**Política de uso aceptable**

**1. Introducción**

El objetivo de esta política es proporcionar un marco amplio y general para que todos los usuarios de las computadoras, teléfonos y servicios de internet de la Universidad Dō comprendan su uso permitido. Esta política no abarca todas las circunstancias, por lo que se recuerda a todos los usuarios que se adhieran a su espíritu general.

**2. Historial de revisiones**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Autor** | **Resumen de cambios** |
| 5 |  | Diana Stirbu | Agregar historial de revisionesAgregar referencia a la política de uso aceptable de Janet Agregar referencia a grabaciones telefónicas Cambiar las referencias de 'CSU' a 'Servicios de TI' Revisar las cláusulas de escritorio limpioRevisar las cláusulas esenciales sobre ciberseguridad |
| 5.1 | 24 de noviembre | Elisabeth Almodovar | Añadir referencias a KCSIE y PREVENT Duty Añadir sección de Inteligencia Artificial Añadir texto del asistente de reuniones de IA |
| 5.11 | 24 de diciembre | ElisabethAlmodovar | Modificaciones menores en la gobernanza de la información |

**3. Alcance de esta Política**

3.1 Esta política se aplica a cualquier persona que utilice las instalaciones de Tecnologías de la

 Información (TI) proporcionadas por la Universidad Dō. Esto incluye a nuestro personal, estudiantes, miembros del consejo directivo, contratistas y visitantes. A lo largo de la política, estas personas se denominarán «usuarios».

3.2 Las instalaciones de TI son vitales para el funcionamiento de la Universidad Dō. Esta política establece el marco dentro del cual los usuarios pueden utilizar las instalaciones de TI.

3.3 La frase “instalaciones de TI” abarca, pero no se limita a, computadoras, software, dispositivos periféricos, identidades emitidas por el la Universidad Dō, recursos en línea o basados en la nube, correo electrónico, teléfonos, acceso a Internet, incluido WiFi y datos almacenados dentro de sistemas informáticos.

3.4 El término «datos personales» se define según la Ley de Protección de Datos. En este contexto, el Grupo se considera responsable del tratamiento de datos.

3.5 El Grupo solicitará la conformidad explícita de todos los usuarios de que han leído y comprendido esta política. Una forma de obtener esta conformidad es mediante la lista de verificación de inducción o el formulario de declaración que se encuentra al final de esta política. Los usuarios también recibirán recordatorios periódicos de que el uso de las instalaciones de TI del Grupo debe cumplir con esta política.

3.6 Esta política debe leerse junto con:

• Política de seguridad informática

• Política de Protección de Datos

• Política de retención de registros

• Código de conducta del personal

• Política de uso aceptable de Janet (https://community.jisc.ac.uk/

library/acceptable-use-policy)

**4. Distribución**

4.1 Esta política, junto con todas las demás, está disponible en la intranet del personal. Durante su inducción, se informará a todo el personal dónde encontrar las políticas del Grupo, incluida esta.

4.2 Una versión abreviada de esta política se muestra durante el proceso de inicio de sesión de la

 computadora.

**5. Uso aceptable**

5.1 En general:

• Las instalaciones informáticas se proporcionan como recursos para apoyar las actividades diarias del Grupo, por ejemplo, para seguir un programa de estudios. Si tiene dudas sobre si el uso previsto de estos recursos está relacionado con la actividad empresarial, consulte primero con su superior inmediato.

• No debe interferir intencionalmente con el funcionamiento de las instalaciones de TI, las computadoras del Grupo, la red o los sistemas de telefonía; ni conectar o desconectar ningún dispositivo; ni instalar ningún software; ni intentar obtener acceso a sistemas restringidos sin la aprobación previa de los Servicios de TI.

• Una identidad de usuario solo puede ser utilizada por la persona a quien se le otorga. Esta persona es responsable del uso y la protección de las credenciales.

• El software solo debe utilizarse de acuerdo con los términos de la licencia.

• Los usuarios deberán utilizar una contraseña única que cumpla con los requisitos de complejidad y se actualice según lo descrito en la guía del Centro Nacional de Seguridad Cibernética y la Política de Seguridad de TI.

• Los usuarios deben cerrar la sesión o bloquear su estación de trabajo cuando dejen su computadora, tableta o dispositivo móvil desatendido para evitar el acceso no autorizado a las instalaciones de TI.

