POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE MANIZALES S.A.S – ERUM S.A.S.

Manizales, Centro Administrativo Municipal CAM
Calle 19 #21 - 44 Torre A pisos 7 y 13
Tels: (+57) 6 8722053• (+57) 6 8720538 • (+57) 6 8720630
contacto@erum.gov.co • www.erum.gov.co

INTRODUCCIÓN

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S con el propósito de proteger la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

Para LA ERUM S.A.S, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general.

Los activos de información de la ERUM S.A.S. son reconocidos como un activo valioso. A medida que los sistemas de información apoyan cada vez más los procesos de misión crítica de la empresa, se requiere de contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Los sistemas y las redes de información de la ERUM S.A.S. enfrentan amenazas de seguridad, las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

Con la promulgación de la presente Política de Seguridad de la Información ERUM S.A.S. formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales y promoviendo la mejora continua dentro de la organización.

Es así, que la ERUM S.A.S. establece los mecanismos para respaldar la difusión, estudio, actualización y consolidación, tanto de la presente política, como de los demás componentes del Sistema de Gestión de la Seguridad de la Información, alineándolos de forma efectiva con el Sistema Integrado de Gestión.

ALCANCE

La Política de SEGURIDAD Y PRIVACIDAD EN LA INFORMACION permite que La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, cuente con un equipo humano y técnico comprometido con la protección de toda la información digital, el buen funcionamiento de los recursos tecnológicos, la seguridad informática y una conectividad continua que facilite a todos los funcionarios las labores diarias relacionadas con el diligenciamiento de documentos y desarrollo de sus procesos.

OBJETIVOS

OBJETIVO GENERAL

Implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en objetivos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios, es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva. Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc.

OBJETIVO ESPECÍFICOS:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuario de ERUM S.A.S.
- Garantizar la continuidad de los procesos frente a incidentes.

DIAGNOSTICO

Una de las herramientas adoptadas para realizar el diagnóstico del proceso de Seguridad y Privacidad de la información, fue la Matriz de autodiagnóstico diseñada por el Departamento Administrativo de la Función Pública, en la cual se identifican las rutas que se deben trabajar para mejorar en el cumplimiento, la eficiencia, la eficacia y la efectividad del sistema.

De igual manera, se tuvo en cuenta la medición de desempeño institucional 2021 para la entidad (FURAG) en la cual se establecieron las siguientes recomendaciones:

Recomendaciones de Mejora por Política

Fecha de generación: 2023-01-16 11:25:39

Entidad: EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE MANIZALES S.A.S.

Departamento: Caldas

Municipio: Manizales

#	Política	Recomendaciones
18	Planeación Institucional	Establecer estrategias de difusión de la información utilizando diversos canales de comunicación adecuados a las características de la población usuaria y ciudadanía, para dar a conocer los derechos a la participación ciudadana en la gestión institucional y el control social, así como sobre los mecanismos de participación que la entidad ha dispuesto para ello.
5	Gobierno Digital	Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de accesibilidad: Idioma. (regla CC27)
6	Gobierno Digital	Cumplir, en todas las secciones de la página web oficial de la entidad, con el criterio de accesibilidad: Imágenes de texto. (regla CC29)
7	Gobierno Digital	Formular el Plan Estratégico de Tecnologías de la Información (PETI), aprobarlo mediante el comité de gestión y desempeño institucional e integrarlo al plan de acción anual de la entidad.

8	Gobierno Digital	Definir un esquema de soporte con niveles de atención (primer, segundo y tercer nivel) a través de un punto único de contacto y soportado por una herramienta tecnológica, tipo mesa de servicio que incluya al menos la gestión de problemas, incidentes, requerimientos, cambios, disponibilidad y conocimiento.
9	Gobierno Digital	Definir un proceso para atender los incidentes y requerimientos de soporte de los servicios de TI, tipo mesa de ayuda.
10	Gobierno Digital	Disponer un catálogo de servicios de TI actualizado para la gestión de tecnologías de la información (TI) de la entidad.
11	Gobierno Digital	Definir Acuerdos de Nivel de Servicios (SLA por sus siglas en inglés) con terceros y Acuerdos de Niveles de Operación (OLA por sus siglas en inglés) para la gestión de tecnologías de la información (TI) de la entidad.
12	Gobierno Digital	Incorporar políticas de TI en el esquema de gobierno de tecnologías de la información (TI) de la entidad.
13	Gobierno Digital	Incorporar, en el esquema de gobierno de tecnologías de la información (TI) de la entidad, un macroproceso o proceso (procedimientos, actividades y flujos) de gestión de TI definido, documentado y actualizado.
14	Gobierno Digital	Incorporar, en el esquema de gobierno de tecnologías de la información (TI) de la entidad, instancias o grupos de decisión de TI.
15	Gobierno Digital	Incorporar, en el esquema de gobierno de tecnologías de la información (TI) de la entidad, la estructura organizacional del área de TI.
16	Gobierno Digital	Incorporar, en el esquema de gobierno de tecnologías de la información (TI) de la entidad, indicadores para medir el desempeño de la gestión de TI.
17	Gobierno Digital	Utilizar acuerdos marco de precios para bienes y servicios de TI con el propósito de optimizar las compras de tecnologías de información de la entidad.
18	Gobierno Digital	Aplicar una metodología para la gestión de proyectos de TI de la entidad, que incluya seguimiento y control a las fichas de proyecto a través de indicadores.
19	Gobierno Digital	Garantizar que todas las iniciativas, proyectos o planes de la entidad que incorporen componentes de TI, sean liderados en conjunto entre las áreas misionales y el área de TI de la entidad.
20	Gobierno Digital	Utilizar el principio de incorporar, desde la planeación de los proyectos de tecnologías de la información (TI) de la entidad,

