1. OBJETIVO

Establecer los criterios de clasificación de datos y manejo de información es proteger la información que el OIN TECNIEND SAS posea o tenga en su poder, mediante la identificación de información comercial crítica y sensible para asignar el nivel apropiado de protección. El cumplimiento de esta política de clasificación de datos y manejo de información es necesario para minimizar el daño comercial al reducir la probabilidad de incidentes de seguridad y confidencialidad a través del mal manejo de la información.

Además, la clasificación de datos ofrece un enfoque estándar simplificado para administrar el objetivo del OIN TECNIEND SAS de cumplir con sus obligaciones legales y normativas relacionadas con la privacidad de los datos.

- Todos los usuarios deben tener en cuenta y poder aplicar el esquema de clasificación de datos aprobado.
- Todos los activos de información deben clasificarse.
- La clasificación de información sensible y crítica comercial se regirá por el principio de "necesidad de saber", es decir, la información debe divulgarse solo a las personas que tengan una necesidad comercial legítima de acceder.
- El nivel de protección otorgado a la información dependerá de la clasificación asignada.
- La información debe manejarse de acuerdo con su clasificación, independientemente de si está marcada o no.

2. ALCANCE

Esta política se aplica a todos los activos de información que posee, crea, modifica, almacena o procesa el OIN TECNIEND SAS o en su nombre, independientemente de su ubicación. La aplicación de la política se aplica a todos los formatos, incluidos los archivos digitales, las comunicaciones electrónicas, la forma física o en forma verbal.
Las disposiciones de la política se clasifican de la siguiente manera:

- Obligatorio: Deben cumplirse los requisitos obligatorios a menos que el Departamento de SST haya aprobado una excepción temporal.

- Recomendado: Los requisitos recomendados deben cumplirse a menos que el Departamento de SST haya aprobado una solicitud de excepción exitosa.

- Guía: Se alienta a las unidades operativas a adoptar pautas de la política.

3. REFERENCIAS

- NTC-ISO-IEC 17020:2012

- ILAC P15

4. DEFINICIONES

Ver TECNIEND-SGI-001 Glosario de términos

5. RESPONSABILIDADES

- Gerente general: Estará al tanto del actuar del personal del OIN de TECNIEND SAS, para verificar el cumplimiento y ejecución de la política.
- Director del sistema de gestión integrado: Estará encargado de apoyar los procesos de divulgación para la clasificación y el manejo de la información y la ejecución de la política.
- Gerente técnico: Realizar la divulgación al personal del OIN de TECNIEND SAS, y estar al tanto del seguimiento del cumplimiento de la política.

6. CLASIFICACION DE DATOS

5.1 Dueño Funcional:

Obligatorio

a) Se debe asignar un líder de proceso responsable de cada activo de información identificado y registrarlo en TECNIEND-SGI-FR-002 Listado maestro de documentos.

5.2. Esquema de clasificación

Obligatorio

a) Las clasificaciones de datos indican la sensibilidad de la información (en términos de la probabilidad y / o impacto resultante del compromiso, pérdida o mal uso) y la necesidad de defenderse contra un amplio perfil de amenazas aplicables.
b) El esquema de clasificación se aplica a la información (u otros activos específicos).
c) Los grandes conjuntos de datos agregados y otros sistemas pueden requerir controles mejorados para gestionar eficazmente los riesgos asociados de confidencialidad, integridad y disponibilidad.
d) Hay cuatro niveles de clasificación, como se ilustra a continuación

PUBLICA	CONFIDENCIAL	ALTAMENTE CONFIDENCIAL	RESTRINGIDA
Información que es específicamente preparada para ser material público.	Información que puede causar daños si es compartida con individuos no autorizados.	Información sensible que puede causar daño significativo si es compartida con individuos no autorizados.	El nivel más alto de confidencialidad, puede causar un impacto significativo al negocio, precios o multas monetarias.

e) La información debe protegerse con el nivel apropiado de personal, controles físicos y de seguridad de la información de acuerdo con la línea de base de control definida para cada clasificación.

Recomendado

a) Los umbrales y el esquema de clasificación de datos deben ser revisados formalmente por el departamento de SST al menos una vez al año.

5.3 Definiciones de clasificación

Obligatorio

a) En casos donde hay la propiedad intelectual no publicada y/o la información privada (personal), el propietario del activo de información o el creador de la información deben clasificar la información como CONFIDENCIAL.
b) El principio de "necesidad de saber" debe cumplirse estrictamente para las clasificaciones ALTAMENTE CONFIDENCIALES y RESTRINGIDAS.
c) Activos de información que contienen cuerpos de información de diversos grados de sensibilidad (que no pueden separarse lógica / físicamente) en diferentes activos de información, debe heredar el nivel de clasificación más alto en el mismo.

Guía

a) Las cuatro clasificaciones de seguridad (PÚBLICO, CONFIDENCIAL, ALTAMENTE CONFIDENCIAL y RESTRINGIDA) indican el aumento de sensibilidad de la información.
b) Todos los servicios del negocio y las operaciones de TECNIEND SAS deben tratarse como CONFIDENCIALES por defecto. Algunos ejemplos incluyen manuales, contratos, informes de seguridad.
c) El principio de "necesidad de saber" debe aplicarse a todos niveles de clasificación por encima de PUBLICA.
d) Los ejemplos de información PÚBLICA pueden incluir folletos, comunicados por correos electrónicos, reglas del servicio, informes de productos, información de marketing e informes anuales de TECNIEND SAS la información que por autorización del cliente se requiera divulgar.
e) Ejemplos de información CONFIDENCIAL puede incluir información operativa general diaria, manuales, notas y toda aquella que el cliente requiera manejar como confidencial.
f) Los ejemplos de información ALTAMENTE CONFIDENCIAL pueden incluir información personal básica (como nombres, direcciones, fecha de nacimiento, etc.), listas de proveedores, listas de clientes, informes de inspecciones.
g) Ejemplos de información RESTRINGIDA puede incluir información personal confidencial (como números financieros, médicos, números de identificación, etc.),
h) Aplicando a una clasificación alta puede inhibir el intercambio y conducir a controles de protección innecesarios y costosos.

i) Aplicando una clasificación baja puede resultar en controles inapropiados y potencialmente poner en riesgo los activos sensibles.

5.4 Manejo de información

5.4.1 Resultados de seguridad de la información

Obligatorio

Para mitigar los riesgos de seguridad de la información asociados con cada clasificación, los controles de seguridad de protección deben lograr los siguientes resultados en capas.

CONFIDENCIAL	
Resultados	• Promover el intercambio responsable y la discreción. • Controles proporcionales apropiados para una sensibilidad de activos • Hacer compromiso accidental o daño improbable
Personal	• Acceso por parte del personal de TECNIEND SAS
Seguridad física (manipulación, uso, almacenamiento, transporte y eliminación)	• Precauciones proporcionales de buenas prácticas contra compromisos accidentales u oportunistas • Controle el acceso a los activos sensibles a través de los procesos comerciales locales y disponga con cuidado para que la reconstitución sea poco probable
Seguridad de la información (almacenamiento, uso, procesamiento o transmisión)	• Proteger contra compromisos deliberados mediante ataques automatizados u oportunistas. • Apunte a detectar un compromiso real o intentado y responda

ALTAMENTE CONFIDENCIAL	
Resultados	• Hacer compromisos o daños accidentales altamente improbables • Detectar y resistir intentos deliberados de compromiso.
Personal Autorizado	• Asegurarse de que el acceso sea solo por el personal apropiado de TECNIEND SAS
Seguridad física (manipulación, uso, almacenamiento, transporte y eliminación)	• Detectar y resistir compromisos deliberados mediante ataques forzados.
Seguridad de la información (almacenamiento, uso, procesamiento o transmisión)	• Detectar y resistir compromisos deliberados por parte de un actor de amenazas determinado y con buenos recursos.

RESTRINGIDO	
Resultados	• Prevenir el acceso no autorizado • Detectar y resistir compromisos reales o intentados
Personal Autorizado	• Alta garantía de que el acceso está estrictamente limitado al personal específico de TECNIEND o con aprobación de la alta dirección
Seguridad física (manipulación, uso, almacenamiento, transporte y eliminación)	• Medidas altamente estrictas para evitar el compromiso de un ataque sostenido y sofisticado.
Seguridad de la información (almacenamiento, uso, procesamiento o transmisión)	• Medidas altamente estrictas para evitar el compromiso de un ataque sostenido por un factor de amenazas determinado y con buenos recursos

Nota: El Resultados de los documentos públicos es Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de "La Organización" o no.

