANITARIO EJE CAFETERO S.A.S,** que recolecta los datos personales y decide sobre la finalidad, contenido y uso de la base de datos para su tratamiento.

- **RIESGO:** Combinación de probabilidad de ocurrencia de un evento de seguridad de la información y su resultante consecuencia.

- **TRATAMIENTO DE DATOS:** Cualquier operación o conjunto de operaciones y procedimientos técnicos de carácter automatizado o no que se realizan sobre datos personales, tales como la recolección, grabación, almacenamiento, conservación, uso, circulación, modificación, bloqueo, cancelación, entre otros.

- **TITULAR:** Dueño de la información personal. Si se trata de un menor de edad, se trata como titular al Represente legal del menor.

4. LINEAMIENTOS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN

4.1 CUMPLIMIENTO Y SANCIONES

4.1.1 LINEAMIENTO

Todos los colaboradores de **ALMACÉN SANITARIO EJE CAFETERO S.A.S**, los contratistas, proveedores deben cumplir y acatar el manual de seguridad de la información.

4.1.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Todo incumplimiento de algún lineamiento aquí desarrollado es causal para iniciar las correspondientes acciones disciplinarias o contractuales, las cuales dependerán de la gravedad del incumplimiento.

4.2 CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

4.2.1 LINEAMIENTO

Todos los colaboradores de **ALMACÉN SANITARIO EJE CAFETERO S.A.**S o terceros autorizados deben disponer de un medio de identificación y su acceso debe estar controlado a través de una identificación.

4.2.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Códigos de usuarios personalizados:** Cada usuario tendrá personalizado para tener acceso a todas las plataformas y aplicaciones que utilice.
- **Creación, eliminación e inhabilitación de códigos de usuarios:** El área de informática y tecnología es la única autorizada de administrar los códigos de usuarios, son los únicos autorizados para crear, eliminar o inhabilitar los mismos. Se deben habilitar los usuarios cuando se tengan más de 8 intentos fallidos de ingreso.
- **Creación de contraseñas:** Cada contraseña será generada de manera automática por el sistema, pero el responsable podrà modificarla cuando ésta le sea asignada.
- **Vigencia de las contraseñas:** Como política de la compañía,podrán cambiar su contraseña en cualquier momento o cuando puedan identificar un posible riesgo de seguridad

4.3 PROPIEDAD INTELECTUAL

4.3.1 LINEAMIENTO

La propiedad intelectual de la compañía como productos, servicios y desarrollos de software debe protegerse.

4.3.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Cesión de derechos:** Todos los colaboradores y terceros que se encarguen de desarrollo de software, patentes, invenciones u otra propiedad intelectual que ellos originen con desarrollo a una relación contractual con ALMACEN SANITARIO EJE CAFETERO S.A.S deberá conceder a ALMACEN SANITARIO EJE CAFETERO S.A.S los derechos exclusivos de sus productos y servicios.

4.4 RESPALDO DE LA INFORMACIÓN

4.4.1 LINEAMIENTO

Todos los archivos de datos y bases de datos de datos sensibles deberán contar con el respaldo necesario para recuperarse en caso de imprevistos o ataques a la seguridad de la información.

4.4.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Plan de recuperación de los servicios de tecnología informática**: Todos los sistemas de información de la entidad deberán tener un plan de recuperación de tecnología informática que permita garantizar una respuesta efectiva y eficiente ante eventos de desastre o interrupciones mayores.
- **Custodia de los medios de respaldo de la información crítica**: Los medios de respaldo que contienen la información crítica del negocio deberán ser almacenados en un lugar externo a la entidad que cumpla con los requerimientos de seguridad y conservación de los medios.

4.5 SEGURIDAD FÍSICA

4.5.1 LINEAMIENTO

Todas las áreas físicas del negocio deberán contar con el nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas. La información confidencial y restringida deberá mantenerse en lugares con acceso restringido cuando no es utilizada

4.5.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Clasificación:** La información deberá ser clasificada según el riesgo que se pueda derivar de la criticidad de los datos personales tratados, nivel de clasificación alto, medio o bajo.

