PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La Plata (H), enero 202

Tabla de contenido

1 INTRODUCCION

La seguridad y privacidad de la información, se enfoca en proteger los recursos informáticos mitigando el robo de datos institucionales con intenciones maliciosas. La seguridad informática se rige por protocolos, normas, estándares, leyes y demás, abarcando una serie de medidas que disminuyen los riesgos a la base de datos, software, archivos, información o infraestructura informática institucional entre otros.

La Empresa Social del Estado San Sebastián de la Plata Huila, busca implementar el plan de Seguridad y Privacidad de la información y el Sistema de Seguridad de la Información, dando cumplimiento a la exigencia del Gobierno Nacional y siguiendo los lineamientos del Ministerio de Tecnologías de la Información y la Comunicación.

1. JUSTIFICACIÓN

Los grandes volúmenes de información institucionales se originan desde diversas fuentes y con estándares tecnológicos heterogéneos, que requieren de una infraestructura de red adecuada, funcional y confiable para su transmisión y almacenamiento.

Para tal efecto, la Empresa Social del Estado San Sebastián de la Plata Huila, cuenta con conectividad de ultima tecnología y servicios informáticos diseñados para soportar aplicaciones de procesamiento de datos, igualmente cuenta con una rigurosidad en parámetros que permiten tener mayor seguridad de la información. El crecimiento exponencial de nuevos servicios y aplicaciones ha exigido la planeación e implementación de redes con nuevas tecnologías mitigando las dificultades en la operación de la red y en la gestión de la seguridad de la información.

El presente documento pretende exponer una serie de lineamientos que permitan implementación las mejores prácticas de Seguridad Informática en la E.S.E. San Sebastián, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad/privacidad de la información institucional.

2. OBJETIVOS

2.1 Objetivo General

Elaborar e implementar los lineamientos de Seguridad y Privacidad de la información en la Empresa social del Estado San Sebastián, que permitirán preservar la integridad, confidencialidad y disponibilidad de la información.

2.2 Objetivos Específicos

- Promover el uso de prácticas de seguridad de la información.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Optimizar la labor de acceso a la información pública al interior de la entidad.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

3. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La Empresa Social del Estado San Sebastián de la Plata Huila, está comprometida con la protección de los activos informáticos institucionales, en pro de ello, define el obligatorio cumplimiento del plan de seguridad y privacidad de la información a todo el personal contratista y de planta de la ESE San Sebastián que cuenten con equipos informáticos institucionales y/o que tengan conexión a la red interna de la entidad.

Todo el personal debe ser capacitado sobre seguridad y privacidad de la información, teniendo claridad en las responsabilidades adquiridas y las sanciones acarreadas por el no cumplimiento de las políticas y estándares de seguridad informática.

3.1 SEGURIDAD DE EQUIPOS INFORMATICOS

3.1.1 El área de Gestión de Sistemas de información (GSI) en cabeza de líder de proceso, debe contar con el respectivo registro de todos los equipos informáticos de la entidad al igual que las hojas de vida debidamente actualizada

3.1.2 Todo equipo informático, periférico y/o accesorio, debe contar con la ubicación adecuada cumplimiento con las condiciones de seguridad física, ambiental y eléctrica, las cuales deberán ser verificadas y garantizadas por el área de SGI y Mantenimiento.

Garantizando igualmente, que los mencionados no estén en contacto directo con la luz solar, con humedades o demás que hagan que el equipo tengo contacto directo con el agua.

3.1.3 Los servidores centrales de la red de la ESE San Sebastián, debe estar ubicado en un lugar exclusivo, con acceso solo al personal del área de GSI cumpliendo con las condiciones adecuadas de espacio, temperatura, iluminación, entre otras.

3.1.4 Todos los equipos informáticos, periféricos y/o accesorios institucionales o externos, que sean conectados a la RED de la ESE San Sebastián, deben cumplir con los procedimientos de instalación dadas por el área de SGI de la ESE San Sebastián de la Plata Huila.