Deben cumplirse las siguientes medidas de control de protección por capas de alto nivel cuando se trabaja con activos de información en cada nivel de clasificación.

CONFIDENCIAL	
Personal Autorizado	Los controles mínimos incluyen: • Controles de contratación adecuados sobre el empleo. • Reforzar la responsabilidad personal y el deber de cuidado a través de la capacitación. • El acceso al personal que no pertenece a TECNIEND SAS
Manejo de documentos físicos	• Manejo por personal autorizado de TECNIEND SAS
Almacenamiento físico	• Almacenamiento bajo barrera simple y/o cerradura y llave
Trabajo Remoto Físico	• Asegúrese de que la información no se pueda pasar por alto inadvertidamente mientras se accede a ella de forma remota
Mover activos por correo / mensajería	• Incluya la dirección del remitente, nunca marque la clasificación en el sobre • Considere el uso del servicio de seguimiento y localización de mensajería de buena reputación
Media removible	• Se minimizará el uso de medios extraíbles, y se deberían utilizar otros mecanismos aprobados de intercambio de información cuando estén disponibles de preferencia • Solo medios extraíbles aprobados por TECNIEND SAS
Comunicaciones de voz, video y fax	• Los detalles del material sensible deben mantenerse al mínimo
Eliminación y destrucción	• Deseche con cuidado utilizando productos y servicios de eliminación aprobados para que la reconstitución sea poco probable

Informe de incidentes	• Arreglos locales para reportar incidentes físicos • Todos los incidentes electrónicos deben ser reportados al Director SGI

ALTAMENTE CONFIDENCIAL	
Personal de Autorizado	Los controles mínimos adicionales incluyen: • Siempre imponga la "necesidad de saber" • Instrucciones de manejo especiales • El acceso al personal que no es de TECNIEND SAS
Manejo de documentos físicos	• Registre y archive documentos de acuerdo con procedimientos determinados localmente. • Mantener registros de auditoría apropiadas
Almacenamiento físico	• Considerar la segregación de gabinetes compartidos.
Trabajo Remoto Físico	• Hacer el seguimiento requerido para el cumplimiento de lo establecido
Mover activos por correo / mensajería	• Hacer el seguimiento requerido para el cumplimiento de lo establecido
Comunicaciones de voz, video y fax	• Los destinatarios deben estar esperando recibir la información solicitada.
Eliminación y destrucción	• Destrucción y/o eliminación de forma apropiada para que la reconstitución sea poco probable.
Informe de incidentes	• Los incidentes electrónicos también se deben informar al propietario del activo de información apropiado y al departamento SST

RESTRINGIDO	
Personal Autorizado	Los controles mínimos adicionales incluyen: • El acceso al personal que no es de TECNIEND SAS
Manejo de documentos físicos	• Realice auditorías anuales para garantizar el procesamiento, manejo y mantenimiento de registros adecuados.
Almacenamiento físico	• La información debe tener un responsable y debe ser almacenada bajo llave.
Trabajo Remoto Físico	• Aprobación debe darse por un líder de proceso
Mover activos por correo / mensajería	• Aprobación debe darse por un líder de proceso
Media removible	• Aprobación debe darse por un líder de proceso
Comunicaciones de voz, video y fax	• Protocolos impuestos por el líder del proceso de la información relevante
Eliminación y destrucción	• Destrucción y/o eliminación de forma apropiada para que la reconstitución sea poco probable.
Informe de incidentes	• Los incidentes electrónicos también se deben informar al líder del proceso apropiado, al director del SGI y al gerente general

Nota: El resultado de los documentos públicos es información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de "La Organización" o no.

7. DOCUMENTOS RELACIONADOS

- TECNIEND-SGI-FR-002 Listado maestro de documentos.
- TECNIEND-SGI-FR-003 Solicitud de creación, modificación y/o eliminación de documentos
- TECNIEND-SGI-FR-004 Distribución de documentos
- TECNIEND-GD-AC-001 Acta de imparcialidad independencia y confidencialidad

DIEGO FERNANDO ROMERO MIRANDA

CC: 80.201.461

Representante Legal