- **Seguridad Física de áreas de Acceso Restringido:** Deberán existir estrictos controles para el ingreso al archivo de
- permitiendo el ingreso únicamente al personal autorizado y llevando un registro exhaustivo del personal que ingresa.

4.6 SEGURIDAD EN EL PERSONAL

4.6.1 LINEAMIENTO

ALMACEN SANITARIO EJE CAFETERO S.A.S se compromete en los casos a que haya a lugar a difundir el manual de seguridad de la información para asegurar que cumplan sus responsabilidad en materia de seguridad.

4.6.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Cumplimiento de los lineamientos y normas de seguridad de la información**: Es obligación de los colaboradores de la entidad, conocer, respetar, cumplir y hacer cumplir las políticas y normas de seguridad de la información contenidas en este documento. Por lo tanto, deberán hacer parte de los contratos de trabajo o en su defecto del reglamento interno de trabajo. Esta norma se aplicará de igual forma para los empleados suministrados por las empresas de servicios temporales y los terceros que prestan servicios a la entidad.
- **Acuerdo de confidencialidad con los colaboradores:** Todos los empleados y contratistas deberán firmar un acuerdo de confidencialidad de la información.
- **Reporte de incidentes de seguridad:** Los empleados deberán reportar cualquier incidente, vulnerabilidad o riesgo potencial que afecte la seguridad de la información.
- **Terminación de contrato:** Al finalizar el contrato, los colaboradores deberán devolver toda la información que sea propiedad de **ALMACÉN SANITARIO EJE CAFETERO S.A.S** y se le bloqueará de manera inmediata de su código de usuario.

4.7 CAPACITACIÓN LEY 1281 DE 2012

4.7.1 LINEAMIENTOS

ALMACÉN SANITARIO EJE CAFETERO S.A.S realizará periódicamente y según la necesidad capacitaciones para fortalecer el principio de seguridad de la información.

4.7.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Capacitaciones:** Se realizarán capacitaciones para desarrollar el contenido de la ley 1281 de 2012 y en especial el principio de seguridad de la información.
- **Divulgación:** Se divulgará el manual de seguridad de la información con el ingreso de cada nuevo colaborador. Se realizarán jornadas de refuerzo cada seis (6) meses para toda la compañía.
- **Medición:** Anualmente se realizará una evaluación de los resultados de las capacitaciones con el fin de establecer la efectividad de la misma.

4.8 CONTRATOS CON TERCEROS

4.8.1 LINEAMIENTOS

Los terceros deben cumplir con la ley 1281 de 2012 y adoptar su manual de seguridad de la información.

4.8.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Cláusulas de seguridad:** Se deberán incluir cláusulas para dar cumplimiento a las medidas de seguridad adoptadas en el presente manual.
- **Acuerdo de confidencialidad:** Se deben firmar acuerdos de confidencialidad con los terceros.
- **Cumplimiento de política de tratamiento de datos:** Se debe verificar que el tercero cumple con su política de tratamiento de datos

4.9 CONEXIÓN A REDES

4.9.1 LINEAMIENTOS

Todas las conexiones por medio de redes públicas (celular, Internet) o por acceso remoto deberán ser autenticadas para evitar que la información sea develada o alterada sin autorización.

4.9.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- Acceso por control remoto: El acceso a los equipos de cómputo y/o servidores de la entidad desde fuera de sus instalaciones sólo será permitido a las personas autorizadas por el líder de gestión de incidentes o quien haga sus veces y se hará a través del establecimiento de redes privadas virtuales. (se debe determinar el líder de gestión de incidentes)
- La red de datos es de uso estrictamente laboral.

4.10 CÓDIGO MALICIOSO

4.10.1 LINEAMIENTO

Todos los documentos electrónicos que ingresen a la entidad deberán ser revisados como medida preventiva de código malicioso por el funcionario de la entidad que recibe el documento.

4.10.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Análisis de archivos:** Los archivos adjuntos al correo electrónico y todos los archivos descargados de Internet deberán ser analizados antes de su ejecución. Medios de almacenamiento externos electrónicos y ópticos (diskettes, CDs, DVDs, memorias USB, etc.) que han estado fuera de control del usuario se deberán ser analizados antes de su uso por parte del funcionario de la entidad que está manipulando el archivo.