• Los usuarios deben mantener la pantalla limpia para evitar que personas no autorizadas vean fácilmente la información que muestran o que sea captada por cámaras u otros dispositivos de grabación cercanos. También deben considerar la información que está abierta en el dispositivo para evitar que se comparta información personal y confidencial al compartir la pantalla a través de software de videoconferencia.

• Los usuarios deben mantener un “escritorio limpio”, asegurándose de que todo el papeleo y los medios extraíbles estén guardados bajo llave antes de dejar el escritorio desatendido.

• Los usuarios deberán cumplir con todas las obligaciones legales, estatutarias y contractuales que sean relevantes para su función.

• Al abandonar el Grupo, los usuarios deben informar a su superior de línea antes de la partida sobre cualquier información importante contenida en su cuenta y, de ser así, asegurarse de que su superior de línea tenga acceso a ella antes de su partida.

5.2 Los requisitos de protección de datos son:

• Todo el personal debe cumplir con la política de Protección de Datos del Grupo en el manejo de datos personales.

• La creación de conjuntos de datos de estudiantes fuera del Sistema de Información de Gestión de Grupos debe ser aprobada previamente por el director de Información y Financiamiento. Es posible que se le solicite que complete una Evaluación de Impacto de la Protección de Datos antes de obtener la aprobación.

• Los usuarios no deben almacenar datos personales en dispositivos móviles (tabletas, smartphones, relojes inteligentes, etc.), dispositivos de almacenamiento portátiles (memorias USB, discos duros

extraíbles, etc.) ni en servicios de almacenamiento en la nube no proporcionados por el Grupo (Dropbox, OneDrive, etc.) sin una evaluación de riesgos aprobada por el director de Tecnologías de la Información. Esta evaluación de riesgos puede adoptar la forma de una Evaluación de Impacto

de la Privacidad de Datos.

• Los usuarios deben tomar precauciones para proteger todos los medios informáticos y dispositivos móviles cuando los lleven fuera de las instalaciones del Grupo (por ejemplo, evitar dejar una computadora portátil desatendida o en exhibición en un automóvil de manera que pueda fomentar un robo oportunista).

• Los usuarios no deben utilizar su dirección de correo electrónico de trabajo para suscribirse a boletines informativos por correo electrónico o registrarse en cuentas de redes sociales sin un uso comercial claro que les permita hacerlo.

• Todo intercambio de datos clasificados, incluidos los datos personales, con organismos externos debe realizarse de forma segura. Los métodos seguros de intercambio de datos incluirán el cifrado, la transferencia directa y el uso de terceros de confianza. Dicho intercambio de datos también deberá ajustarse al uso permitido por la política y los avisos de protección de datos del Grupo, o se solicitará la autorización de las personas implicadas.

• No está permitido enviar datos personales a través de WhatsApp u otros mensajeros de redes sociales no autorizados.

• No se permite el envío de datos personales por fax. El fax se considera inseguro y, por lo tanto, no es adecuado para enviar ni recibir información de clasificación superior a la pública.

5.3 Los requisitos de privacidad son:

• El acceso al correo electrónico y al almacenamiento de archivos de un miembro del personal podrá otorgarse al superior inmediato o a otro miembro del personal que este delegue. Dichas solicitudes deberán presentarse por escrito al director de Tecnología de la Información por parte del superior inmediato y el acceso solo se concederá cuando exista una justificación comercial clara.

• Se podrá acceder al correo electrónico y al almacenamiento de archivos del usuario, así como a la información proporcionada, para cumplir con los requisitos legales. Esto incluye

las obligaciones del Grupo en virtud de la legislación en materia de protección de datos y libertad de información.

• Dado que se puede otorgar acceso al almacén de archivos y al correo electrónico a terceros sin el consentimiento del usuario, este no debe asumir que su almacén de archivos o correo electrónico es privado. No se deben almacenar ni transmitir asuntos personales confidenciales en las instalaciones de TI del Grupo.

• El Grupo supervisa el uso de sus sistemas informáticos y telefónicos para mantener la eficiencia y evitar el uso indebido. También se realiza un seguimiento para identificar y escalar las preocupaciones de protección y para cumplir con los requisitos sectoriales y legales, incluyendo la Protección Infantil en la Educación y la obligación de PREVENIR.

• El Grupo podrá monitorizar las llamadas telefónicas para garantizar un servicio al cliente satisfactorio. En caso de monitorización de una llamada, se notificará a todas las partes implicadas.

• Las llamadas entrantes a los teléfonos fijos del Grupo se graban hasta que la centralita las desvía a una nueva extensión. Este tratamiento se describe en un aviso de privacidad en el sitio web del Grupo y en un mensaje automático al inicio de la llamada.

• Los usuarios deben proteger la información clasificada que envíen, reciban, almacenen o procesen ellos mismos, según el nivel de clasificación asignado, incluyendo copias electrónicas y en papel. Todo material que creen debe estar debidamente etiquetado.

• Los usuarios deben ser conscientes de su entorno de trabajo para asegurarse de que no sean pasados por alto ni escuchados por personas no autorizadas cuando trabajan y deben tener el debido cuidado cuando trabajen con información clasificada.

5.4 Los requisitos del correo electrónico son:

• Se agregará un 'descargo de responsabilidad' o 'pie de página' de grupo a todos los correos electrónicos salientes.

• Todas las conversaciones por correo electrónico con terceros deben considerarse escritas con membrete del Grupo y deben adoptarse las normas de etiqueta y formalidad adecuadas. Los correos electrónicos deben redactarse siguiendo las mejores prácticas de correo electrónico.

Etiqueta. La guía de la Biblioteca Británica es un ejemplo de buenas prácticas de etiqueta para correo electrónico.

• Los usuarios se asegurarán de haber ingresado correctamente la(s) dirección(es) de correo electrónico del destinatario antes de enviar el mensaje, para evitar que se vulnere la información clasificada. Si la dirección de correo electrónico no debe divulgarse, debe colocarse en el campo de copia oculta (CCO).

• Los usuarios no deben representar sus propios puntos de vista como los del Universidad

 Dō ni implicar la formación de un contrato entre el Grupo y un tercero.

• No se debe enviar, recibir ni reenviar intencionalmente material que pueda considerarse obsceno, ilegal o difamatorio o que tenga como objetivo molestar, acosar o intimidar a otra persona.

• Todo el correo electrónico será analizado automáticamente para identificar virus y correo masivo no deseado (también conocido como spam). No se aceptará ningún correo electrónico procedente de direcciones incluidas en la lista negra.

• Se limitará el tamaño de los buzones electrónicos y se eliminarán los archivos obsoletos sin previo aviso. Se aplicarán plazos de retención al sistema de correo electrónico del Grupo. Consulte la política de retención de registros para conocer los plazos de retención aplicables a cada carpeta del buzón.

5.5 Los requisitos de Internet son:

• El Grupo registrará y filtrará el uso de Internet por parte de nuestros usuarios de acuerdo con nuestros requisitos sectoriales y legales, incluidos los de mantener a los niños seguros en la educación y el deber de PREVENIR.

• No está permitido el uso no autorizado de software de mensajería instantánea o de intercambio de archivos peer to peer.

• Los usuarios no deben cargar ni descargar materiales que violen los derechos de autor.

• Los usuarios no deben acceder ni distribuir material que no represente los valores fundamentales del grupo. Esto incluye material que pueda considerarse obsceno, ilegal, difamatorio o que pueda acosar o intimidar a otros.

5.6 Uso de dispositivos personales:

• El uso de dispositivos personales para acceder a los sistemas del Grupo se realiza a riesgo del propietario y el Grupo no acepta ninguna responsabilidad.

• Se desaconseja el almacenamiento de datos personales del Grupo Holding en dispositivos personales, y se deben implementar las medidas de seguridad adecuadas para garantizar su protección contra la divulgación no autorizada. Se considera que un dispositivo cuenta con las medidas de seguridad adecuadas si cumple con todos los criterios de la especificación de ciberseguridad vigente, disponible en el sitio web.

• La inscripción de un dispositivo personal en un servicio del Grupo donde los datos personales relacionados con el Grupo pueden transferirse al dispositivo implica la aceptación de que el Grupo pueda:

− Borrar los datos de forma remota en caso de que la persona abandone su empleo en el Grupo o se pierda el dispositivo.

