1. OBJETIVO

Definir los parámetros y lineamientos para el uso apropiado de la información de SERVICIOS AMBIENTALES S.A. ESP Estas reglas se definen para proteger la información de la compañía y de nuestros clientes, minimizando los riesgos que puedan llegar a afectar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Los términos y condiciones descritos en esta política aplican a todos los procesos, colaboradores internos, consultores, contratistas y proveedores de SERVICIOS AMBIENTALES S.A. ESP, que usen o tengan acceso a la información que sea de propiedad de SERVICIOS AMBIENTALES S.A. ESP o nuestros clientes.

3. NORMAS GENERALES

3.1. Perspectiva ISO

- ISO 9001 de 2015: Sistema de gestión de calidad.

3.2. Reglamento legal

- Ver matriz legal.

4. DEFINICIONES

4.1. Software: En computación, término inglés que hace referencia a todo lo lógico, es todo programa o aplicación, programado para realizar tareas específicas.

4.2. Acuerdo de Confidencialidad: Es un convenio que crea obligaciones a una o a ambas partes que intervienen, con respecto al uso, manejo y divulgación de la información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la misma, como parte de una relación contractual o comercial.

4.3. Activo: Cualquier cosa que tenga un valor de importancia relevante para la organización. Entre los activos de una organización se encuentra hardware, software, documentos electrónicos o físicos, infraestructura, servicios, personal, entre otros. El término Activo es sinónimo de Activo de Información.

4.4. Amenaza: Es una fuente generadora de eventos o acciones que puede producir o causar un daño representativo al activo de información, generando un factor o escenario de riesgo que originaría a la organización pérdidas por riesgo de seguridad de la información. La amenaza es un contexto de seguridad de la información que se manifiesta a través de actos deliberados, intencionados o impredecibles y provocados por las personas, la tecnología, la infraestructura, acontecimientos externos, entre otros.

4.5. Confidencialidad: Propiedad de salvaguardar el activo de información de personas, procesos o entidades no autorizados.

4.6. Controles: Medidas de protección o salvaguardas dispuestas para reducir el nivel de riesgo. Pueden ser políticas, procedimientos, directrices, prácticas, estructuras de la organización, soluciones tecnológicas, entre otros.

4.7. Disponibilidad: Propiedad de garantizar que el activo de información sea accesible y utilizable en el momento que se requiera, por parte de las personas, procesos o entidades autorizada.

4.8. Equipamiento: El equipamiento de procesamiento de la información incluye todo tipo de elemento físico soportado para el desarrollo de las actividades diarias del negocio. Estos elementos pueden ser entre otros: computadores de escritorio o personales, organizadores físicos, teléfonos móviles, escáneres, impresoras, tóner, fotocopiadoras, dispositivos USB, discos removibles, medios de y papel.

4.9. Evento de seguridad de la información: Es la ocurrencia identificada de un estado del activo de información (sistema, servicio, red, entre otros) que indica un incumplimiento posible de la política de seguridad de la información, una falla de controles existentes, o una situación previamente desconocida que puede ser pertinente para la seguridad

4.10. Incidente de seguridad de la información: Uno o una serie de eventos de seguridad de la información indeseados o inesperados que afecta un activo de información y que tienen una probabilidad significativa de comprometer las operaciones del negocio y/o amenazar la seguridad de la información asociada con el mismo.

4.11. Integridad: Propiedad de salvaguardar la exactitud y estado completo del activo de información, de acuerdo a los diferentes métodos de proceso a que se exponga.

4.12. Perímetro de seguridad física: Corresponde a un mecanismo o división implementada e identificable, que permite limitar o aislar un área segura o crítica de la organización con el propósito de brindar niveles de seguridad adecuados para el acceso o restricción al área respectiva.

4.13. Procesamiento de Información: Es la capacidad que tiene un sistema de información de efectuar cálculos con base a una secuencia de operaciones preestablecidas y permitiendo la transformación de datos fuentes en información para ser utilizada en la toma de decisiones.

4.14. Programa de concientización en seguridad de la información: Conjunto de estrategias que busca que todos los Colaboradores de la Compañía y los Colaboradores provistos por terceras partes interioricen y adopten las políticas, normas, procedimientos y guías existentes al interior de la Institución dentro de sus labores diarias.

4.15. Propietario: Se refiere al dueño responsable del activo de información utilizado para el desarrollo y cumplimiento de sus funciones. Está encargado de garantizar la seguridad adecuada del mismo, con base a los principios básicos de seguridad a saber: confidencialidad, integridad y disponibilidad.

4.16. Proteger la organización: Reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste ocurre.

4.17. Riesgo: Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas, legales o de imagen para la organización por deficiencias, fallas o al no adecuado uso y/o manejo del activo de información, a causa de amenazas o vulnerabilidades que le altere su correcto funcionamiento u operatividad.

4.18. **Seguridad de la información**: Preservación fundamental de la confidencialidad, integridad y disponibilidad del activo de información, además de otros criterios o propiedades tales como la autenticidad, no repudio, confiablidad, propiedad y/o responsabilidad, entre otros.

4.19. **Sistema de Información**: Es una disposición de personas, actividades o procedimientos y recursos tecnológicos integrados entre sí, para apoyar y mejorar las operaciones diarias de la organización, con la finalidad de satisfacer las necesidades de información en general y facilitar la toma de decisiones por parte de los directivos de la organización. Ejemplos aplicados: sistemas de automatización de oficina, sistemas de procesamiento de transacciones y sistemas de información de gestión.

4.20. **Software malicioso**: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

4.21. **Tratamiento del riesgo**: Proceso de selección e implementación de controles o acciones para ajustar el nivel de riesgo del activo a los niveles aceptables para la Organización.

4.22. **Vulnerabilidad**: Es la debilidad o incapacidad de resistencia de un activo de información frente a una amenaza.

5. LINEAMIENTOS

5.1. Generales

- La información y sistemas de cómputo de SERVICIOS AMBIENTALES S.A. ESP son activos esenciales para el desarrollo de las operaciones del negocio y su dependencia en estos activos exige que se mantengan protegidos.
- El presente lineamiento define, establece y hace obligatorio el cumplimiento de las siguientes medidas apropiadas para proteger los sistemas de cómputo de la información de SERVICIOS AMBIENTALES S.A. ESP contra la destrucción accidental o maliciosa, daño, modificación o revelación, para así mantener los niveles apropiados de confidencialidad, integridad y disponibilidad de la información contenida en los sistemas de cómputo y de información de la compañía.
- Todos los equipos de cómputo y sistemas de información proporcionados por SERVICIOS AMBIENTALES S.A. ESP permanecen como propiedad exclusiva de SERVICIOS AMBIENTALES S.A. ESP. Cualquier información o propiedad intelectual creada por el usuario permanece como propiedad de SERVICIOS AMBIENTALES S.A. ESP y no debe ser retirada, copiada o compartida, excepto para el cumplimiento de sus funciones y bajo autorización expresa del líder inmediato del proceso.
- Los sistemas de cómputo de SERVICIOS AMBIENTALES S.A. ESP y toda la información contenida en ellos son activos esenciales para las operaciones de la compañía y su uso inadecuado o abuso por parte de un colaborador será, a discreción de SERVICIOS AMBIENTALES S.A. ESP, objeto de acciones disciplinarias de conformidad con el procedimiento

establecido por la compañía.

- Los usuarios deben utilizar los sistemas de información de SERVICIOS AMBIENTALES S.A. ESP y los dispositivos de comunicación de manera apropiada, legitima y consistente según sus obligaciones, con respeto hacia los demás colaboradores, clientes y/o terceros. Estos dispositivos deben ser usados de acuerdo a este lineamiento y cualquier otra directriz, procedimiento, instructivo y/o estándar definido por la compañía para tal fin.
- El uso de los sistemas de cómputo de SERVICIOS AMBIENTALES S.A. ESP facilita a los colaboradores el desempeño de sus funciones garantizando el correcto almacenamiento de la información. Su uso podrá tener características o límite de colaboradores, según se contempla en los términos de estos lineamientos y está a la absoluta discreción de SERVICIOS AMBIENTALES S.A. ESP y ningún usuario puede esperar o reclamar tal uso personal como un derecho o esperar que tal uso sea privado.
- El colaborador y/o usuario se compromete a no divulgar la información suministrada por la compañía por ningún medio electrónico, magnético u otros. En consecuencia, se obliga a no utilizar los sistemas de información y/o cómputo para ningún objeto diferente al de adelantar las tareas que se deriven directamente del cumplimiento del vínculo contractual adquirido con la compañía.