4.11 CLÁSIFICACIÓN DE LA INFORMACIÓN

4.11.1 LINEAMIENTO

La entidad adoptará las medidas necesarias para otorgar seguridad según la clasificación de los datos personales. Las medidas de seguridad serán reforzadas, especiales y más robustas respecto de bases de datos que contengan datos sensibles.

4.11.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- **Clasificación:** La información deberá ser clasificada según el riesgo que se pueda derivar de la criticidad de los datos personales tratados, nivel de clasificación alto, medio o bajo.

- **Clasificación alta:** Es aquella información sensible que tendrá uso restringido y solo podrá ser consultada por ciertos colaboradores. Esta se encontrará en el archivo de datos sensibles, con acceso restringido, se deberá disponer de llaves que dificulten su apertura.
  Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de su medio de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

- **Protección de la información:** Toda la información de la entidad deberá ser protegida por los colaboradores, contratistas y proveedores de acuerdo a su valor.

  Eliminación segura: Toda la información deberá ser desechada de forma tal que se proteja la confidencialidad.

- **Acceso a documentos:** El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado por los responsables del tratamiento, siguiendo los mecanismos y procedimientos definidos.
  El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles (clasificación alta) implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá ser reportado como un incidente de seguridad.

4.12 MEDIDAS PREVENTIVAS PARA HACER FRENTE A UN INCIDENTE DE SEGURIDAD

4.12.1 LINEAMIENTOS

La entidad debe propender por prevenir los incidentes de seguridad. O en su defecto contar con empresas certificadas que manejen la información de la seguridad o que así lo refieran.

4.12.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- Un incidente de seguridad surge debido a la presencia de amenazas para activos que se procesan, almacenan, mantienen, protegen o controlan el acceso a la información.
- Entrenar periódicamente al equipo humano de la organización para actuar frente al incidente de seguridad efectuando simulacros para determinar cómo se debe actuar ante un incidente.
- Auditorías: Las bases de datos que contengan datos personales, objeto de tratamiento por ALMACÉN SANITARIO EJE CAFETERO S.A.S se han de someter a auditorías internas o externas que verifiquen el cumplimiento de las medidas de seguridad contenidas en este manual. El alcance y periodicidad de las auditorías será definido anualmente por la entidad. (se debe definir la política de auditorias, su periodicidad y procedimiento)

4.13 MECANISMOS DE MONITOREO Y CONTROL

4.13.1 LINEAMIENTOS

La entidad debe implementar mecanismos de monitoreo y control para evitar los incidentes de seguridad.

4.13.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN (REALIZAR LOS LINEAMIENTOS DE ACUERDO A LAS CONDICIONES DE LA EMPRESA)

- Realizar procedimientos para la validación de datos de entrada y procesamiento de la información personal con el fin de garantizar que los datos recolectados y procesados sean correctos y apropiados.
- Implementar en las bases de datos el monitoreo de consultas.
- Implementar auditorías de seguridad de información personal que tengan en cuenta el cumplimiento de requisitos, políticas y normas respecto de las bases de datos.
- Implementar controles de seguridad de la información durante el mantenimiento de los sistemas de información personal.

4.14. CONSERVACIÓN DE REGISTROS INTERNOS

4.14.1 LINEAMIENTOS

La entidad conservará los registros de cada incidente de seguridad.

4.14.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- Registros de incidentes: Dentro de los registros de incidentes se debe llevar una descripción general de las circunstancias, la categoría de titulos de la información afectada, la fecha y hora del incidente de seguridad, las indagaciones preliminares, los responsables del manejo de incidente de seguridad, la prueba del reporte efectuado ante la SIC, evaluación del riesgo derivado del incidente, la inclusión de detalles personales y las medidas correctivas.
- Conservación de los registros de incidentes: La entidad deberá conservar cada uno de los registros de los incidentes para una eventual investigación o para evitar que ocurran nuevamente.

5. ROLES Y RESPONSABILIDADES

Apropiar el manual de Seguridad de la Información mediante la incorporación de buenas prácticas en el uso de la información, sistemas de información y recursos informáticos de ALMACEN SANITARIO EJE CAFETERO S.A.S como una herramienta para garantizar la confidencialidad, integridad y disponibilidad de la información.

