Política de Clasificación, Etiquetado y Tratamiento de la Información

Fecha: 29/11/2024
Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
19/11/2024	0.1	Creación del Documento	Comité de Seguridad de la Información
29/11/2024	1.0	Revisión del Documento	Comité de Seguridad de la Información

Contenido

1 Objetivo

El objetivo del presente documento es establecer los criterios de clasificación de la información en poder de ISA Uruguay sin importar el medio que la soporte.

2 Alcance

Esta política abarca toda la información independientemente de su formato y se aplica a todas las clasificaciones de los tipos de información existentes.

Las clasificaciones abarcadas son:

- Información que ha sido identificada como un activo de información por el alcance del Sistema de Gestión de Seguridad de la Información.
- Activos de información identificados en formato electrónico, impresos o comunicados verbal o visualmente.

3 Vigencia

La presente norma entra en vigor a partir de su aprobación y publicación por parte del Comité de Seguridad.

Esta política será revisada en un período no mayor a tres años, o ante cambios que así lo ameriten.

4 Responsabilidades

Directorio – es el responsable de difundir la presente política a todo el personal, independientemente del cargo que desempeñe o su relación contractual con la empresa.

CISO/Comité de Seguridad – debe velar por el cumplimiento y revisión periódica de la presente política, así como la definición del procedimiento para la clasificación de la información, y su integración al Sistema de Gestión de Seguridad de la Información.

Propietarios de los activos - responsables de clasificar la información según corresponda de acuerdo con la política vigente, así como de definir los niveles de acceso y perfiles autorizados para la visualización, modificación y eliminación de la información.

Custodios de la información - responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos, en el marco de lo establecido en la presente política.

Infraestructura/Operaciones - debe proporcionar los medios técnicos para el cumplimiento de esta Política.

Colaboradores - responsable de garantizar la integridad, disponibilidad y confidencialidad de la información sobre la cual tienen control o permisos de acceso mediante el cumplimiento de todas las políticas y procedimientos aplicables.

5 Descripción

Para la correcta gestión de la información la misma debe ser clasificada para de esta manera definir el nivel de acceso necesario para poder acceder a la misma.

Los niveles van de Información Pública, Reservada, Confidencial y Secreta.

5.1 Información Pública

Toda información será considerada pública hasta que sea clasificada en alguna otra categoría.

5.2 Información Reservada

Se clasifica como información reservada toda información que:

a. menoscabe la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otras empresas u organismos internacionales entreguen con carácter de reservado a ISA Uruguay
b. dañe la estabilidad financiera, económica o monetaria de la Empresa
c. ponga en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona,
d. suponga una pérdida de ventajas competitivas para ISA Uruguay o pueda dañar su proceso de producción
e. desproteja descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de ISA Uruguay

Dicha información, permanecerá con tal carácter hasta un periodo de quince años desde su clasificación. Es responsabilidad de los propietarios de los activos y del comité de seguridad la evaluación de la clasificación.

En caso de cumplido el tiempo de reserva, la información pasará a ser publica salvo que el comité de seguridad y el propietario del activo decidan lo contrario por razones justificadas.

5.3 Información Confidencial

Se clasifica como información confidencial toda información que:

1. Sea entregada como confidencial a ISA Uruguay y cumpla con:
    a. Refiere al patrimonio de la persona o empresa.
    b. Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica, que ser usada en contra de los intereses de la empresa.
    c. Esté amparada por una cláusula contractual de confidencialidad.
2. Los datos personales que requieran previo consentimiento informado.
3. La información recibida por terceros entregada a ISA Uruguay en tal carácter.

5.4 Información Secreta

Se clasifica como información secreta la que revelada provoque daños graves a ISA Uruguay para su reputación. La información secreta debe ser accesible para ciertos individuos en base a una necesidad de saber y se deben colocar medidas de seguridad reforzadas para proteger la información.

	C–4 Información Secreta	C–3 Información Confidencial	C–2 Información Reservada	C–1 Información Pública
Etiqueta	Necesaria	Necesaria	Opcional	Opcional
Tipos o ejemplos	Borradores de estados financieros, correos electrónicos, información acerca de fusiones y adquisiciones, proyectos especiales, reestructuras	Información sobre productos, proveedores, colaboradores, procesos, contraseñas, etc.	Información general; manuales, directrices, políticas de la compañía, copias impresas de páginas de intranet.	Diseñada exclusivamente para ser distribuida públicamente, como información del sitio web.

5.5 Etiquetado (Control de Acceso) - Electrónico

Estos lineamientos de etiquetado se aplican solamente a la información en formato electrónico.

C–1 Información Pública: puede considerarse en general como información "Pública" y como tal no requiere ningún control de acceso electrónico especial, ni etiquetado a nivel del documento electrónico.

C –2 Información Reservada: la información "Reservada" se controla mediante los Niveles de Control de Acceso de los sistemas electrónicos y es responsabilidad del dueño del activo el establecer estos niveles de acuerdo con el nivel de clasificación del archivo o documento.

C–3 Información Confidencial: información en este nivel de clasificación se controla mediante los Niveles de Control de Acceso de los sistemas electrónicos y es responsabilidad del dueño del activo el establecer estos niveles de acuerdo con el nivel de clasificación del archivo o documento. Se deben rotular como “C3 - Confidencial” a nivel del documento electrónico.

C – 4 Información Secreta: La información en este nivel de clasificación se controla mediante los niveles de control de acceso y es responsabilidad del propietario de la información el establecer estos niveles de acuerdo con el nivel de clasificación del archivo o documento. Se deben rotular como “C4 - Secreta” a nivel del documento electrónico.

5.6 Tratamiento de la información

La información de ISA Uruguay se clasifica en cuatro niveles: Secreta, Confidencial, Reservada y Pública. Para cada nivel, se describen las medidas y medios actuales para la distribución, garantizando una adecuada seguridad de acuerdo con el nivel de criticidad de la información.

Información Secreta:

- Distribución Interna: Solo puede ser compartida con personas formalmente autorizadas mediante canales seguros. Los documentos digitales deben almacenarse en ubicaciones seguras de la red corporativa con acceso limitado (carpetas cifradas y con permisos de acceso estrictos). Toda transmisión digital debe estar cifrada, idealmente mediante la utilización de una plataforma de colaboración seguras con autenticación multifactor (MFA).

- Distribución Externa: La entrega a terceros debe contar con una autorización expresa del directorio y requerir la firma de un contrato de confidencialidad. Los medios utilizados para la transmisión externa deben ser seguros, como: Plataformas de Transferencia de Archivos Cifrados: Servicios como SFTP o aplicaciones de intercambio de archivos cifrados (Ej.: OneDrive o SharePoint). Contraseña de Cifrado Separada: Las contraseñas para descifrar los archivos deberán ser enviadas por un canal distinto al archivo en sí (ej.:

llamada telefónica), asegurando que ambos elementos no estén accesibles simultáneamente.

Información Confidencial:

- Distribución Interna: Puede ser compartida con empleados autorizados mediante medios seguros, tales como: Utilizar plataformas en la nube (OneDrive, SharePoint) con permisos estrictos y autenticación multifactor. Correo Electrónico Corporativo con cifrado habilitado y validación de destinatarios. De ser posible, utilizar herramientas que permitan la expiración de los accesos o el borrado remoto.

- Distribución Externa: Requiere la firma de acuerdos de confidencialidad previos. Los archivos deben transmitirse mediante: Servicios de Transferencia de Archivos Seguros como OneDrive o, siempre con acceso restringido y autenticación MFA, o plataformas de Colaboración Externas Seguras Como Microsoft Teams, pero solo después de establecer permisos de acceso específicos y garantizar el cifrado de extremo a extremo.

Información Reservada:

- Distribución Interna: Se permite el uso de medios corporativos habituales, tales como: Correo Electrónico Corporativo y Carpetas Compartidas (OneDrive) con control de permisos y acceso según la necesidad de conocer o SharePoint, con permisos ajustados según el perfil del empleado.

- Distribución Externa: Puede ser entregada a terceros siempre que se haya validado la necesidad de conocer y se haya obtenido la autorización del propietario de la información. Para la transmisión: Correo Electrónico con Verificación de Seguridad haciendo uso de firmas digitales o cifrado opcional o una plataforma de almacenamiento en la Nube con Permisos Limitados, garantizando el acceso solo al receptor.

Información Pública:

- Distribución Interna y Externa: No existen restricciones específicas para la distribución de la información pública. Puede ser compartida sin autorización específica a través de cualquier medio corporativo o público (correo electrónico, almacenamiento en la nube, página web), ya que no representa un riesgo significativo para la empresa.

LEONARDO NOACH