5.2. Especificas

5.2.1. Revisión de los lineamientos de Seguridad de la Información

Los lineamientos de seguridad de la información deben tener un dueño, responsable de las actividades de desarrollo, evaluación y revisión de los mismos. La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros: organizacionales, normativos, legales, tecnológicos.

El comité de seguridad de la Información debe revisarlos anualmente y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizados los lineamientos. Además, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como, por ejemplo, cambios tecnológicos, variación del costo de los controles o el impacto de los incidentes de seguridad.

5.2.2. Lineamientos de la compañía de seguridad de la información

Los lineamientos específicos de seguridad de la información se fundamentan en los dominios y objetivos de control de la norma NTC-ISO/IEC 27001:2013.

A continuación, se enuncian las medidas necesarias para garantizar la protección de la información en SERVICIOS AMBIENTALES S.A. ESP.

5.2.2.1. Organización de la seguridad de la información

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de SERVICIOS AMBIENTALES S.A. ESP

5.2.2.2. Organización interna

Dando continuidad al compromiso de la dirección con la seguridad de la información, se aprueba la creación de los siguientes componentes en la compañía:

- Asignación de un responsable de la seguridad de la información (Coordinador de Tecnología).
- Comité Interdisciplinario de seguridad de la Información: SGC, TI y control interno.
- Asignación de responsabilidades asociadas a la seguridad de la información de acuerdo al cargo dentro de la compañía y las funciones del mismo.

a. Funciones del Comité de Seguridad de la información

El comité de seguridad de la información estará conformado por el coordinador de tecnología (o quien haga sus veces) y miembros de alto nivel de los procesos de SERVICIOS AMBIENTALES S.A. ESP. El comité deberá cumplir de forma organizada y coherente con las siguientes funciones:

- Debe revisar el estado general de la seguridad de la información periódicamente.
- Revisar y monitorear los incidentes de seguridad de la información.
- Revisar y aprobar los proyectos de seguridad de la información.
- Aprobar las modificaciones o nuevos lineamientos de seguridad de la información.
- Aprobar y participar activamente en la implantación de la

cultura de seguridad de la información en la compañía.

- Coordinación de la seguridad de la información
- La gerencia de SERVICIOS AMBIENTALES S.A. ESP es responsable de que los colaboradores de alto nivel bajo su cargo, conozcan y apliquen los lineamientos de seguridad de la información y realicen una adecuada retroalimentación a sus grupos de trabajo.
- SERVICIOS AMBIENTALES S.A. ESP, deberá contar con un coordinador de tecnología que asuma las tareas y responsabilidades que conlleva este rol en la compañía.

b. Roles y Responsabilidades

b.1 Gerencia General

- Dirección estratégica e impulso a la seguridad de la información.
- Definir los objetivos estratégicos.
- Compromiso en la asignación de recursos
- Aprobación de los lineamientos, mecanismos de supervisión y métricas
- Supervisar el cumplimiento de las obligaciones regulatorias
- Definir y desarrollar el plan de seguridad de la información.

b.2 Líderes de proceso

- Participar activamente en la implementación de los programas de seguridad de la información.
- Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del programa.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Compromiso en la asignación de recursos

b.3 Oficial de Seguridad de la Información o quien haga sus veces

- Definir y desarrollar el plan de seguridad de la información.
- Definir y actualizar los lineamientos, normas, procedimientos y estándares del Sistema de Gestión de Seguridad de la Información.
- Definir una metodología de riesgo adecuada y alineada con la estructura organizacional.
- Realizar el análisis de riesgo de los procesos críticos del negocio.
- Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio

- Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información
- Emitir lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios
- Promover la formación, educación y el entrenamiento para fortalecer la cultura de seguridad de la información al interior de la compañía.
- Mantenerse actualizado ante la evolución de las amenazas yvulnerabilidades existentes y las nuevas que surjan.
- Realizar estudios de penetración y pruebas de seguridad en todos los ambientes (Desarrollo, pruebas, producción y contingencia)
- Desarrollar e implementar el enfoque de monitoreo.
- Garantizar la identificación y cierre de las brechas.
- Desarrollar métodos y métricas para evaluar el rendimiento del SGSI.

b.4 Administradores de los sistemas de información

Los administradores de los diferentes sistemas deben en forma activa implementar las normas, estándares, formatos y procedimientos, para brindar un nivel apropiado de seguridad de la información.

b.5 Colaboradores (Colaborador directos o en misión)

Los colaboradores son responsables del cumplimiento de los lineamientos de seguridad de la información. Adicionalmente cada colaborador tiene el compromiso de reportar al oficial de seguridad cualquier incidente de seguridad de la información del que tenga conocimiento.

b.6 Contratistas, proveedores y terceros

Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir los lineamientos de la seguridad de la información de SER AMBIENTAL S.A.. E.S.P.

b.7 Custodio

Tienen la responsabilidad de monitorear el cumplimiento de las actividades encargadas.

b.8 Usuario o Propietario

Debe verificar la integridad de la información y velar por que se mantenga la disponibilidad y confiabilidad de la misma.

c. Asignación de responsabilidades para la seguridad de la información.

Las responsabilidades de la seguridad de la información están definidas y asignadas de acuerdo a la clasificación dada a la información.

c.1 Segregación de las tareas

La responsabilidad de la información deberá estar en cabeza de una sola persona para evitar conflicto en cuanto a responsabilidades. Lo anterior permite reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de la compañía.

c.2 Contacto con las autoridades

Se mantendrán los contactos apropiados con las autoridades pertinentes, en caso de encontrar violación al presente lineamiento de seguridad de la información.

Las siguientes autoridades listadas corresponden a las entidades competentes en caso de que se presentara un incidente de cualquier índole que pusiera en riesgo la confidencialidad, integridad, disponibilidad y privacidad de la información. En caso de requerirse el llamado a las autoridades mencionadas, sólo podrán hacerlo los funcionarios encargados.

Descripción	Organización	Contacto
Acceso abusivo a sistemas informáticos	Centro Cibernético Policial (CCP)	http://www.ccp.gov.co/
Violación de Datos personales		
Uso de Software malicioso		
Suplantación de Sitios Web		
Transferencia no consentida de activos		
Hurto por medios informáticos		
Phishing		
Ingeniería Social		

Respuesta a Emergencias Cibernéticas de Colombia	COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	www.colcert.gov.co/
Atención a incidentes de seguridad informática colombiano	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co
Emergencia por Incendio	Bomberos	119
Robo	Policía Nacional	112
Antisecuestro y Antiextorsión	Gaula	165
Siniestros ambientales	Defensa Civil	144
Incidentes Laborales	Cruz Roja	132
Incidentes laborales	Centro Toxicológico	136
Robo	Dijin	157

c.3 Contacto con grupos de interés especial

Se mantendrán los contactos apropiados con los grupos de interés especial (Policía, Bomberos, Defensa Civil) u otros foros de seguridad especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información.

El oficial de seguridad de la información, será el encargado de coordinar los conocimientos disponibles en SER AMBIENTAL S.A.. E.S.P., a fin de brindar ayuda en la toma de decisiones en materia de seguridad, éste podrá obtener asesoramiento de otros organismos.

Se debe mantener contacto permanente con las universidades, los grupos de investigación, entidades del gobierno y proveedores de tecnología que trabajan en pro de mantener actualizado a las personas que se desarrollan dentro del ámbito de la tecnología, para de esta manera mantenerse al tanto en amenazas, incidentes y soluciones.

Grupo de interés
Ministerio de Tecnologías de la Información y las comunicaciones
Microsoft
Fortinet

ESET- Consejos de seguridad para el uso seguro del ordenador y de la información sensible y personal -Alertas ESET
www.welivesecurity.com
https://managedprotection.pandasecurity.com

5.2.3. Dispositivos móviles y trabajo Remoto

Objetivo: Garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.

