

SISTEMA DE GESTIÓN INTEGRADO · TIM-PO-02

POLÍTICA DE SEGURIDAD DE TI

Reglas para el uso aceptable de los sistemas y activos de información de Actuaría Consultores.



POLÍTICA DE SEGURIDAD DE TI

Código:	TIM-PO-02
Versión:	1.0
Fecha de la versión:	2025.07.28
Elaborado por:	Equipo de Proyecto y Roadquality
Revisado por:	Innovation Manager
Aprobado por:	Chief Digital Officer
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
2025.07.28	1.0	Consultora Road Quality - Equipo de Proyecto SGI	Detalle básico del documento

Tabla de Contenido

1.	OBJETIVO, ALCANCE Y USUARIOS	3
2.	DOCUMENTOS DE REFERENCIA	3
3.	USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN	3
3.1.	DEFINICIONES	3
3.2.	USO ACEPTABLE	3
3.3.	RESPONSABILIDAD SOBRE LOS ACTIVOS	4
3.4.	ELIMINACIÓN DE INFORMACIÓN	4
3.5.	ACTIVIDADES PROHIBIDAS	4
3.6.	USO DE ACTIVOS FUERA DE LAS INSTALACIONES	4
3.7.	DEVOLUCIÓN DE ACTIVOS A LA FINALIZACIÓN DE UN CONTRATO	4
3.8.	PROCEDIMIENTO PARA COPIAS DE SEGURIDAD	4
3.8.1	Copias de seguridad de información en respaldo local	5
3.8.2	Copias de seguridad de información de sistemas	5
3.8.3	Copias de seguridad de información de bases de datos	5
3.9.	PROTECCIÓN ANTIVIRUS/MALWARE	6
3.10.	FACULTADOS PARA EL USO DE SISTEMAS DE INFORMACIÓN	6
3.11.	RESPONSABILIDADES SOBRE LA CUENTA DE USUARIO	6
3.12.	RESPONSABILIDADES SOBRE LA CLAVE	6
3.13.	GESTIÓN DE LAS CLAVES COMPARTIDAS	7
3.14.	POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS	7
3.14.1.	Política de escritorio limpio	8
3.14.2.	Política de pantalla limpia	8
3.14.3.	Protección de instalaciones y equipos compartidos	8
3.15.	USO DE INTERNET	8
3.16.	CORREO ELECTRÓNICO Y OTROS MÉTODOS DE INTERCAMBIO DE MENSAJES	9
3.17.	DERECHOS DE AUTOR	10
3.18.	COMPUTACIÓN MÓVIL	10
3.18.1.	Introducción	10
3.18.2.	Reglas básicas	10
3.19.	TELETRABAJO Y TRABAJO DESDE CASA	11
3.19.1.	Introducción	11
3.19.2.	Normas adicionales para el teletrabajo	11
3.20.	SUPERVISIÓN DEL USO DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN	13
3.21.	INCIDENTES	13

4.	GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO	13
5.	VALIDEZ Y GESTIÓN DE DOCUMENTOS	14

1. Objetivo, alcance y usuarios

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

Este documento se aplica a todo el alcance del Sistema de Gestión de Sistema Integrados (SGI); es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del SGI.

Los usuarios de este documento son todos los colaboradores de Actuaria Consultores.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19 y A.8.23
- Política de seguridad de la información
- Política de clasificación de la información
- Procedimiento para gestión de incidentes
- Inventario de activos
- Procedimientos operativos para el departamento de TI
- Política de transferencia de información

3. Uso aceptable de los activos de información

3.1. Definiciones

Sistema de información: incluye todos los servidores en la nube 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, medios 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. Eliminación de información

Cuando ya no sea necesario, el propietario del activo debe eliminar la información confidencial almacenada en su ordenador o dispositivo móvil.

3.5. 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 IT Specialist .
- Utilizar aplicaciones Java, controles Active X y otros códigos móviles, excepto cuando esté autorizado por el IT Specialist.
- Utilizar herramientas criptográficas (encriptado) sobre ordenadores locales, excepto en los casos especificados en la Política de clasificación de la información.
- Descargar códigos de programa de medios 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 IT Specialist; el uso en conformidad con la Política de clasificación de la información está permitido.

3.6. Uso de activos fuera de las instalaciones

Los equipos, la información o software, independientemente de su formato o medio de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo del IT Specialist.

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.

3.7. 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 físico, el usuario debe devolver todos esos activos de información al IT Specialist y debe estar informado de la devolución la Head of HR.

3.8. Procedimiento para copias de seguridad

Se deben crear copias de seguridad para todos los sistemas identificados en el Plan de continuidad de negocio y con la frecuencia según dicha estrategia. Existen 3 tipos de copias de seguridad según el sistema que lo necesita:

- Copias de seguridad de información en respaldo local.
- Copias de seguridad de la información de los sistemas.
- Copias de seguridad de la información en bases de datos.

3.8.1 Copias de seguridad de información en respaldo local

El IT Specialist es el responsable de crear copias de seguridad de información de respaldo local de los computadores de los colaboradores y garantizar que las fallas en las copias de seguridad programadas se aborden adecuadamente. La tecnología utilizada para las copias de seguridad de respaldo local en los computadores de los colaboradores es mediante Google Drive. El IT Specialist al entregar la computadora al colaborador le entrega configurado con las copias de seguridad dentro de las carpetas de “Escritorio” y “Documentos”. Las copias de seguridad se ejecutan dependiendo de la conexión a internet. Si la computadora del colaborador se encuentra conectada a internet, esta se realiza al momento que una de estas dos carpetas detecta cambio ya sea que se agregue, se elimine o se modifique un archivo mediante un proceso síncrono. Si la computadora del colaborador no se encuentra conectada a internet, el respaldo se realiza apenas detecte conexión nuevamente.

3.8.2 Copias de seguridad de información de sistemas

El IT Specialist es el responsable de las copias de seguridad relacionadas en la nube de **Google Workspace** y garantizar que las fallas en las copias de seguridad programadas se aborden adecuadamente.

Se manejan una automatización en las que se capturan los logs de todos los archivos y sistemas en línea y se registra en Google Drive.

Se registran logs de cambios, toda actividad de usuario, es decir, evidencia de cambios o modificaciones en la configuración de servidores, nubes y todo componente que está en la infraestructura. La retención de esta información es mientras exista el activo.

3.8.3 Copias de seguridad de información de bases de datos

El Head of IT es el responsable de las copias de seguridad relacionadas con las bases de datos, mismas que se encuentran en la nube, y también es responsable de garantizar que las fallas en las copias de seguridad programadas se aborden adecuadamente.

Para este tipo de copias de seguridad se maneja dependiendo del tipo de base de datos:

3.8.4 Bases de Firestore y Firestore realtime en Google Workspace

Se hace backups diarios, completo (copia de seguridad continua PITR), empieza la 7:30 am en la zona horaria Bogotá, Lima, Quito y almacena toda la información de las bases de datos de la operación del día. Estos backups tienen una política de retención de 7 días, pasados esos 7 días se retienen por 98 días adicionales y luego se elimina esa copia una vez creada la copia de seguridad de dicho día. Se mantiene de esta manera para poder retornar al momento del tiempo y reducir la pérdida de información, pero se busca mantener las últimas versiones.

3.9. Protección antivirus/malware

En cada ordenador debe estar instalado el antivirus Fortinet con actualización automática activada.

3.10. 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.

3.11. 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 es responsable por su uso y de todas las transacciones realizadas con su usuario y contraseña de la cuenta.

3.12. Responsabilidades sobre la clave

Los usuarios deben aplicar las siguientes buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- No se deben revelar las claves a otras personas, incluyendo la dirección y los administradores del sistema.
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por Head of IT.
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.).
- Las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas o el sistema (en ese caso, se debe informar como un incidente de seguridad de la información).
- Se deben escoger claves seguras de la siguiente forma:
 - utilizando al menos
 - 8 caracteres para cuentas por defecto o administradoras;
 - 8 caracteres para cuentas de usuarios con permisos de acceso por debajo de administrador;
 - utilizando al menos un carácter numérico;
 - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;

- utilizando al menos un carácter especial;
- una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás;
- las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);
- no se deben usar nuevamente las últimas cuatro (4) claves.
- Se deben cambiar las claves cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).
- No se deben utilizar las mismas claves personales para fines privados y para fines comerciales.
- Aplicar un método de autenticación de doble factor en los sistemas de información que sea posible activarlo

3.13. Gestión de las claves compartidas

Cuando se asignan y utilizan claves de usuarios que son compartidas, la plataforma a la que se le puede dar acceso compartido debe cumplir las siguientes reglas:

- Haber pasado al menos una ronda de evaluación de riesgos y no ser activos de información críticos, considerando que:
Considerando la Metodología de Evaluación y Tratamiento de riesgos de la organización; un activo de información no es crítico, cuando en la evaluación el Valor Total del Riesgo se encuentra en bajo, es decir, son activos de información con riesgos aceptables y la acción para el riesgo es de Monitoreo.
- El IT Specialist debe llevar una lista de los sistemas o plataformas de información con credenciales compartidas.
- El IT Specialist debe llevar el control de quiénes tienen las credenciales de acceso compartidas para cada plataforma con estas características.
- Cuando un colaborador que tiene acceso a cualquier plataforma con credenciales de uso compartido cesa sus funciones de la organización, el IT Specialist debe cambiar la contraseña de ese acceso compartido.
- El IT Specialist debe revisar quiénes conservan el acceso para actualizar la nueva contraseña.

El IT Specialist debe realizar un monitoreo cada 3 meses a los accesos de los sistemas o plataformas con claves compartidas.

3.14. Política de escritorio y pantalla limpios

Toda la información clasificada como "Uso interno", "Restringido" o "Confidencial" de acuerdo a lo establecido en la Política de clasificación de la información, es considerada sensible para este punto.

3.14.1. Política de escritorio limpio

Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los dispositivos móviles (terminales), y los medios de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopadoras, etc.) para evitar el acceso no autorizado a los mismos.

Este tipo de documentos, dispositivos móviles y medios deben ser archivados de forma segura, de acuerdo a lo establecido en la Política de clasificación de la información. Cuando los documentos y los medios de almacenamiento ya no sean necesarios, deben eliminarse de acuerdo con la Política de eliminación y destrucción.

3.14.2. Política de pantalla limpia

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 5 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave. Si la persona se ausenta por un período más prolongado (superior a 6 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el puesto de trabajo.

La información de las pizarras (p. ej., las disponibles en las salas de reuniones) debe borrarse cuando ya no se necesite.

3.14.3. Protección de instalaciones y equipos compartidos

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras y fotocopadoras.

Las instalaciones para envío y recepción de correo en Actuaria Consultores están protegidas por la disposición de que solo la Executive Assistant of the CEO es la autorizada para el uso de la impresora y demás componentes compartidos o bajo su autorización.

El uso no autorizado de impresoras, fotocopadoras, escáneres y demás equipamiento compartido para copiado se evita, ya que todos los colaboradores cuentan con una autorización y drivers que permiten en su equipo poder imprimir.

Antes de abandonar las instalaciones por un período más prolongado o de forma permanente, se debe realizar una inspección detallada de las habitaciones, las oficinas y el mobiliario que se encuentra en ellas para asegurarse de que no se dejen atrás los bienes de Actuaria Consultores.

3.15. Uso de Internet

A internet solo se puede acceder mediante la RED inalámbrica "Actuaria General". Como red secundaria se encuentra la RED "Actuaria-IoT y de invitados "Actuaria_Invitados y la red para dispositivos móviles "Actuaria_moviles". El router de la red de Actuaria Consultores maneja un cortafuegos estricto que solo permite acceso a páginas con categorías

autorizadas. El router de la red de invitados maneja un bloqueo a cualquier servicio de categorías bloqueadas y a servicios internos de la empresa.

Para el acceso remoto, las computadoras aplican un doble factor de autenticación asegurando su acceso mediante clave y contraseña de acceso que se encuentran definidos en la tabla de usuarios en el firewall de acceso de Fortinet para acceder las aplicaciones críticas en confidencialidad en Google Workspace.

El IT Specialist puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los colaboradores de la organización, con el fin de reducir el riesgo de acceso a sitios web con contenido malicioso o ilegal, o que puedan ser utilizados para la fuga de datos. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita IT Specialist solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción. Actualmente, se usa la tecnología del antivirus Fortinet para el control de tráfico y control del bloqueo de páginas.

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.

3.16. 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 Email. Así como teléfonos, el envío de mensajes de texto por teléfonos móviles, medios móviles y foros o redes sociales.

De acuerdo con lo estipulado en este documento y con la Política de transferencia de información, como también con la Política de clasificación de la información, el IT Specialist 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 o sospechoso de contenido malicioso, debe informar al IT Specialist.

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 la información.

El usuario debe guardar todos los mensajes que contienen datos importantes para los negocios de la organización utilizando el método especificado por el IT Specialist.

Cada correo electrónico debe incluir una exención de responsabilidad, salvo los mensajes enviados a través de los sistemas de comunicación determinados por el IT Specialist. 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.

3.17. Derechos de autor

Los usuarios no deben realizar copias no autorizadas del software que pertenece a la organización.

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.

3.18. Computación móvil

3.18.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos, sin importar dónde se utilice dicho equipo.

El equipo antes mencionado puede retirarse de las instalaciones solo después de obtener la autorización de acuerdo con la sección 3.6 - Uso de activos fuera de las instalaciones de esta Política.

3.18.2. Reglas básicas

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos (incluidos automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Las actualizaciones de parches y demás configuraciones del sistema se realizan de forma automática en todos los ordenadores de la organización mediante el uso de la herramienta Action1, pasando previamente por el filtro del Fortinet y la validación del

IT Specialist; estas se generan y despliegan de manera automatizada en el sistema operativo.

- La protección contra códigos maliciosos se instala y actualiza de forma automática a través del Fortinet.
- La persona que utiliza equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente copias de seguridad según la Política de copias de seguridad.
- La conexión a redes de comunicación se realiza mediante clave y contraseña de acceso según lo especifica la Política de control de acceso.
- La información que se encuentra en ordenadores portátiles debe estar encriptada, y aplica para toda la información que se almacene en el disco duro.
- La protección de datos sensibles debe ser implementada de acuerdo con la Política de clasificación de la información y la Política de privacidad y protección de datos personales.
- La persona que utilice equipos informáticos móviles fuera de las instalaciones debe observar las instrucciones del fabricante con respecto a la protección del equipo (por ejemplo, de las condiciones climáticas, exposición a interferencias electromagnéticas, vibraciones físicas, etc.)
- Cuando las personas usan sus propios dispositivos, las reglas adicionales que se deben aplicar se definen en la Política BYOD.

El Information Security Officer es el responsable de la formación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

3.19. Teletrabajo y trabajo desde casa

3.19.1. Introducción

Teletrabajo significa que los equipos de información y comunicación se utilizan para permitir que los colaboradores realicen su trabajo fuera de la organización, incluido el trabajo desde casa. El teletrabajo incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

El teletrabajo debe ser autorizado por el Head of HR. Al colaborador se indica y autoriza según el cronograma planificado trimestralmente por la organización e incluso en el transcurso del reclutamiento también se comenta que el teletrabajo es aceptado. Por tanto, consta en el contrato y el reglamento interno de Actuaría Consultores.

3.19.2. Normas adicionales para el teletrabajo

Todas las personas que realicen teletrabajo deben seguir las reglas de computación móvil definidas en la sección 3.17 de este documento, y las reglas definidas a continuación:

- El lugar físico donde se realiza el teletrabajo debe estar protegido de la siguiente forma:
 - **Buena iluminación:** la luz es clave para tener un buen espacio de trabajo
 - **Espacio adecuado:** buscar un rincón o espacio que no tenga distracciones y que no sea una zona de paso donde se interrumpa tu concentración.

- **Tener los mejores elementos:** una mesa y una silla ergonómica donde estés cómodo. Si trabajas con un computador, asegúrate de colocar un soporte para que esté a la altura adecuada y que tus cervicales no sufran.
- **Decoración:** todo lo que coloques en tu espacio de trabajo y que lo haga más ameno afecta directamente a tu actitud a la hora de trabajar. Manténlo siempre ordenado, busca elementos bonitos y funcionales para tener un rincón apetecible.
- **No tener alimentos cerca:** es importante no beber o consumir alimentos mientras se está trabajando de esta manera evitamos que algo se derramen encima del computador y este se dañe.
- **Lugares al aire libre:** si trabajas fuera de casa evita que sea en un lugar sin techo para que los rayos solares no den directo en el computador y este se pueda sobre calentar o se pueda mojar por causa de una lluvia.
- Como mínimo, las personas que realizan teletrabajo deben tener:
 - Contar con servicio de un buen proveedor de internet con partición máxima 8:1 y 50 Mbps de velocidad
 - Tener un regulador eléctrico para evitar averías tras apagones de luz
 - Micrófonos con calidad que permita a los demás entender lo que se habla y que no tenga ECO o interferencia.
- La prevención del acceso no autorizado por parte de personas que viven o trabajan en el lugar donde se realiza la actividad de teletrabajo debe implementarse de conformidad con la Política de control de acceso y la Política de escritorio y pantalla limpios.
- La protección de los derechos de propiedad intelectual de la organización ya sea para software u otros materiales que puedan estar protegidos por derechos de propiedad intelectual, debe implementarse de acuerdo con la Política de clasificación de la información.
- La devolución de datos y equipos en caso de terminación del empleo debe implementarse de acuerdo con la sección 3.7 de esta Política
- Las actividades prohibidas específicas para los colaboradores que realizan teletrabajo son:
 - NO indicar al Head of HR y Coordinador de área que saldrá del país sin previo aviso y aprobación.
 - Uso inadecuado de los bienes o equipos que provee la compañía al teletrabajador para realizar sus tareas.
 - Ausentarse durante la jornada laboral sin indicar al coordinador de área o a la Head of HR que tuvo una emergencia o algún tipo de situación especial.
 - Incumplimiento del acuerdo de confidencialidad por parte del teletrabajador.
 - No presentarse a las reuniones con clientes o internas sin notificación o justificación alguna.
 - No mantener prendida la cámara durante las reuniones internas y externas de la empresa.
- Las actividades específicas permitidas solo para los colaboradores cuando realizan teletrabajo están detalladas en la Política sobre dispositivos móviles tele trabajo y trabajo desde casa.

3.20. 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, etc., independientemente de si es personal o no, se considera propiedad de Actuaría Consultores

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.

3.21. Incidentes

Cada colaborador, proveedor o tercero que esté en contacto con datos o sistemas de Actuaría Consultores 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 / Código / Versión	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Ticket (Autorización de instalación de software)	Jira	IT Specialist	Solamente el IT Specialist tiene acceso	Los registros son almacenados por el plazo de 3 años.
Ticket (Autorizaciones para retirar activos fuera de las instalaciones)	Jira	IT Specialist	Solamente el IT Specialist tiene acceso	Los registros son almacenados por el plazo de 3 años.
Ticket (Autorización para acceder a determinadas páginas de Internet)	Jira	IT Specialist	Solamente el IT Specialist tiene acceso	Los registros son almacenados por el

				plazo de 3 años.
Cronograma de Teletrabajo	Google Drive	Head of HR	Solamente la Head of HR tiene acceso	Los registros son almacenados por el plazo de 3 años.
Registros de las actualizaciones de parches y otras configuraciones del sistema (Automático)	Fortinet	IT Specialist	Solamente el IT Specialist tiene acceso	Los registros son almacenados por el plazo de 3 años.
Lista de plataformas con credenciales compartidas	Google Drive	IT Specialist	Solamente el IT Specialist tiene acceso	Los registros son almacenados por el plazo de 3 años.
Control de personas con credenciales compartidas	Google Drive	IT Specialist	Solamente el IT Specialist tiene acceso	Los registros son almacenados por el plazo de 3 años.

Solamente el IT Specialist puede permitir a otros colaboradores el acceso a cualquiera de los documentos mencionados precedentemente.

5. Validez y gestión de documentos

Este documento es válido hasta el 15 de junio del 2027

El propietario de este documento es el IT Specialist 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 formación o de concienciación de empleados sobre el uso aceptable de los activos de información.