		la visión de los usuarios y la atención de las necesidades de los grupos de valor.
21	Gobierno Digital	Llevar a cabo la documentación y transferencia de conocimiento a proveedores, contratistas y/o responsables de TI,Â sobre los entregables o resultados de los proyectos de TI ejecutados.
22	Gobierno Digital	Definir herramientas tecnológicas para la gestión de proyectos de TI de la entidad.
23	Gobierno Digital	Actualizar el catálogo de componentes de información.
24	Gobierno Digital	Actualizar las vistas de información de la arquitectura de información para todas las fuentes.
25	Gobierno Digital	Implementar procesos o procedimientos de calidad de datos para mejorar la gestión de los componentes de la información de la entidad.
26	Gobierno Digital	Implementar procesos o procedimientos que aseguren la integridad, disponibilidad y confidencialidad de los datos para mejorar la gestión de los componentes de información de la entidad.
27	Gobierno Digital	Actualizar el catálogo de todos los sistemas de información.
28	Gobierno Digital	Actualizar y documentar una arquitectura de referencia y una arquitectura de solución para todas las soluciones tecnológicas de la entidad, con el propósito de mejorar la gestión de sus sistemas de información.
29	Gobierno Digital	Incluir características en los sistemas de información de la entidad que permitan la apertura de sus datos de forma automática y segura.
30	Gobierno Digital	Incorporar dentro de los contratos de desarrollo de los sistemas de información de la entidad, cláusulas que obliguen a realizar transferencia de derechos de autor a su favor.
31	Gobierno Digital	Implementar para los sistemas de información de la entidad funcionalidades de trazabilidad, auditoría de transacciones o acciones para el registro de eventos de creación, actualización, modificación o borrado de información.
32	Gobierno Digital	Actualizar la documentación técnica y funcional para cada uno de los sistemas de información de la entidad.
33	Gobierno Digital	Actualizar los manuales de usuarios y manuales técnicos y de operación para cada uno de los sistemas de información de la entidad.
34	Gobierno Digital	Elaborar y actualizar los documentos de arquitectura de los desarrollos de software de la entidad.
35	Gobierno Digital	Definir e implementar una metodología de referencia para el desarrollo de software y sistemas de información.

36	Gobierno Digital	Definir el esquema de soporte y mantenimiento de los sistemas de información, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.
37	Gobierno Digital	Definir un proceso de construcción de software que incluya planeación, diseño, desarrollo, pruebas, puesta en producción y mantenimiento.
38	Gobierno Digital	Implementar un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información que incluya criterios funcionales y no funcionales.
39	Gobierno Digital	Definir y aplicar una guía de estilo en el desarrollo de los sistemas de información de la entidad e incorporar los lineamientos de usabilidad definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.
40	Gobierno Digital	Incorporar las funcionalidades de accesibilidad establecidas en la política de Gobierno Digital, en los sistemas de información de acuerdo con la caracterización de usuarios de la entidad.
41	Gobierno Digital	Implementar un programa de correcta disposición final de los residuos tecnológicos de acuerdo con la normatividad del gobierno nacional.
42	Gobierno Digital	Actualizar visitas de despliegue, conectividad y almacenamiento de la arquitectura de infraestructura de TI de la entidad.
43	Gobierno Digital	Hacer uso de servicios de computación en la nube para mejorar los servicios que presa la entidad.
44	Gobierno Digital	Documentar e implementar un plan de continuidad de los servicios tecnológicos mediante pruebas y verificaciones acordes a las necesidades de la entidad.
45	Gobierno Digital	Implementar mecanismos de disponibilidad de la infraestructura de TI de tal forma que se asegure el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos.
46	Gobierno Digital	Realizar monitoreo del consumo de recursos asociados a la infraestructura de TI de la entidad.
47	Gobierno Digital	Adoptar en su totalidad el protocolo IPV6 en la entidad.
48	Gobierno Digital	Implementar una estrategia de uso y apropiación para todos los proyectos de TI teniendo en cuenta estrategias de gestión del cambio para mejorar el uso y apropiación de las tecnologías de la información (TI) en la entidad.

49	Gobierno Digital	Implementar una estrategia de divulgación y comunicación de los proyectos TI para mejorar el uso y apropiación de las tecnologías de la información (TI) en la entidad. Desde el sistema de control interno efectuar su verificación.
50	Gobierno Digital	Utilizar la caracterización de los grupos de interés internos y externos para mejorar la implementación de la estrategia para el uso y apropiación de tecnologías de la información (TI) en la entidad.
51	Gobierno Digital	Ejecutar un plan de formación o capacitación dirigido a servidores públicos para el desarrollo de competencias requeridas en TI.
52	Gobierno Digital	Hacer seguimiento al uso y apropiación de tecnologías de la información (TI) en la entidad a través de los indicadores definidos para tal fin. Desde el sistema de control interno efectuar su verificación.
53	Gobierno Digital	Ejecutar acciones de mejora a partir de los resultados de los indicadores de uso y apropiación de tecnologías de la información (TI) en la entidad. Desde el sistema de control interno efectuar su verificación.
54	Gobierno Digital	Realizar un diagnóstico de seguridad y privacidad de la información para la vigencia, mediante la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).
55	Gobierno Digital	Formular la política de seguridad y privacidad de la información de la entidad, aprobarla mediante el comité de gestión y desempeño institucional, implementarla y actualizarla mediante un proceso de mejora continua, de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones.
56	Gobierno Digital	Definir y documentar procedimientos de seguridad y privacidad de la información, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
57	Gobierno Digital	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
58	Gobierno Digital	Identificar los riesgos de seguridad y privacidad de la información de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, valorarlos y actualizarlos mediante un proceso de mejora continua.

59	Gobierno Digital	Implementar el plan de tratamiento de riesgos de seguridad de la información.
60	Gobierno Digital	Elaborar el plan operacional de seguridad y privacidad de la información de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
61	Gobierno Digital	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
62	Gobierno Digital	Publicar todos los conjuntos de datos abiertos estratégicos de la entidad en el catálogo de datos del Estado Colombiano www.datos.gov.co.
63	Gobierno Digital	Mantener actualizados todos los conjuntos de datos abiertos de la entidad que están publicados en el catálogo de datos del Estado Colombiano www.datos.gov.co.
64	Gobierno Digital	Emplear diferentes medios digitales en los ejercicios de participación realizados por la entidad.
65	Gobierno Digital	Utilizar medios digitales en los ejercicios de rendición de cuentas realizados por la entidad.
66	Gobierno Digital	Mejorar las actividades de formulación de la planeación mediante la participación de los grupos de valor en la gestión de la entidad.
67	Gobierno Digital	Mejorar las actividades de formulación de políticas, programas y proyectos mediante la participación de los grupos de valor en la gestión de la entidad.
68	Gobierno Digital	Mejorar las actividades de ejecución de programas, proyectos y servicios mediante la participación de los grupos de valor en la gestión de la entidad.
69	Gobierno Digital	Mejorar la solución de problemas a partir de la implementación de ejercicios de innovación abierta con la participación de los grupos de valor de la entidad.
70	Gobierno Digital	Mejorar las actividades de promoción del control social y veedurías ciudadana mediante la participación de los grupos de valor en la gestión de la entidad.
71	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre las tablas de retención documental.
72	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica

		información actualizada sobre las políticas de seguridad de la información del sitio web y protección de datos personales.
73	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre la información sobre los grupos étnicos en el territorio.
74	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre el calendario de actividades.
75	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre ofertas de empleo.
76	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre la ejecución presupuestal histórica anual.
77	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre el plan anticorrupción y de atención al ciudadano.
78	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre el plan de gasto público.
79	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre los proyectos de inversión en ejecución.
80	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre los mecanismos para la participación de los ciudadanos, grupos de valor o grupos de interés en la formulación de políticas.
81	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre los entes de control que vigilan la entidad.
82	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre el registro de activos de información.
83	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica

		información actualizada sobre el índice de información clasificada y reservada.
84	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre el esquema de publicación de información.
85	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre el programa de gestión documental.
1	Seguridad Digital	Establecer un responsable para el seguimiento al manejo de riesgos dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
2	Seguridad Digital	Establecer una periodicidad para el seguimiento al manejo de riesgos dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
3	Seguridad Digital	Establecer el nivel de aceptación del riesgo dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
4	Seguridad Digital	Establecer niveles para calificar el impacto del riesgo dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
5	Seguridad Digital	Incorporar el análisis del contexto interno y externo de la entidad dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
6	Seguridad Digital	Monitorear el seguimiento a la gestión del riesgo por parte de las instancias responsables para determinar si este se lleva a cabo adecuadamente, por parte del comité institucional de coordinación de control interno.
7	Seguridad Digital	Fomentar la generación de acciones para apoyar la segunda línea de defensa frente al seguimiento del riesgo, por parte del comité institucional de coordinación de control interno.
8	Seguridad Digital	Designar un responsable para llevar a cabo la actividad de control, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles.
9	Seguridad Digital	Establecer una periodicidad para la ejecución de los controles, por parte de los líderes de los programas, proyectos, o

		procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles.
10	Seguridad Digital	Establecer un propósito para el control, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles.
11	Seguridad Digital	Describir como se realiza la actividad de control, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles.
12	Seguridad Digital	Proporcionar una descripción del manejo frente a observaciones o desviaciones resultantes de la ejecución del control con el fin de dar lineamientos sobre los posibles cursos de acción, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles.
13	Seguridad Digital	Presentar una evidencia de la ejecución del control, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles.
14	Seguridad Digital	Incluir los riesgos con mayor impacto dentro de los mapas de riesgos de la entidad.
15	Seguridad Digital	Contar con el monitoreo o seguimiento de los riesgos, dentro de los mapas de riesgos, de acuerdo con la periodicidad establecida en la política de administración del riesgo.
16	Seguridad Digital	Actualizar los mapas de riesgos de la entidad de acuerdo con los resultados del monitoreo o seguimiento.
17	Seguridad Digital	Divulgar oportunamente la actualización de los mapas de riesgos de la entidad.
18	Seguridad Digital	Asegurar que los riesgos identificados son monitoreados de acuerdo con la política de administración de riesgos, por parte de los cargos que lideran de manera transversal temas estratégicos de gestión (tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, líderes de otros sistemas de gestión, comités de riesgos).
19	Seguridad Digital	Hacer seguimiento a los mapas de riesgos y deben verificar que se encuentren actualizados, por parte de los cargos que lideran de manera transversal temas estratégicos de gestión (tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, líderes de otros sistemas de gestión, comités de riesgos).
20	Seguridad Digital	Llevar a cabo una gestión del riesgo en la entidad, que le permita evitar la materialización de los riesgos.

21	Seguridad Digital	Llevar a cabo una gestión del riesgo en la entidad, que le permita controlar los puntos críticos de éxito.
22	Seguridad Digital	Llevar a cabo una gestión del riesgo en la entidad, que le permita ejecutar los controles de acuerdo con su diseño.
23	Seguridad Digital	Hacer seguimiento a los riesgos y controles de sus procesos, programas o proyectos a cargo, por parte de los líderes de los programas, proyectos, o procesos de la entidad en coordinación con sus equipos de trabajo.
24	Seguridad Digital	Contemplar por parte del jefe de Control Interno, que sus informes de seguimiento y auditoría emitidos por las oficinas de control interno contribuyan a la formulación de acciones enfocadas a la gestión del riesgo.
25	Seguridad Digital	Identificar factores sociales que pueden afectar negativamente el cumplimiento de los objetivos institucionales. Desde el sistema de control interno efectuar su verificación.
26	Seguridad Digital	Identificar factores tecnológicos que pueden afectar negativamente el cumplimiento de los objetivos institucionales. Desde el sistema de control interno efectuar su verificación.
27	Seguridad Digital	Evaluar por parte del jefe de control interno o quien haga sus veces en la entidad, que los controles diseñados establezcan el cómo se realiza la actividad de control.
28	Seguridad Digital	Evaluar a través de las oficinas de control interno de la entidad o quien haga sus veces, en el marco de sus roles y en desarrollo del plan de auditoría, los aspectos que no estén cubiertos por otras acciones de seguimiento o monitoreo.
29	Seguridad Digital	Evaluar a través de las oficinas de control interno de la entidad o quien haga sus veces, en el marco de sus roles y en desarrollo del plan de auditoría, la efectividad de las acciones incluidas en los planes de mejoramiento producto de las auditorías internas y de entes externos.
30	Seguridad Digital	Establecer y ejecutar el plan anual de auditoría basado en riesgos por parte del jefe de control interno o quien haga sus veces.
31	Seguridad Digital	Definir en la planta de personal de la entidad (o documento que contempla los empleos de la entidad) los perfiles de los empleos teniendo en cuenta la misión, los planes, programas y proyectos.
32	Seguridad Digital	Realizar un diagnóstico de seguridad y privacidad de la información para la vigencia, mediante la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).

33	Seguridad Digital	Formular la política de seguridad y privacidad de la información de la entidad, aprobarla mediante el comité de gestión y desempeño institucional, implementarla y actualizarla mediante un proceso de mejora continua, de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones.
34	Seguridad Digital	Definir y documentar procedimientos de seguridad y privacidad de la información, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
35	Seguridad Digital	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
36	Seguridad Digital	Identificar los riesgos de seguridad y privacidad de la información de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, valorarlos y actualizarlos mediante un proceso de mejora continua.
37	Seguridad Digital	Implementar el plan de tratamiento de riesgos de seguridad de la información.
38	Seguridad Digital	Elaborar el plan operacional de seguridad y privacidad de la información de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
39	Seguridad Digital	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
40	Seguridad Digital	Recopilar y organizar información que permita a la entidad identificar y caracterizar sus grupos de valor, para diseñar estrategias de intervención ajustadas a cada grupo.
41	Seguridad Digital	Utilizar la información de caracterización de los grupos de valor de la entidad para definir sus planes, proyectos y programas.
42	Seguridad Digital	Utilizar la información de caracterización de los grupos de valor para definir sus estrategias de servicio al ciudadano, rendición de cuentas, trámites y participación ciudadana en la gestión.

43	Seguridad Digital	Mantener actualizada la información recopilada sobre los grupos de valor y así poder diseñar estrategias de intervención ajustadas a la realidad.
44	Seguridad Digital	Definir el direccionamiento estratégico teniendo en cuenta los lineamientos para la gestión del riesgo (Política de Riesgo).
45	Seguridad Digital	Incluir los lineamientos para la evaluación del riesgo en el proceso de planeación de la entidad para diseñar una planeación que garantice la seguridad institucional.
46	Seguridad Digital	Contar con un acto administrativo del Comité de Gestión y Desempeño Institucional que incluya lineamientos para la implementación de la política de Seguridad digital.
47	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del modelo de gestión de riesgos de seguridad digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones.
48	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad estableciendo convenios o acuerdos con otras entidades en temas relacionados con la defensa y seguridad digital.
49	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad.
50	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como registrarse en el CSIRT Gobierno y/o COLCERT.
51	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética.
52	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.
53	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.
54	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en las mesas de construcción y sensibilización del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.

55	Seguridad Digital	Hacer campañas de concientización en temas de seguridad de la información de manera frecuente y periódica, específicas para cada uno de los distintos roles dentro de la entidad.
56	Seguridad Digital	Establecer un procedimiento de gestión de incidentes de seguridad de la información, formalizarlo y actualizarlo de acuerdo con los cambios de la entidad.
57	Seguridad Digital	Efectuar evaluaciones de vulnerabilidades informáticas.
58	Seguridad Digital	Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.
59	Seguridad Digital	Realizar periódicamente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos.
23	Transparencia, Acceso a la Información y lucha contra la Corrupción	Actualizar el catálogo de todos los sistemas de información.
24	Transparencia, Acceso a la Información y lucha contra la Corrupción	Actualizar y documentar una arquitectura de referencia y una arquitectura de solución para todas las soluciones tecnológicas de la entidad, con el propósito de mejorar la gestión de sus sistemas de información.
25	Transparencia, Acceso a la Información y lucha contra la Corrupción	Incluir características en los sistemas de información de la entidad que permitan la apertura de sus datos de forma automática y segura.
26	Transparencia, Acceso a la Información y lucha contra la Corrupción	Incorporar dentro de los contratos de desarrollo de los sistemas de información de la entidad, cláusulas que obliguen a realizar transferencia de derechos de autor a su favor.
27	Transparencia, Acceso a la Información y lucha contra la Corrupción	Implementar para los sistemas de información de la entidad funcionalidades de trazabilidad, auditoría de transacciones o acciones para el registro de eventos de creación, actualización, modificación o borrado de información.
28	Transparencia, Acceso a la Información y lucha contra la Corrupción	Actualizar la documentación técnica y funcional para cada uno de los sistemas de información de la entidad.
29	Transparencia, Acceso a la Información y lucha contra la Corrupción	Actualizar los manuales de usuarios y manuales técnicos y de operación para cada uno de los sistemas de información de la entidad.
30	Transparencia, Acceso a la Información y lucha contra la Corrupción	Elaborar y actualizar los documentos de arquitectura de los desarrollos de software de la entidad.
31	Transparencia, Acceso a la Información y lucha contra la Corrupción	Definir e implementar una metodología de referencia para el desarrollo de software y sistemas de información.

32	Transparencia, Acceso a la Información y lucha contra la Corrupción	Realizar un diagnóstico de seguridad y privacidad de la información para la vigencia, mediante la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).
33	Transparencia, Acceso a la Información y lucha contra la Corrupción	Formular la política de seguridad y privacidad de la información de la entidad, aprobarla mediante el comité de gestión y desempeño institucional, implementarla y actualizarla mediante un proceso de mejora continua, de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones.
34	Transparencia, Acceso a la Información y lucha contra la Corrupción	Definir y documentar procedimientos de seguridad y privacidad de la información, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
35	Transparencia, Acceso a la Información y lucha contra la Corrupción	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
36	Transparencia, Acceso a la Información y lucha contra la Corrupción	Identificar los riesgos de seguridad y privacidad de la información de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, valorarlos y actualizarlos mediante un proceso de mejora continua.
37	Transparencia, Acceso a la Información y lucha contra la Corrupción	Implementar el plan de tratamiento de riesgos de seguridad de la información.
38	Transparencia, Acceso a la Información y lucha contra la Corrupción	Elaborar el plan operacional de seguridad y privacidad de la información de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
39	Transparencia, Acceso a la Información y lucha contra la Corrupción	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
40	Transparencia, Acceso a la Información y lucha contra la Corrupción	Formular el plan de apertura, mejora y uso de datos abiertos de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional e integrarlo al plan de acción anual.

Así mismo la auditoría interna realizada por la Dirección de evaluación y control encontró algunas falencias a las cuales se le realizó el siguiente plan de mejoramiento:

PLAN DE MEJORAMIENTO INSTITUCIONAL EMPRESA DE RENOVACION Y DESARROLLO URBANO DE MANIZALES S.A.S. - ERUM S.A.S.

Número de Auditoría	**CI-AU-02. PC 06. GESTIÓN ADMINISTRATIVA**
Vigencia Evaluada	2022
Modalidad Auditoría	AUDITORÍA INTERNA
Fecha de Suscripción Plan de Mejoramiento	6/12/2022
Fecha de Vencimiento del Plan de Mejoramiento	6/06/2023

No de Relación de Hallazgos formulados por la A.G.R.	Relación de Acciones Correctivas Para Desarrollar	Responsable	Cronograma de Ejecución	Metas Cuantificables	Indicador de Cumplimiento	Seguimiento PM Parcial
Hallazgo 7. Deficiencias en la política de respaldo, custodia y recuperación de la información	Realizar copias de seguridad con periodicidad mensual de cada uno de los equipos en uso, en un disco externo.	Subgerente Administrativo y Financiero - Director de Gestión humana y Organizacional- Gestion Tecnológica (People Contac)	Diciembre 1 de 2022 a enero 30 de 2023	100%	Cronograma de copias de seguridad y hoja de vida de los equipos de cómputo	15 de marzo de 2023
	Realizar reunión informativa a todo el personal sobre el uso y manejo de los backup o almacenamiento de información.	Subgerente Administrativo y Financiero - Director de Gestión humana y Organizacional	Diciembre 1 de 2022 a enero 30 de 2023	100%	Acta de Reunión	15 de marzo de 2023

Hallazgo 8. Seguridad informática. No se está dando cumplimiento a la política de seguridad y privacidad de la información adoptada para el año 2022	Diseñar la política de seguridad de la información de la entidad para vigencia 2023, implementarla y socializarla para una efectiva operacionalización.	Director de Gestión humana y Organizacional-Gestion Tecnológica (People Contac)	Diciembre 1 de 2022 a enero 30 de 2023	100%	Política adoptada para la vigencia 2023 / debidamente publicada en el portal Web de la entidad.	15 de marzo de 2023
Hallazgo 9. Licenciamiento de equipos de cómputo. existen equipos de cómputo con igual número de licencia	Realizar inventario de licencias del sistema operativo de los equipos de cómputo.	Gestion Tecnológica (People Contac)	30 de diciembre de 2022	100%	Inventario de equipos que carecen de registro de licencia	15 de marzo de 2023
	A partir del inventario de equipos que carecen de registro, adquirir las licencias necesarias con un proveedor autorizado.	Subgerente Administrativo y Financiero - Director de Gestión humana y Organizacional	Enero 2 a abril 30 de 2023	100%	Licencia instalada por equipo	15 de marzo de 2023

Fue importante para el diagnóstico tener en cuenta también el **INFORME DEAUDITORÍA TICS Y SEGURIDAD INFORMÁTICA CORTE AGOSTO DE 2021,** realizado por la empresa Nexia Montes y Asociados.

De acuerdo a los resultados anteriores, podemos determinar que la entidad presenta algunas deficiencias en su **POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**, esto significa que es necesario iniciar con una estrategia especial para el fortalecimiento de dicha política de todos los componentes y procesos que la constituyen teniendo en cuenta que La Seguridad y Privacidad de la Información son factores relevantes a la hora de preservar de manera correcta y eficiente las fuentes de información de la Institución, al mismo tiempo permitirle a la ciudadanía el acceso a la información pública de una manera transparente, segura y eficaz.

Dentro de la **POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**, es importante también generar conciencia a nivel interno sobre el tratamiento, la seguridad y el manejo de los datos, generando compromiso por parte de los funcionarios y liderazgo por parte

de la unidad encargada con el fin de obtener los resultados necesarios para el cumplimiento de dicha política.