5.2.3.1. Lineamiento de uso de dispositivos para movilidad

El uso de los equipos portátiles fuera de las instalaciones del SERVICIOS AMBIENTALES S.A. ESP únicamente se permitirá a usuarios autorizados por la gerencia general o gerencia del proceso, previa solicitud de la dependencia respectiva. Éstos se protegerán mediante el uso de los siguientes controles tecnológicos:

- Antivirus.
- Cifrado de datos.
- Deben cumplir con el procedimiento de copias de seguridad y restauración

Todos los dispositivos móviles propiedad de SER AMBIENTAL S.A.. E.S.P o del usuario que lo ponga a disposición de la compañía, debe estar inventariado.

El personal que haga uso del dispositivo móvil (Celular) para almacenar o acceder a la información de SERVICIOS AMBIENTALES S.A. ESP deberá:

- Solicitar al proceso de TI la autorización para ello, aceptando el cumplimiento de la política de dispositivos móviles.
- Aceptar las configuraciones de seguridad del dispositivo y estas no podrán modificarse mientras se acceda o almacene información de SERVICIOS AMBIENTALES S.A. ESP .
- Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.
- Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.
- Es necesario realizar el cifrado del dispositivo móvil.
- En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la SERVICIOS AMBIENTALES S.A. ESP , se debe reportar la perdida a la Oficina de TI lo más pronto posible.

- En cualquier momento el equipo de Seguridad de la Información SERVICIOS AMBIENTALES S.A. ESP podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.

5.2.3.2. Trabajo Remoto

Cualquier colaborador de SERVICIOS AMBIENTALES S.A. ESP autorizado para tener acceso a la información de la compañía desde redes externas, podrá acceder remotamente mediante un proceso de autenticación; uso de conexiones seguras. Lo anterior asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

El trabajo remoto para cualquiera de los colaboradores de la compañía debe estar autorizado por el jefe inmediato y gerente de TI (o quien haga sus veces), a su vez, el colaborador debe solicitar el acceso por los canales autorizados indicando los siguientes datos:

- Nombre del colaborador
- Cargo del colaborador
- Razón por la que se requiere el Trabajo remoto
- Fecha desde cuándo se requiere el Trabajo remoto
- Fecha hasta cuando se hará uso del Trabajo remoto
- Definir los días de la semana y el horario en el que se hará uso del Trabajo remoto
- Especificar las aplicaciones que van a ser usadas

El jefe inmediato debe validar que los requerimientos solicitados están acordes a las funciones asignadas en el rol correspondiente.

Una vez tenga la autorización respectiva para realizar trabajo remoto deberá solicitar al proceso de TI de SERVICIOS AMBIENTALES S.A. ESP :

- Solicitar la instalación del Cliente VPN utilizado SERVICIOS AMBIENTALES S.A. ESP .
- Solicitar el usuario y contraseña para la conexión VPN.

El colaborador que haga uso de teletrabajo debe tener en cuenta las siguientes recomendaciones:

- No realizar conexiones desde un sitio de acceso público como un Café Internet, Aeropuerto y Restaurante, entre otros.
- Se deben considerar los requerimientos de seguridad definidos en Seguridad de la Información para los activos de información involucrados, es decir aplicar todas las

restricciones y protecciones para la confidencialidad, integridad y disponibilidad definidas.

- Reportar cualquier evento anormal al proceso de TI

5.2.4. Seguridad de los recursos humanos

5.2.4.1. Antes de la contratación

Objetivo: Asegurar que los Colaboradores y contratistas entiendan sus responsabilidades y que estas son adecuadas para las funciones que realizan.

a. Investigación de antecedentes

Se realiza la verificación de antecedentes y estudio de seguridad de acuerdo al procedimiento de selección de personal que este alienado con el reglamento interno de trabajo y las leyes y normas y regulaciones del estado colombiano.

b. Términos y condiciones de contratación

Los acuerdos contractuales con los Colaboradores y los contratistas deberán establecer las responsabilidades establecidas por SER AMBIENTAL S.A. E.S.P.en el cumplimiento de la presente Lineamientos de Seguridad de la Información.

5.2.4.2. Durante la contratación y/o empleo

Objetivo: Asegurar que los colaboradores y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.

La capacitación en seguridad de la información es obligatoria para todo el personal que ingrese vinculado de manera temporal y/o indefinida. Se deberá asistir de manera obligatoria durante su inducción, a las charlas que sobre los requerimientos de seguridad de la información se dicten.

a. Responsabilidades de gestión

La gerencia general o su delegado pedirán a todos los colaboradores y contratistas, aplicar la seguridad de la información de acuerdo con las lineamientos y procedimientos establecidos por la compañía. Todos los colaboradores y/o contratistas tendrán acceso permanente a los lineamientos que se obligan a cumplir.

Todos los Colaboradores deben firmar un Acuerdo de Confidencialidad por cumplimiento de los lineamientos de

seguridad de la información, antes de otorgarles su identificación de usuario y contraseña para el uso de los recursos informáticos.

El personal que ingrese vinculado de manera temporal y/o indefinida a la compañía, deberá firmar que conoce y acepta lo definido en la Lineamientos de Seguridad de la información de manera obligatoria.

b. Proceso disciplinario

Se solicitará proceso de descargos contra los colaboradores que hayan cometido una violación de la seguridad de la información, según corresponda la investigación será tramitada por relaciones laborales.

5.2.4.3. Terminación o cambio de empleo

Objetivo: Proteger los intereses de la compañía como parte del proceso de terminación o cambio el empleo**.**

a. Terminación o cambio de puesto de trabajo

Las responsabilidades de seguridad de la información y deberes que siguen vigentes después de la terminación o cambio de empleo, se deben definir y comunicarse al colaborador o contratista y se deben hacer cumplir.
Es responsabilidad de gestión humana asegurar que en el evento de la terminación y/o cambio de cargo al interior de la compañía, el colaborador hace la devolución de todos los activos de información y elementos asignados al jefe inmediato o a la persona encargada por éste, junto con la copia de la información crítica que maneja. La vigencia de los derechos de acceso y su revocatoria, debe estar estrechamente relacionados con la terminación de la relación laboral.

Después que un colaborador se ha retirado de la compañía, su ingreso a la misma sólo lo podrá hacer como visitante.

Gestión humana debe informar de manera inmediata al administrador de los sistemas de información que utiliza, del retiro o cambio de actividades del colaborador en la compañía para la eliminación o reasignación de derechos de acceso sobre los recursos informáticos y sistemas de información. Además, debe informar al personal encargado de la vigilancia y seguridad de SERVICIOS AMBIENTALES S.A. ESP del retiro del Colaborador para prevenir el acceso físico no autorizado a las instalaciones de la Compañía.

5.2.5. Gestión de activos

5.2.5.1. Responsabilidad sobre los activos

Objetivo: Identificar los activos de la compañía y definir las responsabilidades de protección adecuados.

Todos los activos de información en SER AMBIENTAL S.A.. E.S.P.serán clasificados según el contenido y los controles adecuados serán implementados de acuerdo a su importancia en la compañía.

5.2.5.2. Inventario de activos

Los activos relacionados con la información y las instalaciones de procesamiento de información deben ser identificados dentro del inventario de activos de información de SER AMBIENTAL S.A.. E.S.P.

5.2.5.3. Propiedad de los activos

Los activos de información mantenidos en el inventario son de propiedad de SERVICIOS AMBIENTALES S.A. ESP. Todos los activos de información están sujetos a revisiones periódicas por parte de Control Interno o por los colaboradores que SER AMBIENTAL S.A.. E.S.P.delegue para tal fin.

5.2.5.4. Uso aceptable de los activos

Las normas para el uso aceptable de la información y de los activos asociados a la información y las instalaciones de procesamiento de información están identificadas en el presente documento y deben cumplirse de forma obligatoria por sus responsables.

5.2.5.5. Devolución de los activos

Todos los colaboradores y contratistas deberán devolver todos los activos de la compañía en su poder a la terminación de su contrato, a su vez se debe garantizar que fueron entregados cumpliendo con los lineamientos.

5.2.6. Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel adecuado de protección, de acuerdo con su importancia para

SERVICIOS AMBIENTALES S.A. ESP .

5.2.6.1. Directrices de clasificación

La información se clasificará en función de los requisitos legales, el valor, criticidad y sensibilidad a la divulgación o modificación no autorizada. Todos los activos de información serán clasificados según el contenido y los controles adecuados serán implementados de acuerdo a su importancia en la compañía.

