EthicsGlobal

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Código:	SOS-PCLI-PO-34-v1
Versión:	1.0
Fecha de la versión:	17-ene-2022
Creado por:	Javier Flores
Aprobado por:	Dirección General
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
17-sep-2018	1.0	Javier Flores	Primera versión.
17-ene-2022	1.0	Denice Arroyo	Revisión de versión

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar que se proteja la información en un nivel adecuado.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los tipos de información, independientemente del formato, ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas, etc.

Los usuarios de este documento son todos los empleados de EthicsGlobal.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- Política de seguridad de la información
- Informe de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Inventario de activos
- LFPDPPP de México y EU-GDPR
- Procedimiento para gestión de incidentes
- Procedimientos operativos para tecnología de la información y de la comunicación
- Política de Uso aceptable

3. Información clasificada

3.1. Pasos y responsabilidades

Los pasos y responsabilidades para la gestión de la información son los siguientes:

Nombre del paso	***Responsabilidad***
1. Ingreso del activo de información en el Inventario de activos	CISO
2. Clasificación de la información	Propietario del activo
3. Etiquetado de la información	Propietario del activo
4. Manejo de la información	Personas que poseen derechos de acceso de acuerdo con esta Política

Si la información clasificada proviene de afuera de la organización, el CISO es el responsable de su clasificación según las reglas establecidas en esta Política, y esta persona se convierte en el propietario de ese activo de información.

3.2. Clasificación de la información

3.2.1. Criterios de clasificación

El nivel de confidencialidad se determina de acuerdo a los siguientes criterios:

- Valor de la información: según los impactos evaluados durante la evaluación de riesgos.
- Sensibilidad y grado crítico de la información: según el mayor riesgo calculado para cada elemento de información durante la evaluación de riesgos.
- Obligaciones legales y contractuales.

3.2.2. Niveles de confidencialidad

Toda la información debe ser clasificada en niveles de confidencialidad.

Nivel de confidencialidad	***Etiquetado***	***Criterios de clasificación***	***Restricción de acceso***
Pública	(sin etiquetar)	Hacer pública la información no puede dañar a la organización de ninguna forma	La información está disponible para todo el público
Uso interno	USO INTERNO	El acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la organización	La información está disponible para todos los empleados y terceros seleccionados
Restringida	RESTRINGIDA	El acceso no autorizado a la información podría dañar considerablemente el negocio y/o la reputación de la organización	La información está disponible solamente para un grupo específico de empleados y de terceros autorizados
Confidencial	CONFIDENCIAL	El acceso no autorizado a la información podría dañar de forma catastrófica (irreparable) el negocio y/o la reputación de la organización	La información está disponible solamente para personas de la organización

La regla básica es utilizar el nivel de confidencialidad más bajo garantizando un adecuado nivel de protección para evitar gastos de protección innecesarios.

3.2.3. Lista de personas autorizadas

La información clasificada como "Restringida" y "Confidencial" debe estar acompañada de una Lista de personas autorizadas en la que el propietario de la información especifica los nombres o los cargos de las personas que tienen derechos de acceso para esa información.

La misma regla aplica para el nivel de confidencialidad "Uso interno" si las personas externas a la organización tendrán acceso a esos documentos.

3.2.4. Reclasificación

Los propietarios de activos deben revisar el nivel confidencialidad de sus activos de información al menos cada dos años y deben evaluar si se puede cambiar dicho nivel. Si es posible, deberían bajarlo.

3.3. Etiquetado de la información

Los niveles de confidencialidad son etiquetados de la siguiente forma:

- **Documentos en papel**: se indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento; también se indica en la portada o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.
- **Documentos electrónicos**: se indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento.
- **Sistemas de información**: el nivel de confidencialidad en aplicaciones y bases de datos debe ser indicado en la pantalla de acceso al sistema, como también en la esquina superior derecha de cada pantalla consecutiva que muestra información confidencial.
- **Correo electrónico**: se indica el nivel de confidencialidad en la firma del usuario.
- **Soporte de almacenamiento electrónico** (discos, tarjetas de memoria, etc.): se debe indicar el nivel de confidencialidad sobre la superficie de cada soporte.
- **Información transmitida oralmente**: el nivel de confidencialidad de la información confidencial que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

3.4. Manejo de información clasificada

Todas las personas que tienen acceso a información clasificada deben seguir las reglas enumeradas en el siguiente cuadro. El CISO debe activar acciones disciplinarias cada vez que se no se cumplan las reglas o si la información se transmite a personas no autorizadas. Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el Procedimiento para gestión de incidentes.

Los activos de información pueden ser llevados fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en la Política de uso aceptable.

El método para borrado y destrucción segura de soportes está establecido en el documento Procedimientos operativos para tecnología de la información y de la comunicación.

	Uso interno	*Restringida**	*Confidencial**
Documentos en papel	• Sólo las personas autorizadas pueden tener acceso. • Si es enviado fuera de la organización, el documento debe ser enviado por correo certificado. • Los documentos sólo pueden ser guardados en habitaciones sin acceso público. • Los documentos deben ser retirados frecuentemente de impresoras y máquinas de fax.	• El documento debe ser almacenado en un gabinete con llave. • Los documentos pueden ser transferidos dentro y fuera de la organización solamente en un sobre cerrado. • Si es enviado fuera de la organización, el documento debe ser enviado con acuse de recibo. • Los documentos deben ser retirados inmediatamente de impresoras y máquinas de fax. • Solamente el propietario del documento puede copiarlo. • Solamente el propietario del documento puede destruirlo.	• El documento debe ser almacenado en un gabinete con llave. • El documento puede ser transferido dentro y fuera de la organización solamente por una persona confiable y en un sobre cerrado y sellado. • No está permitido enviar el documento por fax. • Es posible imprimir el documento sólo si la persona autorizada está al lado de la impresora.
Documentos electrónicos	• Sólo las personas autorizadas pueden tener acceso. • Cuando se intercambian archivos a través de servicios como FTP, mensajería instantánea, etc., deben estar protegidos con clave. • El acceso a los sistemas de información en los que están almacenados los documentos debe estar protegido por una	• Sólo las personas con autorización para este documento pueden acceder a la parte del sistema de información en el que está guardado el documento. • Cuando se intercambian archivos a través de servicios como FTP, mensajería	• El documento debe ser almacenado en un formato encriptado. • El documento solamente puede ser archivado en servidores controlados por la organización. • El documento no debe ser intercambiado a través de servicios

	clave segura. • La pantalla en la que se muestra el documento debe bloquearse automáticamente luego de 5 minutos de inactividad.	instantánea, etc., deben estar encriptados. • Solamente el propietario del documento puede borrarlo.	como FTP, mensajería instantánea, etc.
Controles de auditoría	• Sólo las personas autorizadas pueden tener acceso. • El acceso al sistema de información debe estar protegido por una clave segura. • La pantalla debe bloquearse automáticamente luego de [cantidad] minutos de inactividad. • El sistema de información puede estar ubicado solamente en habitaciones con acceso físico controlado.	• Los usuarios deben finalizar la sesión en el sistema de información si abandonan temporal o permanentemente su lugar de trabajo. • Los datos deben ser borrados solamente con un algoritmo que garantice un borrado seguro.	• El acceso al sistema de información debe estar controlado mediante un proceso de autenticación que utilice tarjetas inteligentes o lectores biométricos. • El sistema de información solamente puede ser instalado en servidores controlados por la organización. • El sistema de información solamente puede estar ubicado en habitaciones con acceso físico controlado y con control de identidad de las personas.
Correo electrónico	• Sólo las personas autorizadas pueden tener acceso. • El remitente debe verificar cuidadosamente el destinatario. • Aplican todas las reglas mencionadas para "Sistemas de información".	• El correo electrónico debe estar encriptado si se envía fuera de la organización.	• Todos los correos electrónicos deben ser encriptados.
Soportes de	• Sólo las personas	• Los soportes y	• El soporte debe ser

almacenamiento electrónico	autorizadas pueden tener acceso. • Los soportes o archivos deben estar protegidos con clave. • Si es enviado fuera de la organización, el soporte debe ser enviado por correo certificado. • El soporte solamente puede ser guardado en habitaciones con acceso físico controlado.	archivos deben estar encriptados. • El soporte debe ser almacenado en un gabinete con llave. • Si es enviado fuera de la organización, el soporte debe ser enviado con acuse de recibo. • Sólo el propietario del soporte puede borrar sus datos o destruirlo.	almacenado en una caja fuerte. • El soporte puede ser transferido dentro y fuera de la organización solamente por una persona confiable y en un sobre cerrado y sellado.
Información transmitida oralmente	• Sólo las personas autorizadas pueden tener acceso a la información. • Las personas no autorizadas no deben estar presentes en la habitación cuando se comunica la información.	• La habitación debe tener aislamiento acústico. • La conversación no debe ser grabada.	• La conversación mantenida a través de vías de comunicación debe ser encriptada. • No se debe guardar ninguna transcripción de la conversación.

*Los controles se implementan acumulativamente; es decir, los controles para cualquier nivel de confidencialidad conllevan los controles definidos para los niveles inferiores: si se establecen controles más estrictos para un nivel de confidencialidad mayor, sólo se implementan esos controles.

4. Gestión de registros guardados con base en este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Lista de personas autorizadas con acceso a los documentos	Junto con la información en la que se indica el nivel de confidencialidad	Propietario del activo de información	El mismo que para la protección de información	Debe existir la lista siempre que exista la información propiamente dicha

5. Validez y gestión de documentos

Este documento es válido hasta el 05-may-2022.

El propietario de este documento es el CISO que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con el acceso no autorizado a la información.
- Cantidad de activos de información clasificados con un nivel de confidencialidad inadecuado.