POLÍTICA DE USO ACEPTABLE

Versión 1.0
7. Apoyo

Código:	POL-07/024/V1.0-Política de uso aceptable
Versión:	1.0
Fecha de emisión:	2025
Creador por:	Depto. Seguridad de la Información
Responsable:	Coordinación del SGSI
Revisión	Anual o ante cambios regulatorios
Nivel de Confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28-may-25	1.0	Coordinación del SGSI	Creación de documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en EthicsGlobal.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del SGSI.

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

2. Documentos de referencia

• Norma ISO/IEC 27001, capítulos A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
• Política de seguridad de la información
• Política de Clasificación de la Información
• Procedimiento para gestión de incidentes
• Inventario de activos
• Procedimientos operativos para tecnología de la información y de la comunicación
• Política de Transferencia de la Información

3. Uso aceptable de los activos de información

3.1. Definiciones

Sistema de información: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la organización, o que se encuentran bajo responsabilidad de la organización. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

Activos de información: en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

3.2. Uso aceptable

Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades de negocios con el objetivo de ejecutar tareas vinculadas con la organización.

3.3. Responsabilidad sobre los activos

Cada activo de información tiene designado un propietario en el Inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

3.4. Actividades prohibidas

Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad. También está prohibido:

- Descargar archivos de imágenes o vídeos que no tienen objetivos de negocios, enviar cadenas de correos electrónicos, jugar juegos, etc.
- Instalar software en un ordenador local sin el permiso explícito del Coordinador del SGSI.
- Utilizar aplicaciones Java, controles Active X y otros códigos móviles, excepto cuando esté autorizado por el Coordinador del SGSI.
- Utilizar herramientas criptográficas (encriptado) sobre ordenadores locales, excepto en los
- casos especificados en la Política de Clasificación de la Información y cuando el Coordinador del SGSI determine la sensibilidad de la información de algún equipo.
- Descargar códigos de programa de soportes externos.
- Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (por ej., dispositivos USB) sin el permiso explícito del Coordinador del SGSI; el uso en conformidad con la Política de Clasificación de la Información está permitido.

3.5 Uso de activos fuera de las instalaciones

Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo del Coordinador del SGSI por medio de la herramienta de gestión de proyectos de TI o el registro por TI.

Mientras los activos en cuestión permanecen fuera de la organización, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

3.5. Devolución de activos a la finalización de un contrato

Al finalizar un contrato de empleo, o de otro tipo, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todos esos activos de información al propietario del activo.

3.6. Procedimiento para copias de seguridad

El usuario debe organizar los archivos que utiliza para sus labores dentro de su mismo equipo para posteriormente publicar su trabajo en la carpeta del Share Drive que se le indicó para tal propósitos.

3.7. Protección antivirus

En cada ordenador debe estar instalado Avast antivirus o similar con actualización automática activada.

3.8. Facultados para el uso de sistemas de información

Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.

Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.

Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.

3.10. Responsabilidades sobre la cuenta de usuario

El usuario no debe, directa ni indirectamente, permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario; y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido.

El propietario de la cuenta de usuario es su usuario, que es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

3.11. Uso de Internet

Sólo se puede acceder a Internet a través de la red local de la organización, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo de los dispositivos de EthicsGlobal a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet, está prohibido.

El Coordinador del SGSI puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados de la organización. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita por cualquier canal al Coordinador del SGSI solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.

El usuario debe considerar como no confiable la información recibida a través de sitios web no verificados. Ese tipo de información puede ser utilizado con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.

3.12. Correo electrónico y otros métodos de intercambio de mensajes

Entre los métodos de intercambio de mensajes, aparte del correo electrónico, se puede incluir la descarga de archivos desde Internet, la transferencia de datos por medio de JIRA, Workplace, teléfonos, equipos de fax, el envío de mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

De acuerdo con la Política de Transferencia de la Información, como también con la Política de Clasificación de Información, el Coordinador del SGSI determina el canal de comunicación que se puede utilizar para cada tipo de dato, como también las posibles restricciones sobre quién tiene permiso para utilizar los canales; es decir, define qué actividades están prohibidas.

Los usuarios solamente pueden enviar mensajes que contengan información veraz. Está prohibido enviar materiales perturbadores, desagradables, sexualmente explícitos, groseros, difamatorios o cualquier otro contenido inaceptable o ilegal. Los usuarios no deben enviar mensajes basura a personas con las cuales no se ha establecido relación de negocios o a personas que no solicitaron ese tipo de información.

Si un usuario recibe un correo electrónico basura con contenido desagradable, ofensivo o con contenido que atente contra la seguridad de la información, debe informarlo al Coordinador del SGSI.

Si se envía un mensaje con una etiqueta de confidencialidad, el usuario debe protegerlo de acuerdo con lo establecido en la Política de Clasificación de Información.
El usuario debe guardar todos los mensajes que contienen datos importantes para los negocios de la organización utilizando el método especificado por el Coordinador del SGSI.
Cada correo electrónico debe incluir una exención de responsabilidad, salvo los mensajes enviados a través de los sistemas de comunicación determinados por el Coordinador del SGSI. Si un usuario envía un mensaje a través de un sistema de intercambio de mensajes (redes sociales, foros, etc.), debe declarar sin ambigüedades que no representa el punto de vista de la organización.

3.13. Derechos de autor

Los usuarios no deben realizar copias no autorizadas del software que pertenece a la organización, excepto en los casos permitidos por ley, por el propietario o por el Coordinador del SGSI.

Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

3.14. Computación móvil

Todo lo relacionado a computación móvil se encuentra documentado en la Política sobre Dispositivos Móviles y Tele-trabajo.

3.15. Supervisión del uso de sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación de la organización, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se considera propiedad de EthicsGlobal.

Los usuarios aceptan que personas autorizadas de la organización puedan acceder a todos los datos de ese tipo y que el acceso de dichas personas no será considerado una violación de privacidad del usuario.

La organización puede utilizar herramientas especializadas para identificar y bloquear métodos prohibidos de comunicación y para filtrar contenidos prohibidos.

3.16. Incidentes

Cada empleado, proveedor o tercero que esté en contacto con datos y/o sistemas de EthicsGlobal debe reportar toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente, de acuerdo a lo establecido en el Procedimiento para gestión de incidentes.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Autorizaciones para instalación de software, uso de aplicaciones Java y controles Active X, uso de herramientas criptográficas, descarga de códigos de programas desde soportes externos, instalación de dispositivos periféricos - formato electrónico	Tarea/ticket en JIRA	Coordinador del SGSI	Los registros no pueden ser editados, sólo el Coordinador del SGSI puede guardar estos registros	Los registros son almacenados por el plazo de 3 años.

Autorizaciones para retirar activos fuera de las instalaciones - formato electrónico	Carpeta en Share Drive.	Coordinador del SGSI	Los registros no pueden ser editados, sólo el Coordinador del SGSI puede guardar estos registros	Los registros son almacenados por el plazo de 3 años.
Autorización para acceder a determinadas páginas de Internet - formato electrónico	Carpeta en Share Drive.	Coordinador del SGSI	Los registros no pueden ser editados, sólo el Coordinador del SGSI puede guardar estos registros	Los registros son almacenados por el plazo de 3 años.
Autorización para tele-trabajo - formato electrónico	Carpeta en Share Drive.	Coordinador del SGSI	Los registros no pueden ser editados, sólo el Coordinador del SGSI puede guardar estos registros	Los registros son almacenados por el plazo de 3 años.

Solamente el Coordinador del SGSI puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.

4. Validez y gestión de documentos

Esta política será revisada anualmente por el Comité de Seguridad de la Información o, cuando ocurra un cambio significativo en los roles organizacionales.

El propietario de este documento es el Coordinador del SGSI 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 uso inadecuado o no autorizado de los activos de información.
• Cantidad de incidentes relacionados con inadecuados programas de capacitación o de concienciación de empleados sobre el uso aceptable de los activo de información.

Representante de la Dirección General
Liuva Anahí Figueroa Gracián