



POLITICA SEGURIDAD DE LA INFORMACIÓN

Código: ESE-TI-POL-002
Versión: 04
Vigencia: 23/10/2022
Página: 1 DE 14

CONTROL DE VERSIONES Y APROBACIONES							
FECHA VIGENCIA	VERSIÓN	ELABORACIÓN/MODIFICACIÓN		REVISIÓN (R) / APROBACIÓN (A)			CAMBIOS EN DOCUMENTO
		Nombre	Cargo	Rol	Nombre	Cargo	
06/08/2020	01	Gustavo Insignares	Gerente de Efectividad Organizacional	R	Mario Gutierrez	Gerente de Auditoria	
		Vladimir Ibañez	Gerente de T.I.	A	Maria Inés Hurtado	Vicepresidente de Talento y Asuntos Legales	
					Claudia Pinilla	Vicepresidente de Estrategia y Finanzas	
06/09/2021	02	Juliana Valdés	Líder de Gestión y Control TI	R	Vladimir Ibañez	Gerente de T.I.	Actualización de la política para que se encuentre alineada a la política de TI. •Se eliminó la palabra "y terceros" de: Capitulo II. •Se adicionaron los puntos 4 y 5 del Capítulo V: Acceso a Internet •Se adicionó el Capitulo XVI: Gestión de Interfaces. •Se eliminan directrices a nivel general que no aplican actualmente.
				A	Claudia Pinilla	Vicepresidente de Estrategia y Finanzas	
22/07/2022	03	Víctor Martínez	Líder de Seguridad y Servicios de Infraestructura	R	Vladimir Ibañez	Gerente de T.I.	•La declaración expresa del compromiso de la alta dirección. •La obligación para empleados y contratistas de recibir capacitación o inducción en Seguridad de la Información al inicio de su relación con ESENTTIA. •La obligación de los gerentes de proyectos de identificar activos y flujos de información, así como los controles asociados a estos, desde los orígenes de los proyectos. •Mayor énfasis en la responsabilidad por parte de los usuarios titulares, sobre las cuentas de usuarios asignadas.
		Juliana Valdés	Líder de Gestión y Control TI	A	Claudia Pinilla	Vicepresidente de Estrategia y Finanzas	

"Nota: Cualquier documento impreso y/o cualquier archivo electrónico que se encuentre fuera de la herramienta de la Oficina de Procesos será considerado COPIA NO CONTROLADA."



POLITICA SEGURIDAD DE LA INFORMACIÓN

Código: ESE-TI-POL-002
 Versión: 04
 Vigencia: 23/10/2022
 Página: 2 DE 14

							<ul style="list-style-type: none"> •Declaración de responsabilidad por parte de los jefes de área sobre los ajustes de permisos requeridos cuando se presentan cambios en las funciones de sus colaboradores, y estos lo ameriten. La declaración de responsabilidad por parte de los interventores de contratos de hacer cumplir a su contratista lo establecido en la Política de Seguridad de la Información
23/10/2022	04	Camilo Pachón	Analista de Efectividad Organizacional	R	Kelly Pereira	Analista de Efectividad Organizacional	Ajustes generales relacionados con términos incluyentes en la documentación
	05			A			
				R			
				A			

	<h1>POLITICA SEGURIDAD DE LA INFORMACIÓN</h1>	<p>Código: ESE-TI-POL-002 Versión: 04 Vigencia: 23/10/2022 Página: 3 DE 14</p>
--	---	---

1.) POLITICA
SEGURIDAD DE LA INFORMACION

2.) OBJETIVO
<p>Establecer las directrices para la administración y adecuado uso de la información asociada a los procesos, asegurando la integridad, confidencialidad y disponibilidad de los activos de información.</p>

3.) ALCANCE
<p>Aplica para la gestión de los activos de información de ESENTTIA a nivel de IT y OT y debe ser cumplida por los/las funcionarios(as) ESENTTIA, proveedores y contratistas.</p>

4.) DEFINICIONES
<p>Activo de Información: Es un recurso (Software, Hardware, archivo físico) que genera, procesa y/o resguarda información necesaria para la operación y el cumplimiento de los objetivos del negocio. Ejemplo: Lista de Precios en el Servidor.</p> <p>Activo de información Crítico: Son los activos de información cuya pérdida de integridad, confidencialidad y disponibilidad tiene un alto impacto para la operación del negocio y el logro de sus objetivos.</p> <p>Análisis Forense Digital: Es un estudio especializado que comprende un conjunto de principios y técnicas relacionadas con el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales, válidas para soportar la investigación de un incidente de Ciberseguridad.</p> <p>ANS: Siglas de acuerdo de nivel de servicio, también identificado por las siglas en inglés SLA, es un pacto realizado entre un proveedor de servicio y su cliente con objeto de fijar unos parámetros para medir la entrega de dicho servicio.</p> <p>Cuenta de correo genérica: Es aquella cuenta que no está constituida por el nombre y apellido del/la funcionario(a) dueño(a) de esta. Ejemplos: facturacion@ESENTTIA.co; cartera@ESENTTIA.co.</p> <p>Custodio de la Información: Es el/la encargado(a) de proteger, mantener, monitorear e implementar controles para asegurar los activos de información. (Ejemplo: CAD, Tecnología de Información).</p> <p>Evidencia Digital: se entiende al conjunto de datos digitales, comprendido por archivos, su contenido y/o referencias a éstos (metadatos) que se encuentren en los soportes del sistema atacado.</p> <p>Flujo de información: se refiere a la actividad de impartir directrices, o emitir instrucciones, guías, comunicaciones y a la creación, modificación y transmisión de activos de información dentro de una organización. Se puede realizar de forma directa entre los actores o a través de sistemas de información. Puede haber varias direcciones en las que tiene lugar dentro de esta, como por ejemplo hacia abajo, hacia arriba, hacia los pares (horizontal), diagonal y externa.</p> <p>Información Sensible: Se entiende por información sensible aquella que afectan la intimidad de una persona 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</p>



POLITICA SEGURIDAD DE LA INFORMACIÓN

Código: ESE-TI-POL-002

Versión: 04

Vigencia: 23/10/2022

Página: 4 DE 14

garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Información Confidencial: Información que en caso de ser divulgada tendrá un impacto alto para el cumplimiento de los objetivos propuestos por la compañía.

Información de tipo Interno: Información que puede ser de conocimiento de los miembros de uno o más procesos de la compañía.

Información de tipo Publico: Información creada y controlada por entidades estatales o no estatales donde todas las personas tienen derecho a solicitar y divulgar sin ninguna autorización previa. Este tipo de información no tendría ningún impacto en caso de divulgación.

Incidente de seguridad de la información: Es un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad de la información: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

5.) DECLARACIONES / DIRECTRICES GENERALES

Capítulo I: Directrices Generales

- 1.) En ESENTTIA la información es un activo fundamental para su operación y toma de decisiones, razón por la cual existe una responsabilidad expresa de la alta dirección, traducida en comunicar y hacer cumplir por parte de todos(as) los/las empleados(as), proveedores y contratistas según corresponda, su compromiso con la protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos de pérdida de integridad, confidencialidad y disponibilidad, y la consolidación de una cultura de seguridad de la información.
- 2.) Todos(as) los/las empleados(as) y contratistas de ESENTTIA, al iniciar su relación con la organización, y posteriormente, cuando así se requiera, deben recibir capacitación sobre las Políticas y Procedimientos de Seguridad de la información definidos.
- 3.) En ESENTTIA se ha definido que los tipos de información son: Sensible, Confidencial, Interna y Publica.
- 4.) Los/las funcionarios(as) y terceros, al igual que los/las empleados(as) o subcontratistas de estos, no pueden asumir en nombre de ESENTTIA, posiciones personales en encuestas de opinión, foros u otros medios similares. El área de Comunicaciones Corporativas será la responsable de asumir o delegar esta responsabilidad.
- 5.) El Gobierno para la gestión de la seguridad de la información estará conformado por la mesa de ciberseguridad de Ecopetrol, el Comité de Seguridad de la Información, el Oficial de Seguridad de la Información y los/las dueños(as) de los activos de información, quienes son los/las líderes y dueños(as) de los procesos a los cuales pertenecen los activos de información. En el caso de no contar con Oficial de seguridad, el comité de seguridad de la información asumirá sus responsabilidades.

- 6.) El comité de seguridad de la información tiene como objetivo:
- Velar por el cumplimiento de esta política, y establecer directrices, estrategias y acciones para mitigar el riesgo de seguridad de la información definido por la compañía.
 - Revisar periódicamente la definición del riesgo de seguridad de la información definido por el comité Directivo.
 - Definir los criterios para la clasificación de la información con el objetivo de mitigar el riesgo de seguridad de la información definido por la compañía.
- 7.) La Gerencia de TI es la encargada de validar y autorizar el software a utilizar en ESENTTIA. Sin importar el uso para el que se destine, la forma de uso (Instalado o vía web), debe contar con la aprobación de la Gerencia de TI para operar en la compañía. Así mismo, los medios de instalación de software (cuando aplique) deben ser administrados y proporcionados por ESENTTIA a través de esta Gerencia.
- 8.) Es responsabilidad de todos(as) los/las funcionarios(as), interventores, proveedores y contratistas de ESENTTIA reportar inmediatamente al Líder de Seguridad y Servicios de Infraestructura o al Comité de seguridad de la información los incidentes, eventos sospechosos y el mal uso de los recursos que identifique en materia de seguridad de la información de acuerdo con el **Procedimiento para el reporte de incidentes de Ciberseguridad a casa matriz Ecopetrol**.
- 9.) Las violaciones a las políticas y controles de seguridad de la información serán reportadas, registradas y monitoreadas por el comité de seguridad de la información. Para el caso de violaciones por parte de funcionarios(as) ESENTTIA se seguirá lo estipulado para procesos disciplinarios de Talento Humano y para el caso de que el evento sea con proveedores y contratistas se seguirá lo definido en las condiciones contractuales estipuladas.

Capítulo II: Activos de información críticos

- Los activos de información críticos de ESENTTIA, serán identificados y clasificados por los/las dueños(as) de procesos para establecer los mecanismos de protección necesarios, y deberán ser actualizados por el mismo cada vez que se realicen cambios al proceso o se actualice la estrategia de la compañía.
- Los/las Gerentes de los proyectos deberán identificar los activos de información y los flujos de estos, para cada uno de los proyectos gestionados y suministrar a TI los insumos pertinentes para establecer los controles necesarios para mitigar el riesgo de Seguridad de la Información definido por la compañía durante las diferentes etapas de estos y la transición a operación.
- Todos los recursos de información críticos de ESENTTIA deben tener asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario(a) requiera para el desarrollo de sus funciones, definidos y aprobados por el/la dueño(a) de proceso y administrados por la Gerencia de Tecnología.
- El comité de seguridad de la información revisara periódicamente la **Matriz de Controles Transversales** que se encuentra en el **Procedimiento de Gestión de los activos de información de los procesos** definida para mitigar el riesgo de seguridad de la información definido por la compañía.
- El/la dueño(a) del proceso deberá aplicar controles de acuerdo con la **Matriz de Controles Transversales** que se encuentra en el **Procedimiento de Gestión de los activos de información de los procesos** para proteger los activos de información críticos de sus procesos contra ciberataques, pérdida o fuga de información, y adicionalmente debe garantizar su cumplimiento.

- 6.) Los entes de aseguramiento definidos en ESENTTIA, deberán realizar auditorías periódicas de cumplimiento a los controles aplicados.