− Imponga un nivel mínimo de seguridad de forma remota (por ejemplo, cifrado,

 acceso con PIN, bloqueo de pantalla).

− Requerir la instalación de software adicional en el dispositivo para admitir el uso seguro del servicio (como Microsoft Authenticator para admitir la autenticación multifactor).

5.7 Uso de herramientas de Inteligencia Artificial

• Las herramientas de IA no deben utilizarse para falsificar la imagen humana sin consentimiento expreso. Esto incluye, entre otros, texto, imágenes y vídeos.

• Uso de asistentes de reuniones con IA

Los asistentes de reuniones con IA suelen almacenar las transcripciones y otros datos de las reuniones, como vídeos o direcciones de correo electrónico, en ubicaciones no autorizadas y bajo diversos y complejos acuerdos de privacidad. Estos pueden ser invitados a la reunión por otros participantes, a veces automáticamente. El organizador de la reunión debe asegurarse de interrogar a cualquier participante externo no reconocido.

Si está utilizando una herramienta de IA para la transcripción de reuniones, entonces debe

Informar a los participantes de la reunión y obtener su consentimiento antes de unirse a la herramienta a la reunión.

La única herramienta aprobada para Microsoft Teams es la función de transcripción integrada. Si necesita más funciones, consulte con el Equipo de Gobernanza de la Información para usar otro producto.

5.8 El propósito principal del suministro de sistemas informáticos, de red o telefónicos es apoyar las actividades del Grupo. Se permite un uso personal limitado según los términos de esta política y lo siguiente:

• Siempre debe darse prioridad al propósito principal del servicio.

• El uso personal no debe interferir con el correcto funcionamiento del servicio.

• El uso personal de Internet sólo se realiza fuera de la jornada laboral (o durante los descansos) y no debe afectar al desempeño de las funciones del usuario.

• El uso personal no debe estar relacionado con el funcionamiento de una empresa ni entrar en conflicto con las responsabilidades de un miembro del personal como empleado del Grupo.

• El Grupo se reserva el derecho de recuperar los costes del uso personal excesivo.

**6. Consecuencias del mal uso**

6.1 El incumplimiento de esta política podrá dar lugar a medidas disciplinarias. Se podrá retirar el acceso a las instalaciones informáticas y telefónicas en espera del resultado de una investigación o de una medida disciplinaria.

6.2 Es responsabilidad legal del Grupo remitir a la Policía la descarga, visualización o almacenamiento de ciertos materiales (por ejemplo, imágenes ilegales de menores).

6.3 Si un usuario detecta, sospecha o presencia un incidente que pueda suponer una brecha de seguridad o observa cualquier sospecha de debilidad de seguridad de la información en los sistemas o servicios, deberá comunicarlo inmediatamente al delegado de Protección de Datos.

**7. Estado de esta Política**

7.1 Esta política se ha elaborado aplicando las mejores prácticas de la norma ISO 27001 y forma parte del compromiso del Grupo con la obtención y el mantenimiento de las certificaciones de

7.2

ciberseguridad. El director de Operaciones del Grupo supervisará periódicamente su aplicación.

Tecnologías de la información.

|  |  |
| --- | --- |
| Área de Revisión de Políticas | ÉL |
| Gerente principal/Propietario de la política | Director de Grupo de Tecnología de la Información |
| Nivel de aprobación | Equipo de liderazgo del grupo |
| Fecha de aprobación | Marzo de 2025 |
| Ciclo de revisión | Cada dos años |
| Siguiente revisión | marzo de 2027 |

**Declaración de política de uso aceptable**

Cualquier usuario de las instalaciones de TI del Grupo que no haya firmado un contrato de empleo con el Grupo debe leer y aceptar la Política de uso aceptable, firmar la siguiente declaración y devolver esta página a Recursos Humanos antes de que se pueda solicitar inicio de sesión en cualquier PC.

Esta declaración firmada debe proporcionarse a los Servicios de TI junto con la solicitud de inicio de sesión de PC enviada a la mesa de ayuda de Servicios de TI.

**Declaración**

Confirmo que he leído y comprendido la Política de uso aceptable y que debo cumplirla en todo momento.

Soy consciente de que cualquier incumplimiento de esta política puede dar lugar a la retirada del acceso a la TI y a medidas adicionales.

Nombre:

Firmado:

Fecha: