POLITICA DE CONTROL DE ACESO

TECHSYSTEM

Aníbal
Elisabeth
Jorge
Pablo
Verónica

Contenido

Política de Control de Accesos

1. Introducción

1.1. Objetivo

Establecer los controles de acceso a la red de comunicaciones y sistemas informáticos de TechSys Solutions S.L. para **proteger la información confidencial y garantizar la continuidad operativa**.

1.2. Alcance

Aplica a **toda la sede de Barcelona**, empleados **presenciales y teletrabajadores**, así como a cualquier **tercero con acceso a los sistemas**.

1.3. Normativas de referencia

- **ISO 27001/27002** (Gestión de Seguridad de la Información).
- **RGPD** (Protección de Datos Personales).

IRON HACK	Política de control de accesos

Código	Descripción del Control	Estado de Cumplimiento
A.5.1	Establecer y comunicar políticas de seguridad.	No cumple
A.5.2	Asignar claramente funciones de seguridad.	No cumple
A.5.3	Evitar conflictos de interés asignando tareas separadas.	No cumple
A.5.4	Alta dirección debe apoyar y liderar la seguridad.	No cumple
A.5.5	Definir cómo contactar autoridades en incidentes.	No cumple
A.5.6	Participar en grupos de seguridad externos.	No cumple
A.5.7	Usar inteligencia sobre amenazas para anticiparse.	No cumple
A.5.8	Incluir seguridad en la gestión de proyectos.	No cumple
A.5.9	Tener inventario actualizado de activos.	No cumple
A.5.10	Definir reglas de uso de activos.	No cumple
A.5.11	Asegurar devolución de activos al finalizar relaciones.	No cumple
A.5.12	Clasificar información según su sensibilidad.	No cumple
A.5.13	Etiquetar datos según clasificación.	No cumple
A.5.14	Proteger la información en tránsito.	No cumple
A.6.1	Verificar antecedentes del personal.	Cumplimiento parcial
A.6.2	Incluir cláusulas de seguridad en contratos.	Cumplimiento parcial
A.6.3	Sensibilizar al personal en temas de seguridad.	Cumplimiento parcial
A.6.4	Formar regularmente en buenas prácticas.	Cumplimiento parcial
A.6.5	Definir sanciones ante incumplimientos.	Cumplimiento parcial
A.7.1	Delimitar zonas físicas seguras.	Cumple
A.7.2	Controlar el acceso físico a instalaciones.	Cumple
A.7.3	Asegurar zonas sensibles.	Cumple
A.7.4	Proteger contra incendios, agua, etc.	Cumple
A.7.5	Establecer controles en áreas críticas.	Cumple
A.7.6	Evitar exposición visual de información.	Cumple
A.7.7	Colocar y proteger adecuadamente los equipos.	Cumple
A.7.8	Proteger activos fuera de las oficinas.	Cumple
A.7.9	Gestionar soportes físicos de información.	Cumple
A.7.10	Proteger electricidad, climatización, etc.	Cumple
A.7.11	Proteger cables de datos y energía.	Cumple
A.7.12	Mantener y revisar los equipos regularmente.	Cumple
A.7.13	Eliminar o reutilizar equipos de forma segura.	Cumple
A.8.1	Gestionar la seguridad de portátiles, móviles, etc.	Cumple
A.8.2	Controlar accesos con privilegios elevados.	Cumple
A.8.3	Restringir acceso a información según necesidad.	Cumple
A.8.4	Proteger el acceso al código fuente.	Cumple
A.8.5	Usar métodos de autenticación seguros.	Cumple
A.8.6	Asegurar capacidad suficiente de sistemas.	Cumple
A.8.7	Tener protección contra software malicioso.	Cumple
A.8.8	Gestionar vulnerabilidades conocidas.	Cumple
A.8.9	Controlar configuraciones del sistema.	Cumple
A.8.10	Eliminar información cuando no sea necesaria.	Cumple
A.8.11	Enmascarar datos sensibles.	Cumple
A.8.12	Evitar fugas de información.	Cumple
A.8.13	Realizar copias de seguridad.	Cumple
A.8.14	Registrar eventos importantes.	Cumple
A.8.15	Supervisar el uso del sistema.	Cumple
A.8.16	Sincronizar los relojes de sistemas.	Cumple
A.8.17	Controlar herramientas avanzadas.	Cumple
A.8.18	Seguridad en el ciclo de vida de software.	Cumple
A.8.19	Especificar requisitos de seguridad.	Cumple
A.8.20	Diseñar sistemas seguros.	Cumple
A.8.21	Aplicar prácticas seguras de programación.	Cumple
A.8.22	Probar la seguridad en el desarrollo.	Cumple
A.8.23	Gestionar la seguridad en desarrollos externos.	Cumple
A.8.24	Controlar los cambios en sistemas.	Cumple
A.8.25	Proteger los datos en entornos de prueba.	Cumple
A.8.26	Evitar exposición de datos reales en pruebas.	Cumple

Para la RGPD:

Artículo	Nombre del Precepto	Cumplimiento
Artículo 5	Principios relativos al tratamiento de datos	Cumple
Artículo 6	Licitud del tratamiento	Cumple
Artículo 7	Condiciones para el consentimiento	Parcial
Artículo 9	Tratamiento de categorías especiales de datos personales	Pendiente de evaluar
Artículo 12	Transparencia de la información	Pendiente de evaluar
Artículo 13	Información que debe facilitarse al interesado	Cumple
Artículo 15	Derecho de acceso del interesado	Pendiente de evaluar
Artículo 16	Derecho de rectificación	Pendiente de evaluar
Artículo 17	Derecho de supresión ('derecho al olvido')	Pendiente de evaluar
Artículo 18	Derecho a la limitación del tratamiento	Pendiente de evaluar
Artículo 20	Derecho a la portabilidad de los datos	Pendiente de evaluar
Artículo 25	Protección de datos desde el diseño y por defecto	Parcial
Artículo 30	Registro de actividades de tratamiento	No cumple
Artículo 32	Seguridad del tratamiento	Cumple
Artículo 33	Notificación de violaciones de seguridad de los datos personales	Parcial
Artículo 35	Evaluación de impacto relativa a la protección de datos	No cumple
Artículo 37	Delegado de Protección de Datos (DPO)	No cumple
Artículo 44	Transferencias internacionales de datos	Pendiente de evaluar

2. Principios del control de accesos

2.1. Principio de mínimos privilegios (least privilege)

Cada usuario tendrá acceso **únicamente** a los recursos necesarios para su función.

2.2. Control de Acceso Basado en Roles (RBAC)

Departamento	Rol	Accesos Permitidos
TI	Director	VPN administrativa, servidores físicos/virtuales, configuración de VLANs, gestión de usuarios AD, acceso completo a herramientas de monitoreo (SIEM), configuración de firewalls, gestión de copias de seguridad, Microsoft Dynamics 365, SAP ERP (módulos técnicos), todos los sistemas de productividad
TI	Supervisor	VPN administrativa, servidores de aplicaciones, gestión limitada de usuarios, herramientas de monitoreo, configuración básica de red, Microsoft Teams, Office 365,

		herramientas de desarrollo (Visual Studio Code, MySQL Workbench), sistemas antivirus corporativos
TI	Técnico	VPN estándar, acceso de lectura a logs de servidores, herramientas básicas de diagnóstico, soporte remoto, Office 365, herramientas de ticketing, acceso limitado a configuraciones de red, antivirus y actualizaciones
TI	Empleado	VPN estándar, aplicaciones de productividad (Office 365, Teams), herramientas básicas de soporte, acceso de solo lectura a documentación técnica, sistemas de comunicación interna
Consultora	Director	VPN empresarial, acceso completo a repositorios de proyectos, CRM (gestión de clientes), herramientas de gestión de proyectos (Jira, Trello), Office 365 completo, Power BI, documentación confidencial de clientes, sistemas de facturación
Consultora	Supervisor	VPN empresarial, repositorios de proyectos asignados, CRM (lectura/escritura limitada), herramientas de gestión de proyectos, Office 365, acceso a informes de clientes, herramientas de colaboración (Teams, Slack)
Consultora	Técnico	VPN estándar, proyectos específicos asignados, herramientas de desarrollo (según especialización), Office 365, documentación técnica, herramientas de comunicación, acceso limitado a datos de clientes
Consultora	Empleado	VPN estándar, proyectos asignados específicos, herramientas básicas de productividad, Office 365 básico, documentación general, sistemas de comunicación interna
Atención al Cliente	Supervisor	VPN estándar, CRM completo (gestión de incidencias), base de datos de clientes, herramientas de ticketing, Office 365, sistemas de comunicación (centralita Avaya), acceso a informes de satisfacción

Atención al Cliente	Técnico	VPN estándar, CRM (módulo de soporte), base de datos limitada de clientes, sistema de tickets asignados, Office 365 básico, centralita telefónica, herramientas de diagnóstico remoto
Atención al Cliente	Empleado	VPN básica, CRM (solo consulta), sistema de tickets básico, Office 365 limitado, centralita telefónica básica, acceso a FAQ y documentación de productos
Marketing	Director	VPN empresarial, herramientas de marketing digital (todas las plataformas), CRM (módulo de marketing), Google Workspace, Adobe Creative Suite, herramientas de analítica (Google Analytics, Power BI), redes sociales corporativas
Marketing	Supervisor	VPN estándar, herramientas de marketing asignadas, CRM (lectura de leads), Google Workspace, herramientas de diseño (Canva, básico de Adobe), analítica limitada, gestión de contenidos

2.3. Verificación Continua (Zero Trust)

- No confiar en ningún dispositivo o usuario por defecto.
- Monitoreo activo de accesos y autenticación constante.

La infraestructura actual de la sede de Barcelona no permite implementar Zero Trust de forma inmediata, pero cuenta con bases sólidas para una transición poco a poco.

---

3. Políticas de acceso a la red y sistemas

3.1. Acceso a la red interna (sedes físicas)

- Uso de **VLANs segmentadas** para separar tráfico entre departamentos.
- **Autenticación 802.1X** para acceso WiFi.
- Acceso solo a través de dispositivos **corporativos o verificados**.

Categoría	Ítem	Verificación (Si/No)	Comentarios
Firewalls	NGFW activo en sede central con inspección DPI	no	N/A
	Reglas de acceso personalizadas por rol/departamento	si	A través de un AD en servidor dedicado
	Listas blancas implementadas correctamente	si	Administradas en PfSense
	Firewalls locales operativos en Barcelona y Sevilla	si	N/A
	Registro y monitoreo de tráfico en firewalls	si	N/A
VLANs Segmentadas	VLANs definidas por departamento (TI, Dev, Marketing…)	si	Implantación de redes segmentadas en el Firewall central de cada sede
	Reglas de acceso entre VLANs estrictas	si	Separando red de VLAN para invitados
	Uso de IEEE 802.1Q (tagging VLAN)	no	N/A
	Logs de tráfico entre VLANs revisados	si	Centralizados con el SIEM

Autenticación WiFi 802.1X	Uso de 802.1X en WiFi corporativo	si	Usando seguridad WPA2/WPA3-Enterprise
	Protocolo seguro: PEAP / EAP-TLS	no	N/A
	Servidor RADIUS configurado y activo	si	Implantado en MADRID en servidor dedicado Windows Server
	Integración con Active Directory o LDAP	si	AD en cada sede en servidor dedicado / acceso desatendido remotamente
	Intentos fallidos de autenticación registrados	si	Bloqueo por intento de fallos máximos
Dispositivos Autorizados	Solo dispositivos corporativos o BYOD verificados acceden	si	Filtrado de dispositivos corporativos
	Cumplimiento con requisitos BYOD: AV, disco cifrado, MFA	si	MFA a través de herramientas TOPT (implantado en CRM, Google authenticator, Microsoft 365)
	Uso de MDM para control de dispositivos	no	N/A
	Registro de dispositivos conectados a la red	si	N/A
	Revocación inmediata de dispositivos no conformes	si	N/A

3.2. Acceso Remoto y Teletrabajo

- **VPN obligatoria** con autenticación multifactor (MFA).
- **Requisitos de seguridad para BYOD** (cifrado de disco, antivirus actualizado).
- Restricción de acceso según ubicación geográfica.

Categoría	Ítem	Verificación (Si/No)	Comentario
Acceso Remoto y Teletrabajo	VPN obligatoria implementada para acceso remoto	si	
	Autenticación multifactor (MFA) activa para VPN	si	
	Verificación de cifrado de disco en dispositivos BYOD	no	
	Antivirus actualizado en dispositivos BYOD	si	A través de BitDefender descentralizado y acceso desatendido
	Restricción de acceso según ubicación geográfica	no	
	Evaluación de capacidad de la VPN para todos los usuarios	no	
	Procedimientos documentados para conexión remota segura	si	
	Supervisión y monitoreo del tráfico VPN	n/a	A confirmar con Madrid
	Registro de dispositivos autorizados para acceso remoto	n/a	A confirmar con Madrid
	Revisión periódica de cumplimiento de requisitos BYOD	n/a	A confirmar con Madrid

3.3. Control de Acceso a Sistemas y Aplicaciones

- Aplicación del modelo **RBAC** en sistemas internos.
- Implementación de **autenticación multifactor (MFA)** en aplicaciones críticas.
- Registro y auditoría de **todos los accesos**.

Sistema / Aplicación	Funcionalidad de Seguridad	Soporte Confirmado
VPN (Cisco AnyConnect / NordVPN Teams)	Soporta MFA	Sí
Correo corporativo (Outlook / Office 365)	Soporta MFA	Sí
OneDrive / Google Drive	Soporta MFA	Sí
Teams, Zoom, Asana, Slack	Soporta MFA	Sí
Sistemas contables y financieros	Soporta MFA	Sí (según BIA)
Repositorios de código (GitHub / GitLab)	Soporta RBAC	Sí
Sistemas contables y de nóminas	Soporta RBAC	Sí
Infraestructura de red (firewalls, VLANs)	Soporta RBAC	Sí
Aplicaciones internas desarrolladas	Soporta RBAC	Sí (según desarrollo y TI)
SIEM / sistemas críticos	Registro y auditoría de accesos	Sí

4. Métodos de autenticación y seguridad

4.1. Autenticación de Usuarios

- Uso de **contraseñas seguras** y cambio periódico obligatorio.
- Autenticación biométrica opcional en dispositivos móviles.
- Implementación de **SSO (Single Sign-On)** si es viable.

Se exige el uso de contraseñas seguras y su cambio obligatorio cada 90 días. Se aplicará autenticación multifactor (MFA) en servicios críticos. En dispositivos móviles, se permite el uso de biometría (huella o rostro) como segundo factor. Se implementa SSO para simplificar el acceso a múltiples sistemas.

Implementación de SSO y Autenticación Biométrica

Objetivo: Centralizar el acceso a múltiples sistemas mediante una sola cuenta corporativa.

Pasos:

1. Seleccionar un proveedor de identidad (IdP):
    - Ejemplos: Azure Active Directory, Google Workspace, Okta, Auth0.
2. Integrar los sistemas compatibles:
    - Conectar ERP, correo, CRM y otras apps que soporten SAML, OAuth o OpenID.
    - Verificar que cada sistema permite el uso de SSO desde el IdP elegido.
3. Configurar políticas de seguridad:
    - Activar MFA como requisito para el inicio de sesión único.
    - Registrar intentos fallidos y accesos sospechosos.
4. Pruebas y despliegue:
    - Hacer pruebas piloto con un grupo reducido de usuarios.
    - Desplegar por fases para minimizar riesgos.

5. Capacitación al personal:
    - Informar al usuario que solo necesitará una cuenta para todos los accesos.
      Brindar soporte ante problemas de acceso o recuperación de cuenta.

4.2. Seguridad en Dispositivos

- Uso obligatorio de **antivirus y cifrado de disco**.
- Bloqueo de dispositivos tras **tiempo de inactividad**.
- Registro de dispositivos autorizados.

Todos los dispositivos corporativos deben cumplir con las medidas mínimas de seguridad: uso de antivirus actualizado, cifrado de disco y bloqueo automático por inactividad.

Se establece la implementación de una solución de MDM (Mobile Device Management) para mejorar el control y la protección de dispositivos móviles y portátiles.

Objetivos del MDM:

- Gestionar remotamente configuraciones de seguridad.
- Aplicar políticas de uso (cifrado, bloqueo, apps autorizadas).
- Permitir el borrado remoto en caso de pérdida o robo.
- Registrar e inventariar los dispositivos autorizados.

Alcance: Aplicable a todos los smartphones, tablets y portátiles que acceden a recursos de la empresa (correo, VPN, aplicaciones internas), tanto en modalidad presencial como de teletrabajo.

5. Monitoreo y Auditoría

En la sede regional de Barcelona, donde operan los departamentos de **Consultoría** y **Atención al Cliente**, se implementan medidas de control de accesos enfocadas en garantizar la confidencialidad de la información sensible y confidencial que se maneja (informes, documentación técnica, datos personales de clientes, etc.).

5.1. Registro de Accesos

- Todos los accesos deben quedar **registrados y auditados**.
- Uso de **SIEM (Security Information and Event Management)** para análisis de logs.

Todos los accesos a los sistemas corporativos desde esta sede deben quedar **registrados y auditados**, tanto si son locales como si se realizan mediante conexión VPN a los servidores de la sede central (Madrid).

Los dispositivos utilizados por los usuarios (portátiles, tablets, estaciones de trabajo) deberán tener habilitado el registro de actividad: inicio/cierre de sesión, acceso a archivos compartidos, intentos de acceso no autorizados, etc.

Dado que la sede de Barcelona no dispone de servidores propios avanzados ni SIEM local, los registros deben enviarse de forma **centralizada** al sistema de monitoreo ubicado en Madrid.

Se utilizará un sistema **SIEM centralizado** (ya existente o por adquirir) que permita la **correlación de eventos** desde distintas sedes, incluyendo Barcelona.

Es obligatorio que los sistemas de registro cumplan con:

- Identificación de usuario.
- Fecha y hora.
- Dispositivo y ubicación.
- Recursos accedidos y acciones realizadas.

Los registros deben conservarse durante **12 meses como mínimo**, en servidores seguros de la sede central.

5.2. Respuesta ante accesos sospechosos

- Detección de **intentos fallidos** y **accesos fuera de horario habitual**.
- Implementación de alertas de seguridad en caso de actividad sospechosa.

El sistema debe permitir la **detección automatizada de accesos sospechosos** desde la sede de Barcelona, como:

- Accesos repetidos fallidos por parte de consultores o personal de soporte.
- Inicios de sesión fuera del horario laboral habitual (por ejemplo, por la noche o en fines de semana sin justificación).
- Accesos a información de clientes desde ubicaciones inusuales o desde dispositivos no autorizados.

Cualquier actividad que se considere anómala generará **alertas automáticas**, que serán enviadas al equipo de TI en la sede central para su análisis.

En caso de detección, se seguirán los siguientes pasos:

- **Notificación inmediata** al responsable del área y a los administradores del sistema.
- **Suspensión preventiva del acceso** del usuario implicado si se considera necesario.
- **Análisis de logs** para determinar si se ha producido una brecha de seguridad.
- **Documentación del incidente** y, si corresponde, notificación al Delegado de Protección de Datos (DPD).

Todo el personal deberá colaborar en la **investigación de incidentes**, cumpliendo con los protocolos de seguridad definidos por TechSys Solutions.

Actualmente, *TechSys Solutions S.L.* **no dispone de un sistema SIEM plenamente implementado**. El monitoreo de logs y eventos se realiza de forma **descentralizada**, con cada sede gestionando registros localmente mediante herramientas básicas del sistema operativo (por ejemplo, Visor de Eventos en Windows o syslog en Linux), sin correlación ni análisis centralizados.

La empresa aún no cuenta con una solución SIEM capaz de recopilar y analizar de forma remota los logs provenientes de la sede regional de Barcelona, lo cual representa una limitación en su capacidad de detección temprana de incidentes y cumplimiento normativo.

Se recomienda que TechSys Solutions valore la **adquisición de una solución SIEM ligera, escalable y centralizada**, que permita:

- **Recoger logs de todas las sedes y de los teletrabajadores.**
- **Instalar agentes locales en los dispositivos de Barcelona** (por ejemplo, agentes de Wazuh, Graylog o Elastic SIEM).
- Establecer una **plataforma SIEM en la sede central (Madrid)** para análisis, alertas y auditorías, sin necesidad de replicar infraestructuras costosas en sedes regionales.

Este enfoque permite un **control eficaz con bajo coste** y se adapta bien a una empresa mediana con varios centros y teletrabajo.

6. Gestión de Incidentes de Seguridad

6.1. Procedimiento ante accesos no autorizados

1. **Detección y notificación** del incidente.
2. **Bloqueo inmediato** de la cuenta o acceso comprometido.
3. **Análisis forense** del incidente.
4. **Acciones correctivas** y reporte a la dirección.

Ante un intento de acceso no autorizado, se aplicará el procedimiento definido en el protocolo interno de gestión de incidentes de seguridad:

- Detección y notificación inmediata al área de Seguridad de la Información.
- Bloqueo preventivo de la cuenta o dispositivo comprometido.
- Análisis forense básico para determinar el origen, método y alcance del acceso.
- Aplicación de medidas correctivas y comunicación formal del incidente a la Dirección.

Este procedimiento se encuentra documentado y forma parte del plan general de respuesta a incidentes de TechSys Solutions S.L.

6.2. Simulacros y pruebas periódicas

- **Pruebas de penetración** para evaluar la seguridad de accesos.
- **Simulaciones de ataques de phishing** para concienciación.

Para validar la eficacia de las medidas de seguridad definidas y mejorar la capacidad de respuesta del personal, se realizarán pruebas periódicas en el marco del protocolo de gestión de incidentes:

- Simulacros de phishing dirigidos a concienciar sobre técnicas de ingeniería social y reforzar la seguridad del factor humano.
- Pruebas de penetración internas o mediante terceros, centradas en accesos privilegiados y servicios críticos.

Estas actividades están contempladas dentro del protocolo de incidentes y se planifican anualmente como parte del Plan de Seguridad de la Información de TechSys Solutions S.L.

7. Sanciones y Cumplimiento

La política de control de acceso en la sede de Barcelona no sólo implica aspectos técnicos, sino también el cumplimiento por parte de los empleados de las normas establecidas. Este cumplimiento es esencial para proteger la información confidencial de clientes y proyectos de consultoría.

7.1. Consecuencias del incumplimiento

- Advertencias y sanciones disciplinarias según la gravedad del incumplimiento.
- Denegación de acceso a sistemas en caso de **reiteración de malas prácticas**.

Cualquier incumplimiento de la política de acceso será considerado una falta y se actuará en función de su gravedad.

Las medidas disciplinarias incluyen, de forma progresiva:

  - **Advertencia verbal o por escrito**.

- **Suspensión temporal del acceso a sistemas o recursos**.
- **Sanciones internas conforme al reglamento de régimen disciplinario de la empresa.**
- **En los casos más graves, despido procedente** (por ejemplo, robo de datos, uso indebido intencionado, acceso no autorizado reiterado).

En caso de **reiteración de malas prácticas**, como compartir contraseñas, ignorar alertas de seguridad o no respetar las normas de uso de dispositivos, se procederá a la **revocación temporal o definitiva del acceso** a los sistemas informáticos.

IMPORTANTE: Todas las incidencias deben quedar **documentadas** por el equipo de TI y notificadas a la dirección de Barcelona y al equipo de cumplimiento legal de la sede central.

7.2. Responsabilidades de los usuarios

- **Firmar un acuerdo de seguridad** donde aceptan cumplir la política.
- Uso exclusivo de credenciales propias (prohibido compartir accesos).

Todo el personal de la sede de Barcelona deberá **firmar un Acuerdo de Seguridad de la Información** en el que se compromete explícitamente a:

- Cumplir con las políticas de control de acceso.
- No compartir contraseñas ni dejar sesiones abiertas.
- Reportar cualquier uso indebido, sospechoso o pérdida de dispositivo.

El uso de credenciales es **personal e intransferible**. El acceso compartido está estrictamente **prohibido**, incluso entre miembros del mismo equipo.

El acceso a información y sistemas está condicionado al **respeto de las buenas prácticas de seguridad**, como el uso de VPN, la autenticación multifactor (cuando aplique), y el mantenimiento del dispositivo actualizado.

Actualmente, *TechSys Solutions* no cuenta con formación obligatoria en seguridad para todos los empleados. Sin embargo, dado que en Barcelona se manejan datos confidenciales de clientes y documentación técnica, se recomienda establecer una formación básica obligatoria en ciberseguridad, al menos anual.

Este curso debe incluir temas como:

- Uso seguro de dispositivos.
- Prevención del phishing.
- Gestión de contraseñas.
- Identificación de accesos sospechosos.

La formación puede realizarse online y ser gestionada desde la sede central con el apoyo del departamento de TI.

8. Revisión y Actualización de la Política

- **Periodicidad:** La política será revisada **anualmente** o ante cambios en la infraestructura, regulación, cuando haya un incidente de seguridad relacionado con el acceso, cuando hay auditoría y se requieren cambios.
- **Responsable:** El departamento de **TI y Seguridad**.

Rol	Responsabilidad
CISO / Responsable de SI	Liderar el proceso de actualización y validación final.
Responsable de Sistemas	Proveer información técnica y cambios en infraestructura.
DPO (si aplica)	Validar cumplimiento de la normativa de protección de datos.
Responsable de Recursos Humanos	Informar de altas, bajas y cambios de puesto.
Comité de Seguridad	Aprobar y validar la versión definitiva de la política.

- **Registro de versiones:** Se mantendrá un historial de cambios en la política. Se deben registrar los siguientes documentos:
    - Última versión de la Política de Control de Accesos
    - Actas del Comité de Seguridad

- Registro de cambios
- Informe de cumplimiento RGPD (DPO)
- Listado de accesos por rol y sistema

- Etapas:
  - Inicio
    - Se convoca una sesión del Comité de Seguridad de la Información (liderado por el CISO) durante el primer trimestre del año.
    - El CISO designa un equipo de trabajo para recopilar insumos técnicos y organizativos.
  - Revisión del entorno actual
    - El Responsable de Sistemas presenta:
      - Cambios en tecnologías de autenticación
      - Nuevos entornos (cloud, VPN, BYOD)
      - Cambios en roles o grupos de usuarios
  - Evaluación de cumplimiento
    - El DPO valida que los principios de minimización y necesidad del acceso se respetan.
    - Se revisa si se cumplen los requisitos de:
      - RGPD
      - ISO/IEC 27001
      - Políticas internas
  - Redacción de la actualización
    - Se modifican secciones relevantes:
      - Asignación de privilegios
      - Control de accesos remotos
      - Desactivación de usuarios inactivos

- Revisión de logs y auditoría

- Aprobación
  - El Comité de Seguridad revisa el borrador.
  - Se aprueba por mayoría simple
  - Se registra la fecha de aprobación y versión.
- Difusión y publicación
  - Se publica en la intranet corporativa.
  - RRHH envía notificación a todo el personal.
  - Se actualiza en el SGSI y en la documentación de calida

9. Anexos y Referencias

Glosario de términos.

- BYOD (Bring Your Own Device): Política que permite a los empleados usar sus dispositivos personales para acceder a recursos corporativos.
- CISO (Chief Information Security Officer): Director o responsable principal de seguridad de la información en una organización.
- DPO (Data Protection Officer): Delegado de Protección de Datos, figura obligatoria según el RGPD para supervisar el cumplimiento de normativas de privacidad.
- GDPR/RGPD (General Data Protection Regulation): Reglamento General de Protección de Datos, normativa europea que regula el tratamiento de datos personales.
- IdP (Identity Provider): Proveedor de identidad que gestiona las credenciales de usuario y auténtica el acceso a múltiples sistemas.
- ISO 27001/27002: Normas internacionales para la gestión de seguridad de la información que establecen requisitos y controles de seguridad.
- MDM (Mobile Device Management): Sistema de gestión que permite controlar remotamente dispositivos móviles corporativos.
- MFA (Multi-Factor Authentication): Autenticación multifactor que requiere dos o más métodos de verificación para acceder a un sistema.
- NGFW (Next-Generation Firewall): Es una evolución de los firewalls tradicionales con capacidades avanzadas de seguridad.
- NIST 800-53: Marco de controles de seguridad para sistemas de información desarrollado por el Instituto Nacional de Estándares y Tecnología de EE.UU.
- OAuth: Protocolo de autorización que permite a aplicaciones acceder a recursos de usuario sin exponer credenciales.
- OpenID: Estándar de autenticación que permite verificar la identidad de usuarios.
- RBAC (Role-Based Access Control): Control de acceso basado en roles que asigna permisos según la función del usuario en la organización.
- RGPD: Ver GDPR.
- SAML (Security Assertion Markup Language): Estándar para intercambiar datos de autenticación y autorización entre sistemas.

- SGSI (Sistema de Gestión de Seguridad de la Información): Marco organizacional para gestionar y proteger la información empresarial.
- SIEM (Security Information and Event Management): Sistema que recopila, analiza y correlaciona eventos de seguridad de múltiples fuentes.
- SSO (Single Sign-On): Sistema de autenticación única que permite acceder a múltiples aplicaciones con una sola cuenta.
- VLANs (Virtual Local Area Networks): Redes virtuales que segmentan el tráfico de red para mejorar la seguridad y organización.
- VPN (Virtual Private Network): Red privada virtual que crea conexiones seguras y cifradas a través de internet.

Términos Técnicos

- Antivirus: Software que detecta, previene y elimina software malicioso (virus, malware).
- Autenticación biométrica: Verificación de identidad mediante características físicas únicas como huellas dactilares o reconocimiento facial.
- Azure Active Directory: Servicio de identidad y gestión de acceso en la nube de Microsoft.
- Cifrado de disco: Tecnología que protege datos almacenados convirtiendo la información en código ilegible sin la clave correcta.
- Cloud: Servicios de computación en la nube que proporcionan recursos informáticos a través de internet.
- Firewall: Sistema de seguridad que controla el tráfico de red entrante y saliente según reglas predefinidas.
- Ingeniería social: Técnicas de manipulación psicológica para obtener información confidencial o acceso no autorizado.
- Intranet: Red privada interna de una organización accesible solo para empleados autorizados.
- Logs: Registros detallados de eventos y actividades del sistema que permiten auditoría y monitoreo.
- Phishing: Técnica de ciberataque que simula comunicaciones legítimas para robar credenciales o información sensible.
- Pruebas de penetración: Evaluaciones de seguridad que simulan ataques reales para identificar vulnerabilidades.
- Syslog: Sistema estándar para el envío de mensajes de registro en redes de computadoras.

- Zero Trust: Modelo de seguridad que no confía en ningún dispositivo o usuario por defecto y verifica constantemente todos los accesos.

Herramientas y Plataformas Mencionadas

- Auth0: Plataforma de identidad y autenticación como servicio.
- Elastic SIEM: Solución de monitoreo de seguridad basada en Elasticsearch.
- Google Workspace: Suite de productividad y colaboración empresarial de Google.
- Graylog: Plataforma de gestión centralizada de logs y análisis de seguridad.
- Okta: Proveedor de servicios de identidad y gestión de acceso empresarial
- Wazuh: Plataforma de seguridad de código abierto para detección de amenazas y monitoreo
- Procedimientos específicos de acceso a cada sistema.
- Normativas aplicables (ISO 27001, NIST, GDPR, etc.).

Pasos a Seguir para Completar el Documento:

✅ **Confirmar normativas aplicables** (ISO 27001, NIST, GDPR).
✅ **Definir roles y matriz de accesos** (RBAC).
✅ **Validar herramientas de autenticación (MFA, VPN, SSO, SIEM).**
✅ **Asegurar monitoreo de accesos y capacidad de respuesta a incidentes.**
✅ **Definir responsables de aplicación y revisión de la política.**