FORMULACIÓN DE LA PLANEACIÓN ESTRATÉGICA

A continuación, se establecen 11 principios de seguridad que soportan el SGSI de LA Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.

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

- **LA ERUM S.A.S** protegerá la información generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- **LA ERUM S.A.S** protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- **LA ERUM S.A.S** protegerá su información de las amenazas originadas por parte del personal.

- **LA ERUM S.A.S** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- **LA ERUM S.A.S** controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- **LA ERUM S.A.S** implementará control de acceso a la información, sistemas y recursos de red.

- **LA ERUM S.A.S** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- **LA ERUM S.A.S** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- **LA ERUM S.A.S** garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- **LA ERUM S.A.S** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

- **LA ERUM S.A.S**, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a: **Minimizar el riesgo de los procesos misionales de la entidad.**

Esta política aplica a toda la entidad. Sus funcionarios, contratistas y terceros de LA Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S y la ciudadanía en general.

Nivel de cumplimiento: Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente, socialice e interiorice, para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

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

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

• Justificación de la creación de política: Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

• Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

• Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

• Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de esta.

• Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de estas. *Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas*.

2. Cumplimiento: Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

3. Comunicación: Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. *Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de estas;* esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

4. Monitoreo: Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos, ejemplo: indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

5. Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

6. Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

POLITICAS ESPECÍFICAS RECOMENDADAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

En este documento se presenta algunas recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y Privacidad de la Información para las Entidades del Estado. Este conjunto de recomendaciones no es exhaustivo, se aconseja que cada Entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar. A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

1. **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:** Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información. Debe tener los siguientes elementos:

• ¿Quiénes conforman el comité directivo de seguridad de la información?
• Objetivos: Se deben especificar los objetivos del comité como por ejemplo el mejoramiento continuo de los programas o las distintas actividades que se realizarán en dichos comités, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad etc…
• Cumplimiento: Debe establecerse que dicho comité verifique el cumplimiento de las políticas.

2. **GESTION DE ACTIVOS:** Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información. Se realizará la identificación de los activos informáticos de la ERUM S.A.S con una periodicidad de 6 meses determinando el responsable de cada activo.

Las políticas relacionadas con gestión de activos deben contemplar como mínimo:

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

• **Etiquetado de la Información**: Cada activo se etiquetó o rotuló después de clasificarlo, el responsable de este procedimiento es también quien se encarga de la clasificación. Fue de carácter obligatorio el etiquetado de todos los activos, preferiblemente con adhesivos de seguridad que no permitan remover o cambiar el etiquetado.

• **Devolución de los Activos**: Cada funcionario es responsable del uso, almacenamiento y devolución de los activos que están a su cargo una vez finalizado su contrato o periodo laboral en la ERUM S.A.S, estas devoluciones deben coincidir con el inventario de activos físicos actualizado.

• **Gestión de medios removibles**: LA ERUM S.A.S, cuenta con varios medios de almacenamiento de información removibles "THERAS O DISCOS EXTERNOS" los cuales se encuentran relacionados y clasificados como *Medios Removibles* en el inventario y clasificación que se realizado, estos medios están a disposición de algunos funcionarios que justificaron porqué los deben tener, de la misma manera cada funcionario firmó un acta de entrega, manejo y confidencialidad, además el usuario recibió una contraseña de acceso al Disco externo, ésta contraseña se almacena en un lugar seguro tanto por el usuario como por el administrador general del inventario.

Esta política contempla los usos y permisos que tienen los usuarios y/o funcionarios de la Entidad frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Esta política describe detenidamente en qué casos se autoriza y en los que no, el uso de medios removibles y los procedimientos en los cuales se determinen las autorizaciones; adicionalmente describe al responsable de las autorizaciones y responsabilidades de aquellas personas que tienen autorización para el uso del dicho medio de almacenamiento. El uso de medios removibles en la entidad está alineado a las clasificaciones de activos dispuestas en la política de "Clasificación de Activos".

• **Disposición de los activos**: LA ERUM S.A.S, construyó un procedimiento mediante el cual se realiza de forma correcta y segura la eliminación, retiro, traslado o re uso de los Activos, teniendo en cuenta que se debe realizar el Backup o copia de seguridad y almacenamiento final de esa información evitando así el acceso o borrado no autorizado de la información antes de la disposición final del activo. Este procedimiento aplica para discos duros internos, discos duros externos, tabletas digitales, teléfonos celulares, memorias USB.

• **Dispositivos móviles**: Esta política determina a los funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas, quiénes pueden realizar instalación de chats corporativos y/o correos electrónicos de la entidad mediante el uso de este tipo de dispositivos, adicionalmente describe las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles así como como los controles de seguridad que la entidad utiliza para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información, SE PROHIBE EL ACCESO A LAS REDES INALAMBRICAS A PERSONAS AJENAS A LA ALCALDIA DE VITERBO.