Esta clasificación será realizada por el responsable de la misma, teniendo en cuenta: Su valor relativo, su privacidad, sensibilidad, el nivel de riesgo a que está expuesta y/o requerimientos legales de retención.

Si la información clasificada de SERVICIOS AMBIENTALES S.A. ESP debe ser entregada a contratistas, asociados y terceros por efectos del negocio, previamente se deben firmar los acuerdos de confidencialidad respectivos, que incluyan el seguimiento y cumplimiento de las prácticas de gestión segura de la Información al tenor de lo establecido en los lineamientos.

5.2.6.2. Etiquetado y manipulado de la información

El etiquetado de la información será aplicado de acuerdo con el esquema de clasificación de la información aprobada por la compañía, lo anterior teniendo en cuenta las Tablas de Retención Documental aprobadas para las diferentes áreas.

5.2.6.3. Manejo de activos

Se aplicarán los procedimientos para el manejo de los activos de conformidad con el esquema de clasificación de la información aprobada por SERVICIOS AMBIENTALES S.A. ESP .

5.2.7. Manejo de medios de almacenamiento

Objetivo: Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de almacenamiento.

5.2.7.1. Gestión de soportes removibles

- EL uso de medios removibles estará autorizado para aquellos colaboradores que para el cumplimiento de sus funciones así lo requieran.
- Los jefes de proceso serán los encargados de informar al proceso de TI, quienes son los funcionarios autorizados para

el uso de medios removibles.

- El procedo de TI será el encargado de llevar el control de estos medios, de acuerdo a las autorizaciones allegadas por cada proceso.
- El funcionario es el responsable de mantener asegurada la información, libre de software malicioso y cifrada si es información confidencial, sin poner en riesgo a la compañía.
- El funcionario velará por el buen uso de la información, su divulgación y distribución.
- En caso de pérdida de algún tipo de medio, debe ser reportado al proceso de TI, informando el nivel de importancia de la información.
- En caso de ser transportados se deben proteger contra el acceso no autorizado o uso indebido.
- El manejo de la información en medios removibles está expuesta a riesgos, como pérdida, fuga o modificación, que compromete no solamente la información sino también la infraestructura tecnológica de SERVICIOS AMBIENTALES S.A. ESP , por lo tanto, el colaborador que los use será quien asuma las sanciones de ley aplicables en esta materia, siendo responsable de la seguridad del tipo y el tiempo de uso de la información en estos medios.
- El Colaborador es responsable de la información en los medios removibles en todo momento y lugar.
- Los medios de almacenamiento removibles deben ser de uso temporal y el colaborador deberá transferir la información institucional a los medios que SERVICIOS AMBIENTALES S.A. ESP ha establecido para este propósito (computadores, NAS).
- El cifrado debe realizarse antes de que el dispositivo esté en uso, para evitar la pérdida de la información y daño de este.
- Los equipos de cómputo que tienen autorizado el manejo de USB y unidades reproductoras de CD/DVD, deben cumplir los siguientes requisitos.
- Tener habilitado el escaneo automático de virus
- Tener configurada en la herramienta de antivirus, el bloqueo de la reproducción automática de archivos ejecutables

5.2.7.2. Eliminación y/o borrado seguro de soportes.

La información será eliminada y/o borrada de los medios de almacenamiento de forma segura cuando ya no sea necesaria, utilizando los pasos descritos mediante el lineamiento de borrado seguro.

5.2.7.3. Soportes físicos en tránsito

Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte.

5.2.8. Requisitos de negocio para el Control de acceso

Objetivo: Limitar el acceso a las instalaciones de procesamiento de la información y de la información.

5.2.8.1. Lineamientos de Control de accesos

SERVICIOS AMBIENTALES S.A. ESP garantiza entornos con controles de acceso idóneos, los cuales aseguran el perímetro, tanto en oficinas, recintos, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

Los colaboradores que son responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- Las áreas de producción se catalogan como seguras y deben permanecer cerradas y/o custodiadas.
- El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas.
- El acceso a áreas seguras requiere esquemas de control de acceso, como llaves o candados.
- Debe existir mecanismos de revisión y control del ingreso de cualquier tipo de material al centro de datos y al centro de cableado.

Debido a las obligaciones de la Compañía en atención de PQRS, se requiere tener zonas de atención al público para el ciudadano. En estas zonas se hace recepción y entrega de información por parte de los Colaboradores de la compañía a los usuarios del servicio.

5.2.8.2. Control de acceso a las redes y servicios asociados

Los usuarios que dispongan de acceso y servicios de la red son los que han sido específicamente autorizados para su uso. Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de SERVICIOS AMBIENTALES S.A. ESP . Por lo tanto, la identidad de cada usuario de los recursos de información está establecida por el nombre del usuario. Esta identidad de ninguna manera o por ninguna circunstancia podrá

ser compartida. El sobrepaso a este medio será tratado como una infracción a seguridad de la información.

5.2.9. Gestión de acceso de usuario

Objetivo: Asegurar el acceso de los usuarios autorizados para evitar el ingreso no permitido a los sistemas y servicios.

5.2.9.1. Gestión de altas y bajas en el registro de usuarios

Se llevará a cabo un proceso formal de registro y anulación de usuario para permitir la asignación de derechos de acceso. La eliminación de un identificador de usuario debe ser realizada inmediatamente haya finalizado su relación contractual del usuario con SERVICIOS AMBIENTALES S.A. ESP.

5.2.9.2. Gestión de los derechos de acceso asignados a los usuarios.

El acceso a la información de SERVICIOS AMBIENTALES S.A. ESP, es otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad o tipo de servicio. El acceso a los recursos de información de la compañía, es restringido en todos los casos sin excepción, y se da específicamente a quienes lo requieran en razón de sus funciones, con los privilegios apropiados.

Se debe identificar y autenticar a cualquier usuario que, de manera local o remota, requiera utilizar los recursos de operación y tecnología de SERVICIOS AMBIENTALES S.A. ESP, para lo que se requiere contar con sistemas de seguridad que cumplan con las siguientes características:

- Debe estar activo para acceder a la plataforma tecnológica y de operación de SERVICIOS AMBIENTALES S.A. ESP, lo que significa que cada usuario tiene que identificarse y autenticarse antes de acceder a un recurso de tecnología por medio de un usuario y una contraseña.
- Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.
- Los eventos de ingreso y autenticación de usuarios serán registrados y monitoreados por los responsables de la información.
- Los usuarios deben cumplir prácticas como las recomendadas para la selección y uso de las contraseñas donde deben contener una mayúscula, números y letras.

Únicamente el responsable de la información, puede autorizar la creación de un usuario, este identificador de usuario debe ser asociado sólo a un individuo y la solicitud debe obedecer a una razón legítima de la operación.

5.2.9.3. Gestión de derechos de acceso privilegios especiales

La asignación y utilización de los derechos de acceso preferente se deberá restringir y controlar.

- El uso de las claves de usuarios administradoras, tales como: "root", "administrador" y "admin", entre otros, deben ser controladas acorde como lo establece este lineamiento.

5.2.9.4. Gestión de información confidencial de autenticación de los usuarios

La asignación de la información secreta de autenticación se controla a través de un proceso de gestión formal y de acuerdo a la clasificación dada a los activos por parte de los responsables.

5.2.9.5. Revisión de los derechos de acceso de los usuarios

Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares. Cualquier desviación será tratada como un incidente en seguridad de la información.

Los responsables deben dejar trazas del ejercicio de esta actividad, las que serán objeto de revisiones de parte de SERVICIOS AMBIENTALES S.A. ESP.

5.2.9.6. Retirada o adaptación de los derechos de acceso

Los derechos de acceso de todos los colaboradores y/o contratistas de la información e instalaciones de informática serán retirados en el momento de retiro de su empleo y/o terminación de contrato.

5.2.10. Responsabilidades del usuario

Objetivo: Hacer que los usuarios responsables de salvaguardar su información se autentiquen.

5.2.10.1. Uso de la información confidencial para la autenticación

Se exigirá a los usuarios que sigan prácticas de la compañía en el uso de información secreta de autenticación.

5.2.11. Control de acceso a sistemas y aplicaciones

Objetivo: Evitar el acceso no autorizado a los sistemas y aplicaciones.

SERVICIOS AMBIENTALES S.A. ESP tiene establecidos controles de acceso lógico para los activos de información (usuario y contraseña); El acceso en los sistemas de información de SER AMBIENTAL S.A.. E.S.P.debe hacerse únicamente por los aplicativos y sistemas autorizados.

5.2.11.1. Restricción del acceso a la información

El acceso a la información estará restringido de conformidad con los lineamientos de control de acceso.

5.2.11.2. Procedimientos seguros de inicio de sesión.

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro utilizando usuario y contraseña.

5.2.11.3. Sistema de gestión de contraseñas

Junto con el usuario, el colaborador recibirá una contraseña o clave para acceder a los recursos informáticos de la entidad. Dicha contraseña debe tener una longitud mínima de 8 (ocho) caracteres alfanuméricos, diferentes a nombres propios o cualquier otra palabra de fácil identificación.

Por seguridad se recomienda el cambio de dichas claves con una periodicidad de 90 (Noventa) días. Para el sistema de información AIDA el cambio de contraseña es dado por el director de TI, quien es el administrador de este sistema de información.

Se prohíbe el uso de contraseñas compartidas. La contraseña es personal e intransferible. Las contraseñas nunca serán modificadas telefónicamente.

5.2.11.4. Uso de herramientas de administración de sistemas

El uso de programas de utilidad que podrían ser capaces de anular el sistema y de aplicaciones con controles principales será

restringido y estrechamente controlado.

5.2.11.5. Control de acceso al código fuente de los programas

El acceso al código fuente del programa es limitado. Solamente los ingenieros del grupo de desarrollo podrán contar con acceso a esta información y harán uso de la misma.

5.2.11.6. Control de elementos de protección de equipos

Es responsabilidad del usuario mantener asegurados los equipos portátiles con guayas de seguridad que fueron suministradas a cada uno de los usuarios de este tipo de dispositivos.

5.2.12. Cifrado

5.2.12.1. Controles criptográficos

Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

5.2.12.2. Lineamientos sobre el uso de controles criptográficos

Se deben utilizar controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera la compañía.
- Para el uso equipos celulares realizada por el propietario de la información y el responsable de seguridad informática lo requieran.
- Para el uso equipos portátiles realizada por el propietario de la información y el responsable de seguridad informática lo requieran.
- Para el resguardo de información, cuando surja de la evaluación de riesgos realizada por el propietario de la información y el responsable de Seguridad Informática.

5.2.12.3. Administración de claves

Los lineamientos sobre uso, protección y duración de las claves criptográficas se realizan a través de las opciones del aplicativo y la custodia será del propietario de la información.

5.2.13. La seguridad física y del entorno

5.2.13.1. Áreas seguras

Objetivo: Evitar el acceso físico no autorizado, daños e interferencia para la información de la compañía y las instalaciones de procesamiento de información.

5.2.13.2. Perímetro de seguridad física

El perímetro de las áreas que contienen la información y sus instalaciones de procesamiento, bienes sensibles o críticos estarán protegidos de acceso no permitidos.

5.2.13.3. Controles físicos de entradas

- Las áreas seguras se protegerán mediante controles de entrada adecuados para garantizar que se le permita el acceso únicamente al personal autorizado.
- Para el ingreso de terceros al centro de cómputo, se tienen que registrar en la bitácora ubicada en un lugar visible a la entrada a este lugar.
- Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los colaboradores se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.
- Todos los colaboradores deben permanecer con el carnet que los identifica como colaborador de SERVICIOS AMBIENTALES S.A. ESP mientras permanezcan en las instalaciones.
- Todos los colaboradores deben reportar, a la mayor brevedad, cualquier sospecha de pérdida o robo de carnet de identificación.
- Todos los visitantes que ingresan a la compañía, deben ser recibidos y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones del mismo.
- Todos los visitantes que ingresan a la compañía deben cumplir con los procedimientos de ingreso a las instalaciones, en donde se establece el uso del formato para registrar los datos personales, hora de ingreso y salida.

5.2.13.4. Seguridad de oficinas, despachos, salas e instalaciones

- El ingreso de terceros al centro de cómputo debe estar debidamente registrado mediante una bitácora y con compañía del coordinador de tecnología (o quien haga sus veces).
- El Centro de Cómputo debe estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.
- Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deben ser realizados por personal especialista y debidamente autorizado e identificado.
- Se deben realizar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y del sistema de aire acondicionado.
- Se deben realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de SERVICIOS AMBIENTALES S.A. ESP .
- Se debe realizar mantenimiento preventivo y correctivo de las estaciones de trabajo y equipos portátiles con periodos establecidos de manera que conserve la disponibilidad, integridad y confidencialidad de la información contenida en los mismos.
- Se deben tener extintores debidamente aprovisionados, con carga vigente y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.

5.2.13.5. Seguridad de los Equipos

a. Ubicación y Protección del equipo

Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado.

b. Servicios Públicos de soporte

El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos.

c. Seguridad del cableado

El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la intercepción, interferencia o daños.

d. Mantenimiento de los equipos

Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad.

e. Salida de los activos fuera de las dependencias

Los equipos, la información o el software no se sacarán del lugar sin la previa autorización del propietario de la información o del jefe del proceso respectivo.

f. Seguridad de los equipos y de los activos fuera de las instalaciones

Se aplicará seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la compañía.

g. Reutilización o eliminación segura de dispositivos de almacenamiento

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

h. Equipo sin supervisión de los usuarios

Los usuarios deberán asegurarse de que el equipo que no cuenta con vigilancia tenga la protección adecuada.

5.2.14. Lineamientos de escritorio limpio y bloqueo de pantalla

- Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla.
- Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, sobre todo en horas fuera de las normales de trabajo.
- Información confidencial y crítica para SER AMBIENTAL S.A..

E.S.P.debe ser asegurada preferiblemente en armarios resistentes a impacto, fuego e inundación.

5.2.15. Seguridad de las operaciones

5.2.15.1. Responsabilidades y Procedimientos de operación

Objetivo: Asegurar operaciones correctas y seguras de las instalaciones de procesamiento de información.

El proceso de TI, será la encargada de la operación y administración de la plataforma tecnológica (Voz y datos) que apoya los procesos de negocio, asignará funciones específicas a sus funcionarios y/o contratistas, quienes actuarán como responsables de garantizar la adecuada operación y administración de dicha plataforma, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de dichas actividades.

Documentación de Procedimientos de operación

Los procedimientos de operación deberán ser documentados y puestos a disposición de los usuarios que los necesitan.

El proceso de TI debe proveer a sus colaboradores de manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información (comunicaciones y servicios como correo, intranet, WEB) así como todos los componentes de la plataforma tecnológica de la entidad.

Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio en SERVICIOS AMBIENTALES S.A. ESP .

a. Gestión de cambios

SERVICIOS AMBIENTALES S.A. ESP a través del proceso responsable establecerá, coordinará y controlará los cambios realizados en los activos de información tecnológicos y los recursos informáticos, asegurando que los cambios efectuados sobre la plataforma tecnológica, tanto el software operativo como los sistemas de información, serán debidamente autorizados por los procesos correspondientes.

Se debe garantizar que todo cambio realizado sobre la plataforma tecnológica de SERVICIOS AMBIENTALES S.A. ESP , quedará

formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.

b. Gestión de capacidad

El uso de los recursos será supervisado. Se realizarán los pertinentes ajustes, y las proyecciones hechas de las futuras necesidades de capacidad, para asegurar el rendimiento del sistema requerido.

c. Separación de entornos de desarrollo, prueba y producción

El desarrollo, las pruebas y la producción deberán estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo. Se debe garantizar los recursos necesarios que permitan la separación de ambientes de desarrollo, pruebas y producción.

5.2.16. Protección contra código malicioso

Objetivo: asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra el malware.

5.2.16.1. Controles contra el código malicioso

Se aplicarán controles de detección, prevención y recuperación para evitar códigos maliciosos, en combinación con el conocimiento del usuario correspondiente.

SERVICIOS AMBIENTALES S.A. ESP proveerá los recursos necesarios que garanticen la protección de la información y los recursos de procesamiento de la misma, adoptando controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por la contaminación y/o el contagio de software malicioso.

5.2.16.2. El proceso de TI debe garantizar:

- El software usado para la mitigación de virus informáticos cuenta con las licencias de uso aprobadas, garantizando su autenticidad y su periódica actualización.
- La información almacenada en los activos de información

tecnológicos que es transportada por la red de datos, es escaneada con una periodicidad establecida de 6 meses, para garantizar así la seguridad de la misma.

- Los usuarios de los activos de información tecnológicos no pueden modificar la configuración establecida para el software antivirus.
- Los usuarios de activos de información tecnológicos y recursos informáticos deben hacer uso exclusivo de hardware y software autorizado por los colaboradores del proceso de TI.
- Los usuarios de activos de información tecnológicos y recursos informáticos deben garantizar que las descargas de archivos adjuntos de los correos electrónicos o descargados de internet realizadas, provienen de fuentes conocidas, seguras y exclusivas de acuerdo con las funciones encomendadas.
- Los usuarios de activos de información tecnológicos y recursos informáticos deben correr el software antivirus sobre archivos y/o documentos que son abiertos y/o ejecutados por primera vez.
- Los usuarios de activos de información tecnológicos deben comunicarse con el proceso de TI al encontrar un virus, del cual no se sabe cómo eliminarlo, cómo actuar frente al mismo o de considerarlo necesario.

5.2.17. Copias de Seguridad Objetivo:

Evitar la pérdida de datos.

5.2.17.1. Copias de seguridad de la información

Las copias de seguridad de la información se prueban regularmente de acuerdo con lo definido en el presente lineamiento.

Los colaboradores responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de la misma. Los procesos encargados de la información en conjunto con el proceso de TI deberán definir la estrategia a seguir para el respaldo y almacenamiento de la información.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben definir en compañía del Proceso de TI, las estrategias para la correcta y adecuada generación, retención, y rotación de las copias de respaldo de la información.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben velar por el cumplimiento del procedimiento de Copias de Seguridad y Restauración.

El proceso de TI debe generar procedimientos para la correcta y segura generación, así como el adecuado tratamiento de las copias de respaldo.

La información que es salvaguardada por el proceso de TI de SERVICIOS AMBIENTALES S.A. ESP , deberá ser almacenada y respaldada interna y/o externamente a la entidad, de acuerdo con las normas establecidas de tal forma que se garantice su disponibilidad en cualquier momento.

Los administradores de los activos de información tecnológicos y recursos informáticos deben almacenar y respaldar las copias de seguridad según el procedimiento vigente, de tal forma que se garantice su confidencialidad, integridad y disponibilidad.
Se deben realizar todas las copias de respaldo de las bases de datos que contienen los sistemas de información y demás servicios, todos los días, esta tarea debe realizarse de forma automática.

5.2.18. Registro de actividad y supervisión Objetivo:

Registrar eventos y generar evidencia.

5.2.18.1. Registro y gestión de eventos de actividad

Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

5.2.18.2. Protección de los registros de información

Los registros de información se protegerán contra la manipulación y el acceso no autorizado.

5.2.18.3. Registros de actividad del administrador y operador del sistema

Las actividades del administrador del sistema y de la red serán registradas. Estos registros serán protegidos y regularmente revisados.

5.2.18.4. Sincronización de relojes

Asegurar la hora exacta de las transacciones de los servidores, para ello se utilizará el protocolo NTP en los servidores que le permite y soporte las transacciones electrónicas realizadas con otras entidades

5.2.19. Control de software operacional

Objetivo: Garantizar la integridad de los sistemas operativos.

5.2.19.1. Instalación del software en sistemas operativos

Los colaboradores son responsables por la instalación y utilización de software no autorizado en sus estaciones de trabajo y en las plataformas tecnológicas que soportan los sistemas de información de la compañía.

5.2.20. Consideraciones de las auditorías de los sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

5.2.20.1. Controles de auditoría de sistemas de información

Los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas operativos deberán ser cuidadosamente planificados y acordados para reducir al mínimo las interrupciones de los procesos.

5.2.21. Seguridad de las telecomunicaciones

5.2.21.1. Gestión de la seguridad en las redes

Objetivo: Garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.

5.2.21.2. Controles de red

Las redes deberán ser administradas y controladas para proteger la información en los sistemas y aplicaciones.

5.2.21.3. Mecanismos de Seguridad asociados a servicios en red

Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red.

5.2.21.4. Segregación de redes

SERVICIOS AMBIENTALES S.A. ESP debe establecer mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información en la entidad.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

5.2.22. Intercambio de información con partes externas

Objetivo: Mantener la seguridad de la información que se transfiere dentro de la compañía y con cualquier entidad externa.

5.2.22.1. Lineamientos y procedimientos de intercambio de información

Los lineamientos formales de transferencia, procedimientos y controles deberán estar en posición de proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

5.2.22.2. Acuerdos sobre la transferencia de información

Todas las actividades de transferencia de información se regirán por la ley de protección de datos personales 1581 de 2012.

5.2.22.3. Mensajería electrónica

La información involucrada en la mensajería electrónica será debidamente protegida. El correo electrónico es una herramienta de trabajo que facilita la comunicación entre los colaboradores y los proveedores, entidades de control y otras terceras partes interesadas. Se debe garantizar que sea utilizado de manera adecuada y racional para las funciones propias de la compañía,

respetando los principios de confidencialidad, integridad, privacidad y autenticidad de quienes realizan las comunicaciones.

El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

5.2.22.4. Lineamientos de uso de las Comunicaciones Electrónicas

Teniendo en cuenta que la compañía pone a disposición de sus trabajadores y colaboradores distintas herramientas de informática que deberán utilizarse para fines profesionales. Las directrices para el buen manejo de correo son las siguientes:

- La cuenta de correo que proporciona la compañía se destinará a uso profesional, no pudiéndose utilizar para fines particulares, excepto en casos puntuales justificados.
- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado a la compañía.
- Está prohibida la suscripción del correo electrónico corporativo a servicios de noticias no relacionados con la actividad profesional.
- Los mensajes y la información contenida en los buzones de correo son de propiedad de SER AMBIENTAL S.A.. E.S.P.. El usuario podrá crear un histórico de su correo siempre y cuando sea local (almacenado en el disco duro del usuario) y bajo su propia responsabilidad.
- El servicio de correo electrónico cuenta con respaldo de información (Back up) donde se resguardan los últimos 15 días.
- La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.
- Los correos electrónicos importantes para el desarrollo de las funciones de cada usuario deben guardarse en la carpeta “Trabajo” de acuerdo a lo establecido en Respaldo de la Información.
- Todos los colaboradores de la compañía que dispongan de una cuenta de correo corporativa seguirán las siguientes buenas prácticas:
- No facilitar la cuenta de correo a personas no autorizadas.
- No utilizar el correo corporativo con fines comerciales o financieros sin relación con la compañía.
- No participar en el envío de cadenas de mails.

- No distribuir mensajes con contenidos inapropiados (contenido ofensivo, homófobo, racista, discriminatorio, entre otros)
- No enviar grandes cadenas de chistes en forma interna y mucho menos si nos "equivocamos" y ponemos a nuestro jefe en ellas.
- No usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
- Utilizar el correo electrónico como una herramienta de trabajo, y no como nuestra casilla personal de mensajes a amigos y familiares.
- No enviar archivos de gran tamaño a compañeros de oficina, el tamaño deseable por cada correo es de 10 MB, el envío de archivos más grandes ocasiona el bloqueo del servidor. De requerirse se deberá solicitar a TI un método de intercambio de información.
- El máximo número de destinatarios de un correo debe ser 20 personas en total, los servidores externos como Hotmail, Yahoo, Gmail, entre otros. Pueden considerar los correos con demasiados destinatarios como SPAM y reportarnos en listas negra, evitando que los correos lleguen a sus destinatarios.
- No se permite enviar archivos con extensión .exe, .pif, .scr, .vbs, .cmd, .com,.bat, .hta debido a que este tipo de extensiones son propensas a ser utilizadas para propagación de virus. Estos tipos de archivos serán eliminados automáticamente por el sistema de correo.
- Si se recibe un correo de origen desconocido o dudoso, bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, entre otros.
- Los correos no deben contener información que pudiera ser interpretada como ámbito de ataque, discriminación o ilegalidad. Todo lo que escribamos bajo el dominio de la compañía, es en representación de la misma, y nuestras palabras podrían ser utilizadas de formas no previstas. Por eso, antes de cliquear en "Enviar". Releer el correo y corregir de ser necesario, tratando de "suavizar" cualquier frase.
- El acceso al servicio de mensajería instantánea es un permiso que la compañía otorgará a sus colaboradores o contratistas, el cual tiene consigo responsabilidades y compromisos para su uso. Constituyéndose en otro instrumento de trabajo no sólo dentro de la compañía sino externamente, en forma eficiente, ágil y económica; cualquier uso indebido del mismo puede afectar la operación y la buena marcha de las funciones de cada persona, por ende, se espera que los usuarios conserven normas de buen uso, confidencialidad y criterio ético. Para esto el uso apropiado del servicio de mensajería instantánea seguirán las siguientes buenas prácticas:

- El uso del servicio de mensajería instantánea de la compañía será exclusivamente para fines laborales.
- Abstenerse de compartir información o datos personales a través de este servicio. No es aconsejable incluir información personal como contraseñas o números de tarjetas de crédito, cuentas bancarias e incluso un número de teléfono en cierta manera confidencial.
- Compartir por medio de este canal mensajes concisos, breves y veraces.
- Los audios de no deben superar los 20 segundos si se exceden de este tiempo mejor realizar una llamada.

5.2.22.5. Lineamientos para el uso adecuado de Internet

Internet es un activo de la compañía suministrado a los colaboradores para contribuir con la actividad laboral. El uso personal ocasional o eventual de este recurso es permitido, en tanto no interfiera con la productividad del personal y no cause conflictos con la actividad de la compañía. Toda información transmitida por este medio será tratada como información relacionada a su trabajo y debe estar alineada a las normas enumeradas más adelante en este documento.

El personal que requiera el acceso a este tipo de sitos como parte de sus actividades, deberá previamente justificar la necesidad y obtener la autorización de su respectiva jefatura. En caso que el acceso a un sitio en particular esté deshabilitado deberá solicitar la apertura vía mail a julian.castano@serambiental.com

- Acceso a sitios Web relacionados con actividades de juego, apuestas, o actividades ilegales en general
- Acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía.
- Acceso a sitios de música, juegos, videos u otros sitios de entretenimientos on-line.
- Acceso a sitios Web de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, bromas de mal gusto, prejuicios, menosprecio o acoso explícito.

- Acceso a sitios de “hacking” o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información de la compañía.
- Descarga desde Internet de cualquier material (incluyendo software) protegido bajo leyes de derecho de propiedad, o archivos electrónicos para usos no relacionados con la actividad de la compañía. (Ej. Archivos de música o video).
- Publicación de cualquier tipo de información perteneciente a la compañía en sitios personales u otros, sin la autorización correspondiente del propietario de dicha información.
- Publicación de comentarios no profesionales en foros públicos, sitios de chat, Weblogs (Blogs), correo electrónico, o cualquier otro medio de publicación en Internet.
- Participación en cualquier actividad ilegal o criminal
- Solicitud no autorizada de dinero o la operación de negocios personales.
- Obtención de acceso no autorizado sobre otras computadoras pertenecientes a cualquier otra compañía o entidad.
- Instalación y uso de programas de tipo “peer-to-peer” para el intercambio de archivos en internet (Ej. Emule, Ares, bittorrent, utorrent entre otros.)

5.2.22.6. Restricciones complementarias:

- No deje su navegador abierto cuando no esté utilizando Internet, cierre la sesión. De esta manera evitará consumo de ancho de banda innecesario.
- Se deberá cumplir con las leyes y regulaciones sobre transmisión de datos y derechos de autor.
- No duplicar software licenciado o con derechos de autor a menos que se especifique explícitamente que está permitido.
- La descarga de software solo será permitida si el mismo está relacionado con el rubro de la compañía y siempre que se cumplan las siguientes condiciones:

  a. Deber ser autorizado previamente por su jefatura o la autenticidad del software está debidamente comprobada.
  b. Han sido investigadas y determinadas las condiciones para su uso (incluyendo tarifas de shareware), y estas condiciones han sido cumplidas.
  c. Que el software se instale de acuerdo a los lineamientos de seguridad correspondientes;
  d. El software fue examinado por una versión actualizada del antivirus estándar de SERVICIOS AMBIENTALES S.A. ESP .

La compañía monitorea todos los accesos a Internet, por lo tanto, esta herramienta deberá ser utilizada moderadamente cuando se trate de asuntos no relacionados con las actividades de SERVICIOS AMBIENTALES S.A. ESP .

5.2.22.7. Acuerdos de confidencialidad o de no divulgación

Se debe revisar, identificar y documentar regularmente los diferentes requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la Compañía para la protección de la información.

5.2.23. Adquisición, desarrollo y mantenimiento de los sistemas de información

5.2.23.1. Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

a. Análisis y especificación de los requisitos de seguridad.

Los requisitos relacionados con la seguridad de la información serán incluidos en los requerimientos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Los responsables de la provisión de soluciones deben crear y mantener una metodología que controle el ciclo completo de adquisición, desarrollo, mantenimiento y disposición seguro de soluciones de información e infraestructura.

Los requerimientos de seguridad de la información deben ser identificados previos al diseño o requisición de soluciones de información e infraestructura. De ser necesario el desarrollo interno, los requerimientos deben ser incluidos dentro de los sistemas y si una modificación es solicitada, debe cumplir estrictamente con los requerimientos de seguridad de la información, que han sido previamente establecidos.

b. Seguridad de las comunicaciones en servicios accesibles por redes públicas

La información involucrada en los servicios de aplicaciones que pasan a través de redes públicas, serán protegidos de la actividad fraudulenta, el conflicto contractual, la divulgación y/o modificación no autorizada.

c. Protección de las transacciones por redes telemáticas

La información involucrada en las transacciones de servicios de aplicación deberá ser protegida para prevenir la transmisión incompleta, mal enrutamiento, alteración de mensaje no autorizado, la divulgación no autorizada, la duplicación de mensajes no autorizados o la reproducción.

5.2.24. Seguridad en los procesos de desarrollo y soporte

Objetivo: Garantizar que la seguridad informática diseñada e implementada se cumpla durante el ciclo de vida de desarrollo de sistemas de información.

5.2.24.1. Lineamientos de desarrollo seguro de software

Se establecerán y aplicarán reglas para el desarrollo de software de la compañía.

5.2.24.2. Procedimientos de Control de cambios en los sistemas

Los cambios en los sistemas dentro del ciclo de desarrollo deberán cumplir los procedimientos formales de control de cambios.

5.2.24.3. Revisión técnica de las aplicaciones después de efectuar cambios en los sistemas operativos

Cuando se cambian las plataformas de operación, las aplicaciones críticas deberán ser revisadas y probadas para asegurar que no hay impacto negativo en las operaciones de la compañía o de la seguridad.

5.2.24.4. Restricciones a los cambios en los paquetes de software

Las modificaciones a paquetes de software serán disuadidas, limitadas a cambios necesarios y todos los cambios estrictamente serán controlados.

5.2.24.5. Uso de principios de ingeniería en protección de sistemas

Se aplicarán los principios para ingeniería de sistemas segura, se documentará, y aplicará en la implementación de cualquier sistema de información.

5.2.24.6. Entorno de desarrollo seguro

El proceso de TI debe definir y establecer formalmente la documentación requerida en las diferentes etapas de ciclo de vida de los sistemas.

5.2.24.7. Desarrollo tercerizado

El proceso de TI debe contar con un grupo de personas, el cual debe autorizar la creación, adaptación o adquisición de software.

5.2.24.8. Pruebas de funcionalidad durante el desarrollo de los Sistemas

Las pruebas de la funcionalidad se deben llevar a cabo durante el desarrollo del sistema.

5.2.24.9. Pruebas de aceptación del sistema

Se debe cumplir con los formatos y el procedimiento del sistema de SERVICIOS AMBIENTALES S.A. ESP la realización y documentación de las pruebas.

5.2.25. Los datos de prueba

Objetivo: Garantizar la protección de los datos utilizados para prueba.

5.2.25.1. Protección de los datos de prueba

Los datos de prueba deben seleccionarse cuidadosamente, en caso de seleccionar datos reales, estos deben ser protegidos y controlados.

5.2.26. Relaciones con los proveedores

Objetivo: Garantizar la protección de los activos de la compañía que sea accesible por los proveedores.

5.2.26.1. Lineamientos de seguridad de la información para las relaciones con proveedores

Se acordará con el proveedor y se documentaran los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la compañía.

De igual forma se debe incluir un acuerdo formal de niveles de servicios en seguridad de la información, en el que se detallen los compromisos en el cuidado de los recursos de información de la compañía y las sanciones en caso de incumplimiento. El cumplimiento de los niveles de servicios en seguridad de la Información de terceros debe ser verificado y controlado permanentemente por quienes ejerzan las funciones de interventoría.

5.2.26.2. Tratamiento del riesgo dentro de acuerdos con proveedores

Todos los requisitos de seguridad de la información pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la información de SERVICIOS AMBIENTALES S.A. ESP.

5.2.26.3. Cadena de suministro en tecnologías de la información y comunicaciones

Incluir los requisitos para los acuerdos con proveedores para abordar los riesgos de la seguridad de la información, asociada con los servicios de las tecnologías de información y comunicación, y de la cadena de suministro de productos.

5.2.27. Gestión de la prestación de servicios por proveedores

Objetivo: Mantener un nivel convenido de seguridad de la información y la prestación de servicios en los acuerdos con los proveedores.

5.2.27.1. Seguimiento y revisión de los servicios de proveedores

Cada servicio con proveedor deberá tener con un supervisor encargado de revisar y auditar la prestación de servicios a proveedores.

5.2.27.2. Gestión de cambios en los servicios prestados por proveedores

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales LINEAMIENTOS de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y reevalúan los riesgos.

5.2.28. Gestión de incidentes de seguridad de información

5.2.28.1. Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes en la seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la información.
El responsable de la Información debe definir los eventos considerados como críticos junto con sus respectivas alertas y registros de seguridad de la información, los cuales deberán ser generados. Éstos deben ser activados, vigilados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera inmediata al equipo de respuesta de los incidentes. Los registros y los medios que se generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las evidencias.

Los incidentes de seguridad, resultantes del incumplimiento de los lineamientos y normas de seguridad de SER AMBIENTAL S.A.. E.S.P. serán direccionados por el procedimiento de manejo de incidentes establecido por el proceso de TI, con el objetivo de realizar la respectiva investigación y entregar los resultados a los respectivos responsables dentro de la compañía, encargados de tomar las acciones correctivas y preventivas del caso.

Los colaboradores deberán estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de los lineamientos de seguridad de la información o alguno de los elementos que la soportan. En cualquier caso, se hará un seguimiento de acuerdo con el procedimiento establecido para el

manejo de incidentes de seguridad

5.2.28.2. Responsabilidades y procedimientos

La responsabilidad y el procedimiento de manejo para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información está en cabeza del proceso de tecnología.

a. Informar sobre los eventos de seguridad de información

Los eventos de seguridad de información se comunicarán a través de canales de gestión adecuadas tan pronto como sea posible.

b. Notificación de puntos débiles de la seguridad

Los colaboradores y contratistas que utilizan los sistemas y servicios de información deben observar y reportar cualquier debilidad de seguridad de información observada o sospechada en los mismos.

c. Valoración de eventos de seguridad de la información y toma de decisiones

El proceso de tecnología es la encargada de valorar los eventos de seguridad de información y decidir si han de ser clasificados como incidentes de seguridad de la información.

d. Respuesta a incidentes de seguridad de la información

Los incidentes de seguridad de información deberán recibir una respuesta de conformidad con los procedimientos documentados.

e. Aprendizaje de los incidentes de seguridad de la información

Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de información se deben utilizar para reducir la probabilidad o el impacto de los incidentes en el futuro.

f. Recopilación de evidencias

SERVICIOS AMBIENTALES S.A. ESP debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.

5.2.28.3. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

a. Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Verificar la información de continuidad de los controles de seguridad establecidos y aplicados a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.

5.2.29. Cumplimiento

5.2.29.1. Cumplimiento de los requisitos legales y contractuales

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de lainformación y de los requisitos de seguridad.

Las situaciones o acciones que violen el presente lineamiento deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

Con el fin de mantener un nivel de seguridad adecuado con el negocio de SERVICIOS AMBIENTALES S.A. ESP, este lineamiento se debe apoyar con las mejores prácticas de seguridad de la información y aquellas que el mercado y la compañía reconozcan como tal.

El sistema de gestión en seguridad de la información de SERVICIOS AMBIENTALES S.A. ESP será auditado anualmente para verificar y garantizar su grado de cumplimiento, implementación y madurez.

La información de auditoría generada por el uso de los controles de seguridad de los recursos de tecnología, debe ser evaluada por el responsable para:

- Detectar violaciones a los lineamientos.
- Reportar incidentes de seguridad.
- Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.

Periódicamente se debe evaluar el cumplimiento de los requerimientos de seguridad por parte de los usuarios. El incumplimiento de los requerimientos de seguridad, se debe registrar como un incidente a los lineamientos de seguridad de la información que debe ser resuelto de acuerdo con los procedimientos de manejo de incidentes de SERVICIOS AMBIENTALES S.A. ESP. Deben establecerse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

5.2.29.2. Identificación de la legislación aplicable y los requisitos contractuales

Todos los requisitos pertinentes, legislativos estatutarios, reglamentarios, contractuales y el planteamiento de la entidad para cumplir con estos requisitos deberán estar explícitamente identificados, documentados y protegidos al día para cada sistema de información y la compañía.

5.2.29.3. Derechos de propiedad intelectual

Se aplicarán procedimientos apropiados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales, relacionados con los derechos de propiedad intelectual y uso de productos de software propietario.

Se debe establecer en los contratos de trabajo de los colaboradores y en los contratos de desarrollo realizados por proveedores y contratistas, cláusulas respecto a la propiedad intelectual de SER AMBIENTAL S.A. ESP, al material y productos generados en el desarrollo del negocio.

5.2.29.4. Protección de los registros

Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarias, contractuales y comerciales.

5.2.29.5. Protección de datos y privacidad de la información personal

Se garantizará la privacidad y la protección de la información de identificación personal de acuerdo a lo dispuesto en la legislación y la reglamentación pertinente en su caso.

5.2.29.6. Regulación de los controles criptográficos

Los controles criptográficos serán utilizados en cumplimiento a todos los acuerdos pertinentes, la legislación y los reglamentos.

5.2.30. Revisiones de la seguridad de la información

Objetivo: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con los lineamientos y procedimientos de la compañía.

5.2.30.1. Revisión independiente de la seguridad de la información

El enfoque de la compañía para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, lineamientos y procedimientos para la seguridad de la información) se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

5.2.30.2. Cumplimiento de las lineamientos y normas de seguridad

El proceso de TI deberá comprobar periódicamente el cumplimiento de los procedimientos de procesamiento de la información dentro de sus responsabilidades con los lineamientos, las normas y otros requisitos de seguridad.

5.2.30.3. Comprobación del cumplimiento

Los sistemas de información deben ser revisados regularmente para cerciorarse que se da cumplimiento a los lineamientos y normas de seguridad de la información de la entidad.

Las situaciones o acciones que violen los presentes lineamientos deben ser detectadas, registradas, analizadas, resueltas e informadas al comité de seguridad de la información y a los procesos responsables por su tratamiento de manera inmediata.

6. APLICABILIDAD

SERVICIOS AMBIENTALES S.A ESP, no cuenta con un sistema de gestión de seguridad de la información implementado en norma ISO 27001, sin embargo, actualiza su política de seguridad de la información con base en el lineamiento nacional generado por el proceso de TI corporativo por lo cual todos los colaboradores deben conocer y difundir el presente lineamiento.

7. ANEXOS

No aplica.

HISTORIAL DE CAMBIOS

REVISIÓN NO.	FECHA	ELABORADO/MODIFICADO POR	DESCRIPCIÓN DEL CAMBIO
1	07/07/2020	Yudi Paola Rodriguez	Versión original
2	11/11/2020	Julian Castaño – Alfredo Ramos	Actualización por lineamiento de gerencia corporativa de TI

Elaboró: Gerente de TI corporativo	**Revisó:** Coordinadora de Calidad
Aprobó: Gerencia General	

COPIA CONTROLADA	SI ■	NO