3.1.5 El cambio y/o traslado de equipos informáticos dentro y/o fuera de las diferentes sedes de la ESE San Sebastián, debe ser notificados, aprobados y ejecutados por el área de GSI, incluyendo el préstamo de equipos informáticos en periodos cortos (horas o días)

Toda área que requiera cambio de locación de múltiples equipos periféricos y/o accesorios informáticos, debe realizar la respectiva notificación con 5 días de antelación.

3.1.6 Los equipos informáticos externos que sean ingresados a la institución, deberán ser registrados en el área de portería con la ayuda del orientador o quien cumpla dicha función, a su vez deberá ser informado al área de SGI para la conexión respectiva a la red institucional si así lo requiere.

Todo propietario de equipos externos conectados a la red eléctrica y/o datos de la ESE San Sebastián, se hará responsable en su totalidad de los daños que el mismo pueda presentar, dejando claro que la Institución no se hace responsable de daños físicos o lógicos que presenten equipos o periféricos de terceros.

3.1.7 Todo equipo, periférico y/o bien informático institucional, debe ser registrado al momento de ser extraído de la institución y con previa autorización del área de Gestión de Sistemas de información, siempre y cuando sea para uso expreso de las funciones laborales asignadas.

3.1.8 Todo equipo infantico conectado a la red de la institución deberá contar con un dispositivo de protección eléctrica, ya sea estabilizador de corriente o UPS, que resguarde al equipo ante un cambio brusco en la corriente eléctrica de la entidad o del sector donde se ubica.

Equipo que no cuente con protección eléctrica, no puede ponerse en funcionamiento, colaborador que no acate la política indicada ocasionando daño parcial o total en el bien informático institucional, será el directo responsable.

En caso que se necesite poner en funcionamiento un equipo que no tenga UPS o estabilizador, podrá hacerse de manera temporal y con el acompañamiento del personal del área de GSI.

3.1.9 La protección física (hardware) de los equipos informáticos, periféricos y/o accesorios ubicados en cada una de las áreas de trabajo, es responsabilidad de cada colaborador que tenga asignado como activo fijo el bien informático; a su vez, tiene la responsabilidad de informar inmediatamente al área de SGI todo daño, perdida o cualquier eventualidad identificada que afecte el equipo informático.

3.1.10 El personal de la ESE San Sebastián de la plata Huila, tiene prohibido ingerir alimentos junto a equipos informáticos, adicionalmente, no debe ubicar sobre o cerca al equipo elementos que causen daños o riesgo alguno; No tiene permitido obstruir con ningún tipo de elemento (forros, documentos etc.) el área de ventilación de los equipos informáticos.

En caso de presentar algún incidente mencionado, debe apagar inmediatamente el equipo e informar al área de SGI, quien tomara las medidas correctivas necesarias para salvaguardar el bien informático.

3.1.11 El personal del área de GSI son los únicos autorizados para realizar instalaciones y/o mantenimientos de equipos, impresoras, scanner o brindar soportes técnicos a nivel de hardware, sin importar su nivel de complejidad, por ende, no se autoriza que personal externo al área de GSI manipule los equipos informáticos de la entidad.

Quien incurra en esta conducta no autorizada, será notificado y se tomaran las medidas correctivas necesarias.

3.1.12 El personal del área de GSI no esta autorizado a brinda soporte, mantenimiento y/o actualización a equipos informáticos que no hacen parte de los bienes informáticos de la ESE San Sebastián de La Plata Huila.

3.1.13 Los equipos de computo de la ESE San Sebastián de la Plata Huila, contaran con clave de administrador la cual será de uso exclusivo del área e GSI, a su vez contara con clave para el manejo del área asignada teniendo conocimiento el líder del proceso y/o colaborador correspondiente.
Las claves asignadas, serán institucionales y solo podrán ser actualizadas por el personal de GSI.