PROCESOS

Gerencia de desarrollo humano Velar por el cumplimiento del Reglamento Interno de Trabajo, en los casos que aplique con respecto a los lineamientos de seguridad de la información enunciados en el presente manual. Además, tendrá acceso a la información sensible y deberá asegurarse de la custodia de las hojas de vida.

Las hojas de vida de los aspirantes solo pueden ser conocidas por el área de talento humano o el personal responsable de manejo de información sensible dispuesta en el archivo esa información será de carácter transitorio hasta que se dé por finalizado el proceso de selección de la vacante. Cuando se haya vinculado a el colaborador, las demás hojas de vida serán desechadas de acuerdo con el procedimiento acá desarrollado.

ÁREA DE INFORMÁTICA

Líder sistema de información: Es el encargado de la administración e interacción con las funcionalidades del sistema de información. Es la persona que tiene la responsabilidad de asegurar y otorgar el acceso a la información que genere el proceso y que es soportada por los Sistemas de Información

Líder técnico: Es el encargado de mantener tecnológicamente los recursos informáticos y sistemas de información disponibles para su uso. Se encarga de la administración técnica del software base, entornos de ejecución, programas ejecutables y servicios del sistema.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Propender por la apropiación del Manual de Seguridad de la Información mediante la incorporación de buenas prácticas en el uso de la información, sistemas de información y recursos informáticos.
Además de realizar y conservar los registros internos de la entidad.

GRUPO DE RESPUESTA A INCIDENTES

Está conformado por los gerentes de cada área y el representante legal de la compañía, son los encargados de analizar y validar cada incidente reportado y determinar el alcance los incidentes.

- Líder Gestión de Incidentes: Gerente del área informática
- Líder Equipo de Respuesta a Incidentes: Gerente del área de recursos humanos. VERIFICAR DE ACUERDO A LAS CONDICIONES DE LA EMPRESA

6. POLÍTICA PARA EL CORRECTO TRATAMIENTO DE LA INFORMACIÓN PERSONAL

Para darle un correcto tratamiento a la información personal se han desarrollado una serie de exigencias dependiendo del ciclo de vida del dato.

6.1 Recolección

Para la recolección de los datos personales se debe contar con la debida autorización del titular, asegurándose de informar sobre la ley de habeas data y la política de tratamiento de datos de la entidad.

6.2 Circulación

Durante la custodia de la información por parte de **ALMACÉN SANITARIO EJE CAFETERO S.A.S**, la compañía se compromete a implementar el manual de seguridad de la información, restringir el acceso de los datos sensibles a ciertos colaboradores e implementar medidas tecnológicas para evitar que la información sea consultada por personal no autorizado.

6.3 Disposición final

Para la supresión total de los datos, la compañía adoptará un procedimiento de (lineamientos para garantizar que los documentos han sido eliminados y desechados).

7. LINEAMIENTOS DE SEGURIDAD PARA LA GESTIÓN DE INCIDENTES

Un incidente de seguridad surge debido a la presencia de amenazas para activos que se procesan, almacenan, mantienen, protegen o controlan el acceso a la información.

7.1 TIPOS DE INCIDENTES

- **VIOLACIÓN DE UNA POLÍTICA DE SEGURIDAD**: Violación de la política de tratamiento de datos de ALMACÉN SANITARIO EJE CAFETERO S.A.S

- **HURTO O PERDIDA DE DISPOSITIVOS O RECURSOS HARDWARE:** Pérdida física de un recurso tecnológico (computadores de escritorio, portátiles, celulares, servidores, equipos de telecomunicaciones) de propiedad de ALMACÉN SANITARIO EJE CAFETERO S.A.S

- **INTENTO DE ACCESO**: Se detecta el intento de ingreso al sistema con una contraseña errónea por más de ocho (8) veces, o en su defecto por lo dispuesto por los mecanismos de control a cada una de las aplicaciones que se pudieran tener y den para su manejo propio de seguridad.

- **ACTIVIDAD DE VIRUS INFORMÁTICOS**: Un virus, gusano, troyano, botnets, keylogger, rootkit, apt, código malicioso etc., que se base en código desarrollado con el propósito de infectar una estación de trabajo, servidor o sistemas de ALMACÉN SANITARIO EJE CAFETERO S.A.S con el fin de capturar contraseñas o información confidencial, modificar registros de auditoría, para esconder o eliminar actividades no autorizadas.

- **DIVULGACIÓN O FUGA DE INFORMACIÓN:** Este incidente consiste en la pérdida o revelación de información catalogada como sensible o confidencial de forma intencional o no intencional, a través de impresoras, equipos de cómputo, correo, internet y red, entre otros.

- **ACCESO NO AUTORIZADO:** Una persona obtiene acceso (intencional o inadvertido) lógico o físico sin permiso o autorización a una red o recurso de la entidad, sistemas de información o, información (p.e. información de logs, bases de datos, datos personales de trabajadores) y en general cualquier recurso tecnológico bajo la custodia de la entidad.

7.2 REPORTE GESTIÓN DE INCIDENTES

Todos los colaboradores, contratistas y proveedores externos son responsables por reportar en forma inmediata y mediante los canales y medios destinados (comunicación a área informática por correo electrónico) para tal fin, cualquier condición anormal o vulnerabilidad que detecten en el uso de los recursos informáticos y/o de la información de la entidad, así como la violación de los lineamientos de Seguridad de Información de la entidad por parte de colaboradores, estudiantes o terceros.

7.3 GESTIÓN DE INCIDENTES

- La administración de los incidentes de Seguridad de la Información estará a cargo de la dirección de sistemas
- Todo incidente o alerta de seguridad debe ser tratado de principio a fin mediante un procedimiento de tratamiento de incidentes que garantice el análisis, investigación, documentación, solución, seguimiento a los mismos y en algunos casos permita adelantar acciones administrativas/legales correspondientes.

- La dirección de sistemas es la responsable de analizar y determinar qué eventos son considerados incidentes de Seguridad de la Información, así como de realizar la categorización y priorización de los mismos.

- El Grupo de Respuesta a Incidentes, debe analizar y validar cada incidente reportado y determinar el alcance de los incidentes, tal como redes, sistemas o aplicaciones afectadas, origen del incidente de seguridad reportado, herramientas o métodos de ataque utilizados, vulnerabilidades explotadas y daños causados por el mismo.

- El Grupo de Respuesta a Incidentes es el responsable de:

  a) La investigación, gestión y solución de los incidentes de seguridad de la Información.

  b) Realizar el levantamiento de información y material que sirva de soporte o prueba de una investigación.

  c) Garantizar la retención segura de toda la información perteneciente al incidente para un análisis posterior (de ser necesario).

  d) Definir el plan de trabajo y la implantación de las acciones correctivas requeridas, de acuerdo con los daños evidenciados en la investigación del incidente.

  e) Documentar en la base de conocimiento todas las medidas, actividades y tareas

  realizadas durante la gestión del incidente, de acuerdo a requerimientos regulatorios y legales que apliquen.

  f) El GRI debe estar disponible para atender los llamados que realice el *Líder del Equipo de respuesta a incidentes*, cuando se identifique o se sospeche que se ha producido un incidente y que de acuerdo a la severidad asignada deba ser atendido y gestionado por el GRI.

- El *Equipo de respuesta a incidentes (GRI)* será convocado por parte del *Líder Equipo de Respuesta a Incidentes*, para el tratamiento y atención de incidentes con una severidad de Crítico o Alto.

- Los incidentes de seguridad de la información con una severidad de Medio y Bajo, serán atendidos y tratados directamente por el *Líder Gestión de Incidentes, el Líder Equipo de Respuesta a Incidentes y/o Gestor Incidentes*, por lo tanto, no se convocará el *Grupo de Respuesta a Incidentes (GRI).*

- La información de la Gestión de Incidentes de Seguridad, así como las investigaciones realizadas es de carácter confidencial para la entidad y su divulgación o distribución está bajo la responsabilidad del Líder de la Gestión de Incidentes.

8.0 DISPOSICIONES

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.