Capitulo III: Acuerdos de confidencialidad

- 1.) Todos(as) los/las funcionarios(as) que obtengan y manejen información en el desarrollo de sus funciones deberán firmar un “acuerdo de confidencialidad de la información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerada como un “incidente de seguridad”.
- 2.) Mientras persista una relación laboral con ESENTTIA, todos sus empleados(as), cederán a la compañía los derechos de propiedad intelectual de los desarrollos que originen como parte de sus responsabilidades laborales con la compañía.
- 3.) Para el caso de proveedores, contratistas y terceros que hagan uso de información de la compañía, los respectivos contratos y ordenes de servicios deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de ESENTTIA a personas o entidades externas.
- 4.) Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Capitulo IV: Protección y ubicación de los equipos - Control de acceso físico

- 1.) Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido, las cuales deben estar señalizadas.
- 2.) Todas las áreas de acceso restringido deben contar con medidas de control de acceso físico en el perímetro que puedan ser auditadas, así como con documentos y/o protocolos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales. Los terceros siempre deberán permanecer acompañados por un funcionario(a) de la compañía.
- 3.) De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones. Los/las funcionarios(as) y terceros, incluyendo sus empleados(as) o contratistas, que tengan acceso a los centros de datos de ESENTTIA no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.
- 4.) Los equipos que hacen parte de la infraestructura tecnológica de ESENTTIA tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

- 5.) ESENTTIA mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Data center).

Capítulo V: Control de acceso lógico

- 1.) El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso digital de información de ESENTTIA debe ser asignado “por medio de nombres de usuario y contraseñas personales e intransferibles según lo definido en la Política de Tecnología de Información,” de acuerdo con la identificación previa de requerimientos de Seguridad y del negocio que se definan por las diferentes áreas de la compañía, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información. Está prohibido el préstamo de cuentas (revelación de contraseñas) de los sistemas (aplicativos, dominio, VPN, etc). El/la ciudadano(a) ESENTTIA a quien por su propia culpa, dolo o preterintencional le sea utilizada su clave por parte de terceros y registre transacciones no autorizadas, le será iniciado un proceso disciplinario donde se estudiará la situación y las posibles consecuencias de esta.
- 2.) Las contraseñas de acceso a los sistemas de información no deben ser escritas en medios físicos o digitales no protegidos; deben ser memorizadas o almacenadas digitalmente: bajo técnicas de cifrado de datos, o usando archivos protegidos por contraseñas que sigan las directrices consignadas en Política de Tecnología de Información. La Gerencia de Tecnología de Información asigna los accesos a plataformas, usuarios previa solicitud del área responsable, los cuales deben ser revisados de manera periódica por los/las dueños(as) de proceso. Todo(a) funcionario(a) o tercero que requiera tener acceso a los sistemas de información de ESENTTIA debe seguir las directrices indicadas por la Política de Tecnología de Información numeral 5.
- 3.) Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de ESENTTIA siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.
- 4.) Cuando se produzcan cambios de funciones o roles dentro de un área que impliquen la reasignación de privilegios sobre los sistemas o repositorios de Información, los/las jefes(as) de los/las funcionarios(as) implicados serán los responsables de aprobar la asignación y/o remoción de estos permisos. Estos cambios se deben tramitar con la mesa de ayuda de la Gerencia de Tecnología y serán atendidos de acuerdo con los ANS definidos.
- 5.) Los/las funcionarios(as) y/o contratistas que realicen labores de desarrollo de Software, no deberán tener privilegios de escritura sobre los sistemas del ambiente de producción de la compañía. Los cambios requeridos en dicho ambiente serán realizados de forma controlada.
- 6.) Los cambios a datos de producción deberán ser autorizados por el/la Gerente de Tecnología de Información.

Capítulo VI: Riesgos relacionados con proveedores, contratistas y terceros

- 1.) El/la dueño(a) del activo de información identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los proveedores, contratistas y terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

- 2.) Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por los proveedores, contratistas y terceros mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.
- 3.) Los/las interventores de contratos serán los/las responsables de solicitar a la Gerencia de Tecnología de Información la validación de seguridad informática de los equipos de cómputo y/o dispositivos móviles con capacidad de procesamiento de datos, propiedad de proveedores, contratistas y terceros, que requieran ser ingresados a las instalaciones de ESENTTIA y conectados a la red corporativa.

Capítulo VII: Uso adecuado de los activos de información

- 1.) El acceso a los documentos físicos y digitales estará determinado por los permisos y niveles de acceso definidos por el/la dueño(a) del activo de información de acuerdo con el **Procedimiento de Gestión de los activos de información de los procesos** y que deberán ser consignados en las tablas de retención documental.
- 2.) Para la consulta de documentos cargados en el software de Gestión Documental Softexpert se establecerán privilegios de acceso a los/las funcionarios(as) y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el/la dueño(a) del proceso, quien comunicará al grupo encargado de la administración del software su parametrización en la herramienta.

Capítulo VIII: Acceso a Internet

- 1.) En materia de internet No está permitido:
 - a. El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra del código de conducta de la compañía, las leyes vigentes o políticas aquí establecidas.
 - b. Compartir información confidencial y sensible relacionada con las operaciones y procesos de la compañía en Internet, como por ejemplo redes sociales, correos personales, Streaming, servicios de almacenamientos en la nube como Dropbox, entre otros.
 - c. El intercambio no autorizado de información de propiedad de ESENTTIA, de sus clientes y/o de sus funcionarios(as), con terceros.
 - d. La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. Cualquier excepción a lo anterior deberá ser revisada y autorizada por la Gerencia de TI.
- 2.) El uso de Internet no considerado dentro de las restricciones anteriormente expuestas es permitido siempre y cuando se realice en cumplimiento del código de conducta, de la ley, sea razonable y responsable, no abusivo y sin afectar la productividad ni la protección de la información de ESENTTIA.
- 3.) La Gerencia de Tecnología de Información puede inspeccionar, registrar, monitorear y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente.

- 4.) Sólo se permitirá el uso del chat corporativo o previamente autorizado por la Gerencia de TI.
- 5.) Dentro del documento *Guía De Seguridad de la información* custodiado por la Gerencia de TI, se encuentran definidos los perfiles de navegación con los permisos establecidos para los usuarios del servicio de internet.

Capítulo IX: Correo electrónico

Los/las funcionarios(as) de ESENTTIA, proveedores, contratistas y terceros autorizados, a quienes ESENTTIA les asigne una cuenta de correo deberán seguir las siguientes directrices:

- 1.) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de ESENTTIA. La información contenida en los buzones de correo es propiedad de ESENTTIA y por tal, ésta se reserva el derecho de usar herramientas que le permitan monitorear el uso dado tanto al servicio de correo electrónico, como a la información que fluye a través de él.
- 2.) El correo electrónico podrá ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad. ESENTTIA no se hace responsable del uso personal que se le dé a este recurso corporativo.
- 3.) En caso de requerir enviar información confidencial, deben emplearse las facilidades especiales que ofrece el sistema de correo, de acuerdo con el Instructivo para el envío de correos confidenciales.
- 4.) No es permitido:
 - a. Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Empresa, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales. De igual forma, enviar cadenas de correo a externos no autorizados.
 - b. Utilizar correo electrónico de ESENTTIA como punto de contacto en las redes sociales o cualquier otro sitio que no tenga que ver con las actividades laborales.
 - c. El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
 - d. El envío de archivos de música y videos que no sean de carácter laboral.
- 5.) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que ESENTTIA proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.
- 6.) El envío masivo de mensajes publicitarios corporativos deberá realizarse según lo definido en el proceso de Gestión de Comunicaciones de ESENTTIA.
- 7.) En el caso de requerir el envío masivo de mensajes publicitarios corporativos a terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución.



POLITICA SEGURIDAD DE LA INFORMACIÓN

Código: ESE-TI-POL-002
Versión: 04
Vigencia: 23/10/2022
Página: 10 DE 14

- 8.) Si un área debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre del área respectiva y/o servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.
- 9.) Toda información de ESENTTIA generada en los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la compañía, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Gerencia de Tecnología. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.
- 10.) El envío de Información confidencial fuera o dentro de la organización a usuarios no autorizados debe ser aprobado por el dueño del activo de Información.
- 11.) Todos los mensajes enviados deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Capitulo X: Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por ESENTTIA a sus funcionarios(as) y/o terceros se reglamenta bajo los siguientes lineamientos:

- 1.) Los equipos de cómputo, dispositivos móviles, y celulares asignados por Esenttia a sus funcionarios(as) y/o contratistas, son herramientas de trabajo y deben ser utilizados para fines laborales. El/la usuario(a) a quien le hayan sido asignados será responsable de su buen cuidado y correcto uso.
- 2.) Toda la información almacenada en los equipos de cómputo de Esenttia es propiedad de la compañía, y debe ser clasificada de acuerdo con los criterios establecidos según el tipo de información (Confidencial, sensible, interna y/o pública). Lo(a)s empleado(a)s que tengan bajo su cargo estos equipos serán responsables de la custodia de los registros que almacenen.
- 3.) Si un(a) funcionario(a) mantiene información personal en equipos de cómputo de Esenttia, ésta deberá ser almacenada en un directorio nombrado como "Personal".
- 4.) Los/las usuarios(as) no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red y usuarios locales de la máquina. Estos cambios pueden ser realizados únicamente por la Gerencia de Tecnología.
- 5.) Únicamente los/las funcionarios(as) y terceros autorizados(as) por la Gerencia de Tecnología, previa solicitud escrita por parte del área que lo requiera, pueden conectarse a la red inalámbrica corporativa de ESENTTIA.
- 6.) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de ESENTTIA, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Gerencia de Tecnología.
- 7.) Sólo personal autorizado(a) puede realizar actividades de administración remota de dispositivos, equipos y/o servidores de la infraestructura de procesamiento de información de ESENTTIA; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Gerencia de Tecnología.

- 8.) Solo la Gerencia de Tecnología está autorizada para realizar conexiones a nivel de red o modificaciones sobre estas.
- 9.) Toda información corporativa es propiedad de ESENTTIA y el uso de esta desde cualquier dispositivo de propiedad personal o corporativa, se le aplicaran los controles técnicos requeridos para garantizar la disponibilidad, integridad y confidencialidad. ESENTTIA se reserva el derecho a emplear sistemas informáticos automáticos que monitoreen el uso dado a la información propiedad de la compañía.

Capítulo XI: Segregación de funciones

- 1.) Toda tarea en la cual los/las funcionarios(as) tengan acceso a la infraestructura tecnológica y a los sistemas de información debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

Capítulo XII: Protección contra software malicioso

- 1.) Es responsabilidad de la Gerencia de Tecnología de la Información asegurar que todos los recursos informáticos de ESENTTIA estén protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de estos a la red corporativa, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código malicioso.
- 2.) La Gerencia de Tecnología definirá e implementará las soluciones (Hardware y/o Software) que permitan controlar el software malicioso en los equipos de cómputo corporativos y/o que hagan parte de la infraestructura de TI. De igual forma restringirá la posibilidad de inactivación de estas por parte de los usuarios y promoverá su actualización permanente.
- 3.) No está permitido:
 - a. La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por la Gerencia de Tecnología de la Información.
 - b. Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
 - c. Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

Capítulo XIII: Copias de respaldo

- 1.) La Gerencia de Tecnología y el/la dueño(a) de proceso debe asegurar que la información con cierto nivel de clasificación contenida en la plataforma tecnológica de ESENTTIA, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

- 2.) La Gerencia de Tecnología establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá en conjunto con las áreas los períodos de retención de esta. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- 3.) Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Capitulo XIV: Gestión de medios removibles

- 1.) El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, cintas) sobre la infraestructura para el procesamiento de la información de ESENTTIA, estará autorizado por la Gerencia de Tecnología, previo visto bueno del/la jefe(a) Inmediato(a), para aquellos/aquellas funcionarios(as) cuyo perfil del cargo y funciones lo requiera. Así mismo, el/la funcionario(a) autorizado(a) por la Gerencia de Tecnología debe asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de ESENTTIA que éste contiene.
- 2.) La Gerencia de Tecnología es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de ESENTTIA, sólo los/las funcionarios(as) autorizados(as) pueden hacer uso de los medios de almacenamiento removibles.

Capitulo XV: Intercambio de información

- 1.) Todo(a) funcionario(a) de ESENTTIA es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.
- 2.) Los/las propietarios(as) de la información que requieren intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad requeridos.
- 3.) Una vez implementado, por la Gerencia de TI, el sistema de almacenamiento en la nube en cada uno de los computadores, los/las usuarios(as) deberán hacer uso de la sincronización como método de copia de respaldo para la información que se encuentra ubicada en su computador.
- 4.) El trámite de permisos a carpetas de red debe ser realizada de acuerdo con el *Procedimiento para la Gestión de Usuarios (ESE-TI-PRO-007)*.

Capitulo XVI: Gestión de Interfaces

- 1.) Creación y Modificación: Toda interfaz debe ser revisada y validada por el/la jefe(a) Integrador(a) de Soluciones y Proyectos de TI, previa autorización del dueño del proceso funcional que se beneficie o afecte la integración.



POLITICA SEGURIDAD DE LA INFORMACIÓN

Código: ESE-TI-POL-002

Versión: 04

Vigencia: 23/10/2022

Página: 13 DE 14

- 2.) Eliminación: Toda interface debe darse de baja por el/la jefe(a) Integrador(a) de soluciones y Proyectos de TI previa solicitud del/la dueño(a) del proceso que usa la interface o por disposición directa del área de Tecnología cuando esta genere un riesgo para la compañía. El riesgo debe ser soportado por el/la Líder de Seguridad e Infraestructura de TI.
- 3.) La documentación de la interface debe contener por lo menos: Sistema Origen, Sistema Destino, Tipo de Interface, En línea o Batch. Esta documentación está en custodia del/la jefe(a) Integrador(a) de Soluciones y Proyectos de TI para ser requerida cuando se necesite.
- 4.) Para cualquier actividad que afecte una integración ya sea de creación, modificación o eliminación se deberá actualizar su documentación existente.

Capitulo XVII: Escritorio y pantalla limpia

- 1.) Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos(as) los/las funcionarios(as) de ESENTTIA deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.
- 2.) Todos(as) los/las usuarios(as) son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Capitulo XVIII: Segregación de redes

- 1.) La plataforma tecnológica de ESENTTIA que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La Gerencia de Tecnología es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- 2.) ESENTTIA establece 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 de la Organización.

Capitulo XIX: Identificación de requerimientos de seguridad

- 1.) Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre ESENTTIA y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad de la Gerencia de Tecnología garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la Jefatura de Asuntos Legales establecer estos aspectos con las obligaciones contractuales específicas.



POLITICA SEGURIDAD DE LA INFORMACIÓN

Código: ESE-TI-POL-002
Versión: 04
Vigencia: 23/10/2022
Página: 14 DE 14

Capitulo XX: Incidentes de Seguridad de la Información

- 1.) Los/las usuarios(as) de los sistemas de información no deben, bajo circunstancia alguna, intentar probar una supuesta debilidad de Seguridad de la Infraestructura Tecnológica de ESENTTIA, por cuanto la comprobación de esta acción será interpretada como una falta grave y será analizada de acuerdo con lo establecido en el Código de Ética y Conducta (ESE-AEC-CO-001).
- 2.) Cuando se considere pertinente, ESENTTIA podrá recurrir a la realización de análisis forense para recopilar mayor cantidad de información probatoria que soporte la investigación de un incidente de Seguridad de la Información. Los incidentes de seguridad de la información identificados e investigados deberán ser reportados a Ecopetrol según lo definido en el Procedimiento para el reporte de incidentes de Ciberseguridad a casa matriz Ecopetrol (ESE-TI-PRO-022).

6.) DOCUMENTOS DE REFERENCIA

CÓDIGO	NOMBRE
ESE-TI-PRO-022	Procedimiento para el reporte de incidentes de Ciberseguridad a casa matriz Ecopetrol
ESE-TI-PRO-020	Gestión de los activos de información de los procesos
ESE-AEC-CO-001	Código de Ética y Conducta
ESE-TI-PRO-007	Procedimiento para la Gestión de Usuario