3.1.14 El personal de la ESE San Sebastián, que conecte dispositivos de almacenamiento extraíble (USB, CD-DVD etc.) en los equipos informáticos de la institución, deberá velar por el buen uso del mismo mitigando fallas y retrasos en los procesos.

3.1.15 Los equipos informáticos, periféricos y/o accesorios de la ESE San Sebastián de la Plata Huila, deben ser utilizado en cumplimiento a las funciones asignadas por la entidad, por ende, no deben ser usados para asuntos personales.

3.1.16 Todo funcionario que, por negligencia, descuido y/o mal uso de los bienes informático institucional cause daño parcial o total a los mismos, se hará acreedor a reporte de incumplimiento de las políticas de seguridad y la amonestación que ello conlleve

3.1.17 La adquisición de nueva infraestructura de procesamiento de la información (hardware, software, aplicaciones e instalaciones físicas) o la actualización de la existente, deberá ser verificada y autorizada por el área de GSI junto con el líder de proceso del área implicada.

3.1.18 El personal de planta o contratista de la ESE San Sebastián de La Plata Huila, debe realizar entrega de todo equipo o bien informático asignado a su cargo dentro del cumplimiento de sus funciones contractuales, al momento de culminar su vinculación contractual con la entidad, en las mismas condiciones (Hardware) que lo recibió.

3.2 SEGURIDAD DE USUARIOS

3.2.1 El personal de planta y contratistas de la ESE San Sebastián de La Plata Huila, debe cumplir a cabalidad con los requerimientos de seguridad de información, a su vez deberán recibir inducción sobre el Plan de seguridad y privacidad de la información institucional.

3.2.2 La información manejada y almacenada en los equipos informáticos de la ESE San Sebastián, es de propiedad de la institución, cada usuario es responsable de su integridad, conservación y disponibilidad de la misma.

3.2.3 Ninguna persona que tenga vinculación laboral de cualquier tipo con la ESE San Sebastián de La Plata Huila, tiene permitido divulgar, alterar, borrar información de los equipos informáticos sin previa autorización del área de GSI y el líder de proceso del área directamente implicada.

3.2.4 Las credenciales de acceso facilitadas a cada uno de los colaboradores de la institución, son de uso personal e intransferible, cualquier información que sea registrada, manipulada y/o eliminada serán responsabilidad del personal a quien se habilito y entrego las respectivas credenciales.

3.2.5 Los permisos asignados al personal institucional estarán ligados a las funciones contractuales, no se habilitarán permisos adicionales a estos.

De requerir un permiso adicional en plataforma o software institucional, deberá registrar solicitud debidamente avalada por el líder del área directamente implicada con la debida justificación.

3.2.6 Los usuarios que contengan credenciales de acceso a plataformas y/o software institucional, deberán renovar periódicamente las claves, solicitando al área de GSI acompañamiento para el debido proceso.

3.2.7 Se encuentra totalmente prohibido el El intento o violación de los controles de seguridad establecidos, El uso sin autorización de los activos informáticos; El uso no autorizado o impropio de la conexión al sistema; el uso indebido de la las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios Aún con la autorización expresa del usuario propietario de la misma.

3.2.8 El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados sin previo consentimiento o autorización del área de Gestión de Sistemas de Información.

3.2.9 Se debe notificar al área de GSI cualquier anomalía, sospecha de virus o demás programas que generen riesgo latente para a información almacenada en el equipo y/o red institucional, no debe distribuir dentro o fuera de la institución.

3.2.10 Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software mal intencionado que impida el normal funcionamiento de los sistemas de la entidad.

3.2.11 Los funcionarios deben velar por la conservación y privacidad de la información que contenga el bien informático que se haya asignado para el cumplimiento de las funciones laborales, por ende, es responsabilidad única la fuga de información almacenada en los equipos asignados a su cargo.

3.3 SEGURIDAD DE SOFTWARE

3.3.1 El área de GSI es la única autorizada para instalar los softwares informáticos y de telecomunicaciones requeridos para el desempeño de las obligaciones contractuales.

3.3.2 No se permite la instalación de programas de mensajería, juegos y/o software que no tengan relación alguna con las funciones laborales asignadas.

3.3.3 Todos los equipos informáticos de la ESE San Sebastián de La Plata Huila, deben conta con software de seguridad instalado y debidamente actualizado (antivirus, controles de acceso entre otros), quien no cuente con el mismo no debe ser conectado dentro de la red institucional.

3.3.4 La adquisición y actualización de software para los equipos de cómputo y telecomunicaciones serán acordados entre el área de GSI y la alta gerencia, teniendo en cuenta las necesidades recepcionadas y la disponibilidad presupuestal de la entidad.

3.3.5 Todo personal institucional que maneje información masiva y de carácter privado, debe informar al ares de GSI la necesidad de las copias de seguridad permanentes, considerándose esta información como un activo fijo de la entidad que debe ser preservado.

3.3.6 El área de GSI es la encargada de administrar las diferentes licencias de los softwares implementados en la institución, a su vez verificar la vigencia y renovación de las mismas.

3.4 SEGURIDAD DE RED

3.4.1 El área de GSI de la ESE San Sebastián, es la encargada de configurar todos los equipos informáticos dentro de la res institucional, ya sea con direccionamiento IP fijo y/o estático, y demás configuraciones que sean requeridas.

3.4.2 Se prohíbe el uso de dispositivos red que no sean de propiedad de la ESE San Sebastián de La Plata Huila, que sean dirigidos a crear redes LAN alternas a la institucional.

3.4.3 Queda prohibido dar uso a los servicios de la red institucional para actividades lucrativas, comercial de carácter individual, privada o para negocio particular, quien realice incumplimiento de la misma, se hará creedor a las notificaciones y/o sanciones que esta acarreen.

“Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.” (Ley 734 de 2002) Código Único Disciplinario

3.4.4 Se prohíbe el uso de los servicios de comunicación de la ESE San Sebastián, incluyendo los correos electrónicos o cualquier otro recurso, para intimidar o insultar a personas internas y/o externas de la institución, o para interferir en el trabajo de los demás.

3.4.5 Los medios de comunicación de la ESE San Sebastián, no deberán ser utilizados para accesos a redes y sistemas remotos no autorizada.

3.4.6 Se prohíbe el uso de los recursos de la red y medios de comunicación de la ESE San Sebastián, para monopolizar en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado

3.4.7 El personal del área de GSI es el único autorizado para realizar conexiones remotas a quipos de la institución, requeridos para tramites netamente laborales dentro y/o fuera del horario laboral.

3.4.8 Se prohíbe el uso de la red institucional para para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.

3.4.9 No se permite el intercambio de información de propiedad de la ESE San Sebastián con terceros mediante la red institucional.

3.4.10 Se prohíbe el uso de los recursos informáticos y de comunicación para acceder a paginas de música, video, pornografía, ocio entre otros, igualmente se prohíbe la descarga de videos, audios y demás información que no hagan parte del desempeño de las funciones laborales.

3.4.11 Se prohíbe dar uso a los recursos de la red institucional y de comunicación para infringir el derecho a la intimidad de los colaboradores y/o personal externo.

3.4.12 Los mensajes y la información contenida en los buzones de correo institucionales o que en su defecto se hayan creado para funciones laborales, son de propiedad de la Ese San Sebastián. Los buzones no deberán contener mensajes mayores a dos años de antigüedad, dejando el respectivo histórico del registro de los mensajes.

3.4.13 Toda alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red de la institución, será motivo de verificación y tendrá como resultado directo, la realización de una auditoría de seguridad y un reporte de los hallazgos a la oficina de Control Interno y Control Interno disciplinario para que se tomen las medidas pertinentes.

3.5 SEGURIDAD DE DATOS INFORMACION

3.5.1 El área de GSI debe garantizar la copia de seguridad de la Base de datos institucional, que permita la restauración de información en caso de ser requerida.

3.5.2 Las copias de seguridad de la Base de Datos institucional, se deben realizar diariamente en horario no laboral, evitando la congestión de la red y/o demora en procesamiento de información.

3.5.3 La ESE San Sebastián debe garantizar las copias de seguridad externas (nube), que garanticen el respaldo de la información al momento de presentarse una catástrofe.

3.5.4 Las auditorías de uso de los recursos informáticos a cada dependencia deberán realizarse periódicamente de acuerdo al calendario que establezca la Oficina de sistemas de información. Los hallazgos encontrados serán reportados a la oficina de Control Interno, Control Interno Disciplinario y Gerencia para que se establezcan los correctivos necesarios

3.6 ADMINISTRACION DE SEGURIDAD INFORMATICA

3.6.1 El área de GSI deberá realizar periódicamente auditorias de uso de los recursos informáticos a cada dependencia, que permita verificar el cumplimiento del plan de seguridad y privacidad e la información, los hallazgos identificados deberán ser reportados a Control interno disciplinario y gerencia general para seguimiento y toma de correctivos necesarios.

3.6.2 Toda la información que reposa en los equipos informáticos de la ESE San Sebastián de La Plata Huila, debe ser auditados por el área de GSI en la verificación del cumplimiento del plan de seguridad y privacidad de la información, los hallazgos identificados deberán ser reportados a Control interno disciplinario y gerencia general para seguimiento y toma de correctivos necesarios.

3.6.3 Los lideres de proceso serán los responsables en la implementación y garantía inicial del cumplimiento del plan y/o políticas que hayan sido publicadas, modificadas o adicionadas recientemente. Cualquier violación a las políticas y/o normas de seguridad establecidas en este documento y aprobadas mediante acto administrativo será sancionada disciplinaria o penalmente. Para las infracciones más graves, se acatará lo estipulado en la ley 1273 de 2009 de delitos informáticos, y Ley 734 de 2002 Código Único Disciplinario.

4. NORMATIVIDAD

- **BS 7799-3:2006:** Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).
- **Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013**: Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2693 de 2012:** Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
- **Decreto 2578 de 2012:** Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.
- **Ley 1273 DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 DE 2009:** Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- **Ley 1150 DE 2007:** Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
- **NTC 27001:2006:** Sistema de Gestión de Seguridad de la Información (SGSI). En 2005, con más de 1700 empresas certificadas en BS7799-2, ISO publicó este esquema como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799 y esta última norma se denomina ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido, así como el año de publicación formal de revisión.
- **ISO 27002:2005:** Esta norma proporciona recomendaciones de las mejores prácticas en la Gestión de la Seguridad de la Información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.
- **ISO/IEC 27001 2005:** Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.
- **Ley 962 DE 2005**: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **ISO/IEC TR 18044:2004:** Ofrece asesoramiento y orientación sobre la Seguridad de la Información de Gestión de incidencias para los administradores de seguridad de la información y de los administradores de sistemas de información.
- **Ley 599 DE 2000:** Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la

comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

5. GLOSARIO

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **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…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo**: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un Sistema o a la organización. (ISO/IEC 2700).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- I**nformación Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Ley de Habeas Data**: Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que

generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sea asociado de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

CONTROL DE DOCUMENTO Y DISTRIBUCIÓN

Control del Documento

	Nombre	Cargo	Dependencia	Fecha
Autor	Vilma Nordally Ramírez Nuñez	Contratista	GSI	2024
Revisión	Johnson Feller Perez	Subgerente	Subgerencia	
Aprobación	Javier Mauricio Bahamon Sala.	Gerente	Gerencia	

Estado:	Preparación:	X	Revisión:	**x**	Aprobación	X

Control de los Cambios

Versión No.	Fecha de Aprobación	Descripción de los Cambios	Solicitó
1	Enero 2023	Segunda versión Plan Privacidad de la Información.	Gerencia
2			
3			

Lista de distribución

VERSIÓN	FECHA	ÁREA	FIRMA
1	Enero 2024	Gestión de Sistemas de Información	
2			