3. **CONTROL DE ACCESO** Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales la Entidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos

a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso contemplan como mínimo:

• **Control de acceso con usuario y contraseña**: Para este procesamiento se tuvo en cuenta la cantidad de estaciones de trabajo, el tipo de red que se manejara y el tipo de acceso que se suministrara a cada usuario, Cada estación de trabajo se identificó con un NOMBRE DE USUARIO, ejemplo ERUMDGTH, de acuerdo a la necesidad se activaron los accesos a carpetas compartidas, impresoras y acceso a otros usuarios, de la misma manera se implementó un generador de contraseñas con varios niveles de seguridad, permitiendo cambiar la contraseñas con una periodicidad de 30 días, este cambio será efectuado por el administrador de la red o el encargado del inventario de activos, esta contraseña es almacenada en un lugar seguro tanto por el usuario como por el administrador, estas contraseñas son intransferibles, podrán ser eliminadas o cambiadas por el administrador cuando sea pertinente o cuando se realice algún cambio de funcionario, contratista o tercero el cual deberá tener un nuevo usuario y una contraseña para el acceso.

El administrador también tiene a cargo el manejo de los accesos a las diferentes plataformas, aplicaciones y software que sean requeridos para el buen funcionamiento y gestión de los procesos de la ERUM S.A.S.

• **Perímetros de Seguridad**: LA ERUM S.A.S define los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuáles no, la política definió los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

• **Áreas de Carga**: LA ERUM S.A.S Definió las condiciones e instalaciones físicas en las cuales se realizará despacho y carga de paquetes físicos para bodegas o espacios definidos de carga, esto con el fin de evitar el acceso no autorizado a otras áreas de la entidad.

Las empresas de carga y descarga solamente podrán realizar acciones en la unidad de Gobierno en Línea y Atención al Ciudadano, es allí donde se recepciona toda la correspondencia de la ERUM S.A.S, ningún representante de las empresas de carga podrá acceder a otra dependencia sin previa autorización.

4. **NO REPUDIO**. En cuanto a que la seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción se tienen en cuenta los siguientes aspectos.

- Autenticación: Permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.

- Autorización: Permite controlar el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber superado el proceso de autenticación.

- Auditoría: Verifica el correcto funcionamiento de las políticas o medidas de seguridad tomadas.

- Encriptación: Ayuda a ocultar la información transmitida por la red o almacenada en los equipos, para que cualquier persona ajena no autorizada, sin el algoritmo y clave de descifrado, pueda acceder a los datos que se quieren proteger.

- Realización de copias de seguridad e imágenes de respaldo, para que en caso de fallos nos permita la recuperación de la información perdida o dañada.

- Antivirus: Como su nombre indica, consiste en un programa que permite estar protegido contra las amenazas de los virus.

- Cortafuegos o firewall: Programa que audita y evita los intentos de conexión no deseados en ambos sentidos, desde los equipos hacia la red y viceversa.

- Servidores proxys: Consiste en ordenadores con software especial, que hacen de intermediario entre la red interna de una empresa y una red externa, como pueda ser Internet. Estos servidores, entre otras acciones, auditan y autorizan los accesos de los usuarios a distintos tipos de servicios como el de FTP (transferencia de ficheros), o el Web (acceso a páginas de Internet).

- Utilización firma electrónica o certificado digital: Son mecanismos que garantizan la identidad de una persona o entidad evitando el no repudio en las comunicaciones o en la firma de documentos. También se utilizan mucho hoy en día para establecer comunicaciones seguras entre el PC del usuario y los servidores de Internet como las páginas web de los bancos.

- Conjunto de leyes encaminadas a la protección de datos personales que obligan a las empresas a asegurar su confidencialidad.

5. **PRIVACIDAD Y CONFIDENCIALIDAD:** Las políticas de tratamiento y protección de datos personales se aplica, conforme a lo establecido en la normatividad vigente. La política de privacidad consta de:

✓ Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
✓ Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.

- ✓ Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.

- ✓ Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

- ✓ Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.

- ✓ Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.

- ✓ Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- ✓ Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

GLOSARIO

SGSI: El Sistema General de Seguridad de la Información (**SGSI**) es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información corporativa en las empresas.

Teras: Los teras y las gigas son las medidas que actualmente se utilizan para medir la capacidad de las memorias actuales, ya que otras unidades menores se han quedado pequeñas actualmente. Un **terabyte (TB) se encuentra compuesto por 1024 gigabytes (GB).**

Backup: Es una copia que se realiza frecuentemente a los datos, archivos o información CRITICA. El backup nos permite estar tranquilo que la información puede recuperarse en caso de que los equipos o las aplicaciones se dañen.

No Repudio: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Existirán por tanto dos posibilidades: - No repudio en origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío.