

# UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

## UNIDAD DE POSGRADO

Facultad de Ingeniería de Sistemas e Informática – FISI

Maestría en Ingeniería de Sistemas e Informática Mención en Ingeniería de Software



**CURSO: GESTIÓN DE LA CALIDAD DEL SOFTWARE**

**Docente: REMBRANDT UBALDE**

**GRUPO N.<sup>o</sup> 1:**

Heber Hualpa Canales.

Melissa Rodriguez Sandoval.

Ronald Ticona Humpiri.

Sihomara Ochoa Cisneros.

Jhonathan Pauca Joya.

Lima, Octubre de 2025

# PROYECTO BITWARDEN

---

Transformación Estratégica de la Gestión de Credenciales e Identidad

**Alcance:** Análisis de Riesgos (μPILAR) | Arquitectura Técnica | Plan de Implementación (Roadmap)

**Objetivo:** Elevación del Nivel de Madurez CMM de L2 a L4

Noviembre 2025 | Preparado para: Dirección de Tecnología y Seguridad de la Información

## Fase 1: Contexto & Diagnóstico (AS-IS)

- › **Análisis Situacional:** Evaluación de prácticas actuales descentralizadas y vulnerabilidades críticas detectadas.
- › **Justificación del Negocio:** Impacto financiero y operativo de la inacción.
- › **Análisis de Activos (μPILAR):** Inventario detallado de activos esenciales y de soporte.
- › **Identificación de Amenazas:** Mapa de vectores de ataque actuales (Phishing, Ingeniería Social).

## Fase 2: Solución Técnica (TO-BE)

- › **Arquitectura Bitwarden:** Diseño de despliegue Self-Hosted con Docker.
- › **Criptografía:** Análisis profundo del modelo Zero-Knowledge y derivación de claves.
- › **Integración Directory Connector:** Sincronización automatizada con Active Directory.
- › **Gestión de Secretos DevOps:** Eliminación de credenciales hardcodeadas.

## Fase 3: Gestión de Riesgos

- › **Evaluación de Madurez (CMM):** Comparativa visual de evolución de L2 a L4.
- › **Matriz de Riesgos:** Estrategias de mitigación, transferencia y aceptación.
- › **Planes de Contingencia:** Recuperación ante desastres y continuidad del negocio.

## Fase 4: Implementación & Futuro

- › **Roadmap Detallado:** Cronograma de 3 meses (Fases 1, 2 y 3).
- › **Monitorización Continua:** KPIs de seguridad y reportes de salud de bóveda.
- › **Conclusiones:** Resumen ejecutivo y solicitud de aprobación.

## ESTADO ACTUAL: DESCENTRALIZACIÓN INSEGURA

La organización opera bajo un modelo de "confianza implícita" sin controles técnicos que garanticen la seguridad de las credenciales.

### Hallazgos Críticos

- ☒ **Almacenamiento:** Archivos Excel ("claves.xlsx") en servidores de archivos compartidos y equipos locales sin cifrado.
- ☒ **Transmisión:** Envío recurrente de contraseñas en texto plano por Teams/Email, quedando en historiales perpetuos.
- ☒ **Ciclo de Vida:** Nula rotación de credenciales de servicio. Cuentas de ex-empleados activas semanas post-salida.
- ☒ **Shadow IT:** Uso de cuentas personales (Gmail) para registrar servicios SaaS corporativos.

## MATRIZ DE IMPACTO EN EL NEGOCIO

Evaluación cualitativa del riesgo basada en la probabilidad de ocurrencia y la severidad del impacto operativo/legal.

Dimensión	Detalle del Impacto	Nivel Riesgo
<b>Confidencialidad</b>	Exposición de secretos industriales y datos de clientes. Acceso no autorizado por parte de atacantes internos o externos.	CRÍTICO
<b>Integridad</b>	Modificación no autorizada de contraseñas, causando denegación de servicio a usuarios legítimos. Falta de control de versiones.	ALTO
<b>Disponibilidad</b>	Dependencia de archivos locales. Si el PC de un administrador falla, se pierde el acceso a sistemas críticos (Single Point of Failure).	MEDIO
<b>Trazabilidad</b>	Inexistente. Imposible determinar quién usó una cuenta genérica ("admin") para realizar cambios en producción. Incumplimiento normativo.	CRÍTICO
<b>Legal / Cumplimiento</b>	Violación potencial de GDPR/ISO 27001 por falta de controles de acceso adecuados a datos sensibles.	ALTO

Transición hacia una plataforma unificada de gestión de secretos que garantiza la confidencialidad, integridad y disponibilidad mediante criptografía avanzada y gobernanza centralizada.



## Centralización Segura

Consolidación de todos los secretos en una bóveda cifrada accesible vía Web, Móvil, Desktop y CLI.

- › Eliminación de archivos planos.
- › Acceso federado (SSO).
- › **MFA Forzado:** Requisito obligatorio de 2FA (TOTP/Yubikey).



## Gobernanza & RBAC

Estructura jerárquica de permisos basada en el principio de "Need-to-Know" (Necesidad de Saber).

- › **Organizaciones:** Segregación lógica.
- › **Colecciones:** Agrupación por departamento/proyecto.
- › **Roles:** Owner, Admin, User, Custom.



## Auditoría Total

Capacidad forense y de cumplimiento normativo mediante registros inmutables.

- › Logs de acceso detallados (Quién, Cuándo, Qué, Desde dónde).
- › Reportes de higiene de contraseñas.
- › Integración con sistemas SIEM.

### Beneficio Estratégico Cuantificable:

Reducción del 90% en la superficie de ataque relacionada con credenciales, optimización del tiempo de onboarding en un 60%, y cumplimiento del 100% de los requisitos de auditoría de acceso a sistemas críticos.

## ACTIVOS ESENCIALES [ESSENTIAL]

El valor intrínseco del negocio que requiere protección. El daño a estos activos impacta directamente en la misión de la organización.

- **[INFO] Credenciales Corporativas:** Accesos privilegiados a ERP (SAP), CRM (Salesforce), Banca Online, y Redes Sociales Corporativas. Valoración: Crítico.
- **[SRV] Continuidad Operativa:** La capacidad de los empleados para acceder a sus herramientas de trabajo diarias sin interrupciones. Valoración: Alto.
- **[INT] Propiedad Intelectual:** Secretos industriales, patentes y bases de datos de clientes protegidas por claves de cifrado. Valoración: Crítico.
- **[REP] Reputación:** Confianza del mercado y clientes, dependiente de evitar brechas de seguridad públicas. Valoración: Muy Alto.

## ACTIVOS DE SOPORTE [SUPPORT]

La infraestructura técnica y lógica donde residen y se gestionan los activos esenciales.

- **[keys] Claves Criptográficas:** Master Passwords, Claves Privadas SSH, Certificados SSL, Tokens API. Punto crítico de falla.
- **[falta] Datos de Validación:** Directorio Activo (AD), Base de datos SQL de Bitwarden (MFA seeds, hashes).
- **[com] Canales de Comunicación:** Vías de transmisión de secretos (Bitwarden Send vs Email/Chat).
- **[sw] Software Cliente:** Extensiones de navegador, Aplicaciones de Escritorio, Apps Móviles.
- **[hw] Infraestructura Física/Virtual:** Servidores Docker, Balanceadores de Carga, Firewalls.

**Análisis de Dependencia Crítica:** Los activos de soporte [keys] representan el "Reino de las Llaves". Su compromiso implica la caída total en cascada de todos los activos esenciales [INFO] e [INT].

Análisis de los escenarios de amenaza más probables y dañinos en el contexto actual (AS-IS), justificando la necesidad de controles.

Cód.	Amenaza	Descripción del Escenario	Probabilidad (AS-IS)
A.5	Suplantación de Identidad	Compromiso de credenciales mediante campañas de Phishing dirigidas. Sin 2FA, el atacante obtiene acceso inmediato a sistemas críticos.	MUY ALTA
A.19	Fuga de Información	Ex-empleados conservan acceso a sistemas o copias locales de archivos de contraseñas (Excel) tras su desvinculación.	ALTA
A.15	Ingeniería Social	Solicitud de claves por canales no verificados (WhatsApp/Teams) simulando ser personal de soporte TI o directivos (CEO Fraud).	ALTA
E.1	Intercepción (Sniffing)	Captura de tráfico de red interno. Credenciales enviadas en texto plano (HTTP/Email) son leídas por atacantes o malware en la red.	MEDIA
A.9	Error Operativo	Borrado accidental o corrupción de archivos de contraseñas locales sin copias de seguridad centralizadas o versionamiento.	MEDIA

## Conclusión del Análisis:

El perfil de riesgo actual es inaceptable. La combinación de alta probabilidad de Phishing y la falta de controles técnicos (2FA) expone a la organización a un riesgo inminente de compromiso.

Mapa de ruta para la evolución de los procesos de seguridad de la información, desde el caos actual hasta la optimización gestionada.

## Nivel Actual: L1/L2 (Reactivo)

**L1 - Inicial/Ad-hoc:** Procesos caóticos. La seguridad depende completamente de la competencia individual ("Héroes"). No hay estándares.

**E2 - Repetible pero Intuitivo:** Existen patrones de comportamiento (ej. "todos guardan claves en Excel"), pero no hay gestión formal, documentación ni auditoría. El éxito depende de la "buena voluntad".

- › Gestión manual de altas/bajas.
- › Sin métricas de seguridad.
- › Respuesta a incidentes improvisada.

## Nivel Objetivo: L4 (Gestionado)

**L3 - Proceso Definido:** Política de contraseñas documentada, herramienta estándar (Bitwarden) desplegada y procedimientos de uso establecidos.

**L4 - Gestionado y Medible:** Control cuantitativo. Métricas de fortaleza de contraseñas, logs de auditoría centralizados, automatización de revocación. La seguridad es predecible.

- › Sincronización automática de usuarios.
- › Auditoría proactiva de accesos.
- › Políticas técnicas forzadas (Enforced Policies).

## ESTRATEGIA DE CIERRE DE BRECHA

Para transitar de L2 a L4 se requiere una intervención tridimensional: **Tecnología** (Plataforma Bitwarden) + **Procesos** (Políticas de Seguridad) + **Personas** (Gestión del Cambio y Capacitación).

## COMPONENTES DEL DESPLIEGUE

Despliegue on-premise para garantizar la soberanía total de los datos, utilizando orquestación de contenedores.

- › **Proxy Inverso (Nginx):** Punto de entrada único. Maneja terminación SSL/TLS, cabeceras de seguridad y enrutamiento interno.
- › **Bitwarden Core (API):** El cerebro del sistema. Procesa lógica de negocio, sincronización de bóvedas y gestión de organizaciones.
- › **Bitwarden Identity:** Servidor de autenticación (IdentityServer4). Gestiona login, emisión de tokens JWT y federación SSO.
- › **Base de Datos (MSSQL):** Persistencia de datos. Almacena usuarios, grupos y los blobs cifrados de las bóvedas.
- › **Admin Console:** Interfaz web para gestión de servidor, visualización de logs de sistema y configuración global.

### Configuración: Docker Compose

```
version: '3' services: bitwarden: image: bitwarden/self-host:latest restart: always ports: - "80:8080" # HTTP redirect - "443:8443" # HTTPS traffic volumes: - ./bwdata:/etc/bitwarden environment: - BW_DOMAIN=vault.empresa.com - BW_DB_CONNECTION_STRING="Server=sql,1433;..." - BW_ENABLE_ADMIN=true - SMTP_HOST=smtp.empresa.com - SMTP_PORT=587 - SMTP_SSL=true
```

\*Configuración simplificada para ilustración. Requiere hardening de servidor host.

# Modelo de Seguridad: Zero-Knowledge

El principio fundamental es que Bitwarden (el servidor) NUNCA conoce la contraseña maestra ni las claves de descifrado. Solo almacena "blobs" de datos cifrados.

## 1. Derivación (Cliente)

Todo comienza en el dispositivo del usuario. Se utiliza **PBKDF2 SHA-256** (o Argon2id) con un alto número de iteraciones (>600k) y el email como

"salt".  
 $\text{Master Key} = \text{KDF}(\text{MasterPassword}, \text{Email})$

La **Master Key** resultante reside SOLO en la memoria volátil del cliente.

## 2. Autenticación (Tránsito)

Para loguearse, no se envía la Master Key. Se deriva un hash adicional:

$\text{Auth Hash} = \text{KDF}(\text{Master Key}, \text{PasswordHash})$

El servidor compara este **Auth Hash** con el almacenado en la BD. Si coinciden, entrega el token de sesión y los datos cifrados.

## 3. Descifrado (Cliente)

El cliente recibe el "Cipher Blob". Usa su Master Key local para descifrar la **Symmetric Key** de la cuenta, y con ella descifra los datos finales.

$\text{Data} = \text{AES-256}(\text{CipherBlob}, \text{SymmetricKey})$

Este proceso garantiza que ni un administrador de BD pueda leer los secretos.

## SINCRONIZACIÓN LDAP/AD

Bitwarden Directory Connector es la pieza clave para la escalabilidad y la seguridad operativa, eliminando la gestión manual de usuarios.

- › **Sincronización Unidireccional:** AD es la fuente de verdad. Los cambios en AD se reflejan en Bitwarden, no al revés.
- › **Mapeo de Grupos:** Los Grupos de Seguridad de AD (ej. "Finanzas", "DevOps") se mapean automáticamente a Grupos de Bitwarden, asignando permisos a Colecciones instantáneamente.
- › **Desaprovisionamiento Automático:** Crítico para la seguridad. Si un empleado es desvinculado en AD, el conector revoca su acceso a la organización en la siguiente sincronización.

### Flujo de Proceso de Sincronización

1. **Consulta:** El conector interroga al AD usando filtros LDAP configurados (ej. memberOf=CN=BitwardenUsers...).
2. **Comparación:** Compara el estado actual de AD con la base de usuarios de Bitwarden Organization.
3. **Ejecución:**
  - › *Nuevos:* Envía invitación por email.
  - › *Eliminados:* Revoca acceso a la organización (el usuario mantiene su cuenta personal, pero vacía de datos corporativos).
  - › *Modificados:* Actualiza pertenencia a grupos.
4. **Login Híbrido:** El usuario usa SSO para autenticarse, pero mantiene una Master Password para el descifrado local (Modelo Zero-Knowledge).

Solución al problema endémico de credenciales "hardcodeadas" en código fuente, scripts o archivos de configuración (.env), mitigando el riesgo de fugas en repositorios.

## Bitwarden Secrets Manager

Plataforma dedicada para gestionar secretos de infraestructura (API Keys, DB Strings, Certificados).

- › **Service Accounts:** Identidades no humanas para servidores, aplicaciones o pipelines CI/CD.
- › **Projects:** Agrupación lógica de secretos (ej. "Producción", "Staging").
- › **Access Tokens:** Autenticación granular. Tokens de larga duración con permisos específicos (Read-Only, Read-Write) limitados a proyectos concretos.
- › **SDKs y CLI:** Integración nativa en flujos de trabajo de desarrollo.

## Ejemplo de Implementación (CI/CD Pipeline)

```
# Pipeline de Despliegue (Jenkins / GitHub Actions) # OBJETIVO: Inyectar secretos en tiempo de ejecución sin guardarlos en disco. # 1. Autenticación con Token de Service Account (Variable de entorno del CI) export BWS_ACCESS_TOKEN="" # 2. Inyección Dinámica # El comando 'bws run' recupera los secretos y los pasa al proceso hijo # como variables de entorno. bws run -- npm start # 3. Recuperación Explicita (Scripting) # Obtener un secreto específico (ej. password de DB) DB_PASS=$(bws secret get "f8a2-uuid-secreto" | jq -r .value) echo "Conectando a DB con password recuperada dinámicamente..." ./db_migrate.sh --password "$DB_PASS"
```

# Planificación y Tratamiento de Riesgos

Estrategias  
Proactivas

Definición de respuestas formales ante los riesgos residuales y operacionales identificados durante el análisis.

Riesgo Identificado	Estrategia	Acción Concreta de Implementación
Olvido de Master Password	Mitigación	Configurar política de "Admin Password Reset" (requiere Enterprise Key Connector) o implementar protocolo de "Trusted Emergency Contacts" para recuperación entre pares autorizados.
Caída del Servidor Self-Hosted	Contingencia	Implementar backups automatizados diarios de la base de datos MSSQL y el directorio de adjuntos (bwdata). Configurar arquitectura de Alta Disponibilidad (HA) si es crítico.
Usuario Comprometido (Phishing)	Prevención	Forzar política global de <b>Two-Step Login (2FA)</b> . Exigir uso de aplicaciones TOTP (Authy, Google Auth) o llaves de hardware (YubiKey), prohibiendo SMS si es posible.
Ex-empleado con acceso residual	Eliminación	Automatización total mediante Directory Connector. El script de sincronización se ejecuta cada 15-30 minutos para garantizar revocación casi inmediata.
Uso de contraseñas débiles	Mitigación	Reportes de "Vault Health" obligatorios. Política de contraseñas forzada en el generador integrado (mínimo 14 caracteres, complejos).

Bitwarden permite forzar reglas de comportamiento para asegurar el cumplimiento de estándares de seguridad en toda la organización.

## Autenticación & Acceso

- › **Two-Step Login:** Obligatorio para todos los usuarios y administradores.
- › **Master Password Complexity:** Mínimo 14 caracteres, requiere números y símbolos.
- › **Vault Timeout:** Bloqueo automático de la bóveda tras 15 minutos de inactividad o al cerrar el navegador/app. Acción: Bloquear (requiere PIN/Biometría) o Cerrar Sesión.

## Uso de la Bóveda

- › **Remove Individual Vault:** (Opcional) Forzar que todos los ítems se guarden en la Organización, eliminando el almacenamiento personal no supervisado.
- › **Disable Vault Export:** Prevenir que los usuarios descarguen una copia no cifrada (CSV/JSON) de las credenciales corporativas.
- › **Generator Policy:** Configuración por defecto del generador de contraseñas segura.

## Bitwarden Send

- › **Send Options:** Restringir el uso de la herramienta Send.
- › **Text Only:** Permitir solo envío de texto (credenciales), prohibir archivos para evitar fuga de documentos (DLP).
- › **Force Password:** Obligar a proteger los enlaces externos con una contraseña separada.
- › **Force Deletion:** Máximo 24 horas de vida para cualquier enlace.

## HITOS CLAVE

- Aprovisionamiento de Infraestructura:** Despliegue de servidor virtual (Linux/Ubuntu) con Docker y Docker Compose. Configuración de Firewall y Networking.
- Configuración de Dominio y SSL:** Asignación de subdominio (vault.empresa.com) y gestión de certificados TLS (Let's Encrypt o Wildcard corporativo).
- Instalación Bitwarden:** Ejecución de scripts de instalación, configuración de variables de entorno (SMTP para correos transaccionales es crítico).
- Prueba de Concepto (PoC):** Configuración inicial de la Organización y onboarding del equipo de TI (5-10 usuarios) para validación técnica.

### Entregables de la Fase

- ✓ Instancia Bitwarden operativa y accesible vía HTTPS.
- ✓ Configuración de correo SMTP validada (invitaciones llegan correctamente).
- ✓ Documentación técnica de instalación.
- ✓ Plan de Recuperación ante Desastres (DRP) inicial probado (Backup/Restore).

## HITOS CLAVE

- Configuración Directory Connector:** Instalación del agente, configuración de conexión LDAP/AD, definición de filtros de usuarios y grupos. Test de sincronización (Dry Run).
- Estructura RBAC:** Definición final de la taxonomía de Colecciones y Grupos. Mapeo de grupos AD a roles en Bitwarden.
- Aplicación de Políticas:** Activación de las Enterprise Policies definidas (2FA, Timeout, Exportación).
- Migración de Datos:** Ejecución de scripts de limpieza sobre archivos Excel heredados e importación masiva a las colecciones correspondientes.

### Estrategia de Migración de Datos

Se realizará un inventario de todos los repositorios actuales de contraseñas (Excel, KeePass, navegadores). Se sanitizarán los datos (formato CSV compatible) y se importarán a una "Colección de Staging" para su clasificación y redistribución segura, asegurando que no se pierda acceso operativo durante la transición.

## HITOS CLAVE

- Despliegue Masivo de Cliente:** Instalación silenciosa de la extensión de navegador y app de escritorio mediante GPO/MDM en todos los endpoints corporativos.
- Onboarding General:** Invitación masiva a todos los empleados (sincronización AD completa).
- Programa de Capacitación:** Talleres obligatorios sobre higiene de contraseñas, uso de la bóveda, detección de phishing y uso de Bitwarden Send.
- Go-Live Oficial:** Apagado de métodos antiguos. Prohibición normativa del uso de Excel para claves.

### Gestión del Cambio (Change Management)

La resistencia al cambio es el riesgo principal en esta fase. La estrategia se centra en demostrar la **conveniencia** (Auto-fill, no tener que recordar claves) antes que la seguridad. Se establecerá un canal de soporte dedicado "Hypercare" durante las primeras 2 semanas.

La seguridad es un proceso, no un estado. Bitwarden proporciona herramientas para la vigilancia continua de la postura de seguridad.

## Informes de Salud (Vault Health)

Análisis proactivo de credenciales almacenadas:

- **Exposed Passwords:** Alerta si una clave aparece en brechas de datos públicas (Dark Web).
- **Reused Passwords:** Identifica reciclaje de claves (alto riesgo de credential stuffing).
- **Weak Passwords:** Detecta claves que no cumplen complejidad.
- **Inactive 2FA:** Identifica cuentas externas que soportan 2FA pero no lo tienen configurado.

## Logs de Eventos (Auditoría)

Registro forense para cumplimiento:

- **Eventos de Usuario:** Login (éxito/fallo), visualización de ítem, copia de contraseña.
- **Eventos de Organización:** Cambios en políticas, invitación de usuarios, cambios en grupos.
- **Exportación SIEM:** Envío de logs a Splunk/ELK para correlación de amenazas.

## Rutinas de Mantenimiento

- **Revisión Trimestral:** Auditoría de accesos privilegiados y cuentas de emergencia.
- **Limpieza:** Purga de cuentas inactivas y ítems obsoletos.
- **Simulacros:** Ejecución semestral del plan de recuperación ante desastres (restauración de backup).

## EL PROBLEMA

La necesidad de enviar credenciales (ej. acceso WiFi, FTP, CMS) a proveedores externos, auditores o clientes. Actualmente se hace por email o WhatsApp, dejando la credencial expuesta permanentemente.

## LA SOLUCIÓN: BITWARDEN SEND

Mecanismo para transmitir información sensible de forma efímera y cifrada.

- › **Cifrado E2E:** El contenido se cifra en el dispositivo del remitente. El servidor solo ve un blob cifrado.
- › **Enlace Seguro:** Se genera una URL única para compartir.
- › **Control Total:** El remitente define las reglas de acceso.

### Configuraciones de Seguridad Disponibles

Borrado Automático	El "Send" se autodestruye tras X horas (ej. 1 hora) o tras X días.
Límite de Accesos	El enlace expira automáticamente tras ser abierto 1 vez (evita reenvíos).
Protección con Contraseña	Requiere una clave (comunicada por otro canal) para abrir el enlace.
Visibilidad	El remitente puede ver si el enlace fue abierto, cuándo y desde qué IP.

## Estructura de Costos (TCO)

- **Licenciamiento:** Costo por usuario/año (Modelo Enterprise). Incluye SSO, Políticas, Self-host.
- **Infraestructura:** Recursos de cómputo (VM 2vCPU, 4GB RAM) y almacenamiento para backups. Mínimo impacto.
- **Operaciones:** Horas hombre de ingeniería para implementación inicial y mantenimiento mensual (actualizaciones Docker).

## Beneficios Tangibles e Intangibles

- **Eficiencia Operativa:** Reducción del 40% en tickets de Helpdesk por "reset de contraseñas" gracias al autoservicio y memoria centralizada.
- **Mitigación de Riesgos:** El costo promedio de una brecha de datos supera los cientos de miles de dólares. Bitwarden actúa como un seguro preventivo.
- **Continuidad:** Eliminación de la dependencia de empleados clave. Si un administrador se va, las claves quedan.
- **Cumplimiento:** Facilita auditorías ISO/SOC2 al proveer evidencia de control de accesos.

*"El costo de implementar Bitwarden es una fracción del costo de recuperación de un solo incidente de ransomware o fuga de datos."*

## RESUMEN EJECUTIVO

La implementación de Bitwarden Enterprise no es meramente una actualización tecnológica; constituye un **cambio cultural fundamental** hacia la madurez en ciberseguridad.

Estamos migrando de un modelo basado en la confianza ciega, la memoria humana y herramientas inseguras (L2), a un modelo basado en verificación estricta ("Zero Trust"), control centralizado y criptografía probada (L4).

## ACCIONES INMEDIATAS REQUERIDAS



### Aprobación Presupuestaria

Validación de costes de licencias e infraestructura.



### Provisión Recursos

Asignación de servidor y dominio para Fase 1.



### Kick-off Meeting

Inicio formal y comunicación al equipo de TI.

# DATOS DEL PROYECTO BITWARDEN

P Datos del proyecto

Editar

código	btw001
nombre	Implementación de Bitwarden
Organización	Backus
Descripción	Proyecto de Gestión de Calidad para la implementación de Bitwarden
Autor	Grupo 1
Versión	1
Fecha	21.11.2025
clase	0
informes - clasificación	DIFUSIÓN LIMITADA
descripción	Proyecto de Gestión de Calidad para la implementación de Bitwarden
Responsable del Sistema	Jhonathan Pauca
Responsable de la Seguridad de la Información	Heber Hualpa
RGPD	contexto

?

< >

# CONTEXTO - ROLES

P Datos del proyecto > RGPD

RGPD

- roles
- necesidad
- ciclo de vida
- necesidad y proporcionalidad

[btw001] Implementación de Bitwarden

**DPD (Delegado de Protección de Datos)**  
Interpretar y supervisar la aplicación del RGPD en la organización

**Responsable del tratamiento**  
Art. 4.7: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros

**Encargado del tratamiento**  
Art. 4.8: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento

◀ ▶

Este diagrama modela la arquitectura de actores en el sistema. Identificamos a los **Sujetos** (Usuarios, Administradores, Servicios) y su relación con los **Objetos** (Información). El objetivo aquí es mapear la superficie de interacción: ¿Quién toca qué dato? Esto es fundamental para definir los permisos en Bitwarden

# CONTEXTO - NECESIDAD

Datos del proyecto > RGPD

RGPD

- roles
- necesidad**
- ciclo de vida
- necesidad y proporcionalidad

[btw001] Implementación de Bitwarden

**Análisis de la necesidad de realizar una EIPD**

**1 Tipos de operaciones específicamente considerados por la Autoridad de control**

¿El tratamiento a analizar se encuentra dentro de la lista de tipos de tratamientos de datos publicados por la AEPD que requieren una EIPD?

[ ] 1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.

[ ] 2. Tratamientos que implican la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.

[ ] 3. Tratamientos que implican la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

[ ] 4. Tratamientos que implican el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

[ ] 5. Tratamientos que implican el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

[ ] 6. Tratamientos que implican el uso de datos genéticos para cualquier fin.

[ ] 7. Tratamientos que implican el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

[ ] 8. Tratamientos que implican la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.

[ ] 9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guarda y custodia.

10. Tratamientos que implican la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

[ ] 11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.

Gráfico que justifica el proyecto. Muestra la dependencia crítica que tiene el negocio sobre la disponibilidad y confidencialidad de las credenciales. Visualiza que, sin acceso seguro a las claves, los procesos operativos se detienen.

# CONTEXTO - NECESIDAD

Datos del proyecto > RGPD

RGPD

- roles
- necesidad**
- ciclo de vida
- necesidad y proporcionalidad

RGPD.

**Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.5**

1. Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.

2. Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD, siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.

3. Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se oblige a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.

4. Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.

5. Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

6. Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.

7. Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2(d) de dicho Reglamento.

**2 Sensibilidad de los datos**

¿Se van a tratar categorías especiales de datos?

No. El proyecto de implantación de Bitwarden no implica el tratamiento de categorías especiales de datos según el artículo 9 del RGPD. Únicamente se gestionan datos de identificación y credenciales técnicas necesarias para el acceso a sistemas corporativos.

¿Se van a tratar categorías especiales de datos a gran escala?

Para evaluar si un tratamiento se realiza a gran escala debe tenerse en cuenta:

- \* Número de afectados en términos absolutos o relativos de una determinada población
- \* Volumen y variedad de datos tratados
- \* Duración o permanencia del tratamiento
- \* Extensión geográfica del tratamiento Véase el documento wp243

Finalidades del tratamiento

Profundizamos en la necesidad operativa. Este gráfico ilustra los puntos de dolor actuales: tiempos perdidos por restablecimiento de contraseñas, riesgos por compartir claves en texto plano y la falta de auditoría. Es la justificación cualitativa del problema.

# CONTEXTO - NECESIDAD

Datos del proyecto > RGPD

Extension geográfica del tratamiento. Véase el documento Wp243

**3 Finalidades del tratamiento**

**El tratamiento involucra datos de menores de edad en materia de Protección de Datos (14 años según la LOPDGDD)?**

El artículo 7 de la Ley Orgánica 3/2018 determina que el tratamiento de datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

**La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad?**

Ejemplos de personas que pueden considerarse vulnerables: menores, personas mayores, discapacitados, refugiados y/o solicitantes de asilo, víctimas de violencia de género, personas en riesgo de exclusión social, pacientes o enfermos, etc.

**Con las operaciones de tratamiento, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?**

La utilización de datos personales puede dar lugar a analizar o predecir aspectos como situación económica, salud, hábitos de vida, preferencias personales, intereses, comportamiento, ubicación o movimientos del afectado, etc.

**Los tratamientos evaluados se amparan en la adhesión a un código de conducta dentro de los límites fijados por el RGPD?**

Para llevar a cabo el tratamiento el responsable y, en su caso, el encargado ¿se han adherido a un código de conducta?

**Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?**

El scoring consiste en una técnica de marketing a través de la cual se otorga una puntuación o calificación individual al interesado respecto a su nivel de afinidad a un producto o servicio de la empresa. A modo de ejemplo, una vez otorgadas las calificaciones de todos los interesados se les segmenta para decidir qué producto es más adecuado ofrecerles.

**A partir del tratamiento de los datos, ¿se toman decisiones que pueden afectar significativamente o perjudicar de alguna manera a las personas afectadas?**

Con el resultado del scoring o decisión automatizada es posible que el interesado se vea penalizado o perjudicado en alguna de sus acciones.

**Se tratan datos de clientes para realizar labores de gestión de morosidad o utilizando como referencia ficheros externos, tales como ASNEF o CIRBE?**

¿Se consultan los ficheros de solvencia económica con el propósito de obtener información complementaria a la aportada por el interesado?

**Se van a tratar datos relativos a la observación sistemática a gran escala de zonas de acceso público?**

¿Se pretende utilizar herramientas de monitorización, seguimiento o vigilancia, como por ejemplo: video vigilancia, monitorización del puesto de trabajo, seguimiento online, etc..?

**El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? Por ejemplo, un departamento que no participe en el tratamiento?**

"Aquí enfocamos la necesidad desde la perspectiva legal y normativa. Muestra cómo la falta de gestión de claves actual nos pone en incumplimiento de contratos con clientes o normativas de privacidad. Bitwarden viene a cerrar esta brecha de 'Compliance'

# CONTEXTO - NECESIDAD

Datos del proyecto > RGPD

RGPD

- roles
- necesidad
- ciclo de vida
- necesidad y proporcionalidad

¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? Por ejemplo, un departamento que no participe en el tratamiento?

A lo largo del proceso de tratamiento, se puede dar el hecho de que gran cantidad de personas puedan interactuar con los datos del interesado. Únicamente el personal autorizado debería tener acceso a los datos para el desempeño de sus funciones.

Para llevar a cabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado?

¿Se supera el alcance del tratamiento del que pudiese haber sido informado el interesado al inicio del mismo?

¿Se utilizan datos de carácter personal anonimizados de forma no irreversible?

¿Se tiene previsto anonimizar datos para con fines estadísticos, históricos o de investigación científica, etc. de manera que posteriormente puedan volver a utilizarse para identificar al interesado?

¿La base legal del tratamiento es el consentimiento?

Por ejemplo, en el caso de transferencias internacionales, comunicaciones comerciales, mercadotecnia directa, etc.,

**5 Tecnologías empleadas para el tratamiento**

¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado o con elevado riesgo para el acceso no autorizado?

Tecnologías innovadoras o experimentales que no ofrecen las garantías suficientes para los derechos y libertades de las personas.

**6 Encargados de tratamiento, cesiones de datos y transferencias internacionales de datos**

¿Se ha delegado alguna de las tareas que compone el tratamiento a un proveedor externo a la entidad? (en caso afirmativo detallar cuales)

A modo de ejemplo, proveedores que accedan a datos personales en el marco de la prestación de servicios.

¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuales)

¿Se comparte la información del interesado con terceros, ajenos o no, al tratamiento en aquellas actividades que requieran el consentimiento del interesado?

¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuales)

El siguiente listado contiene los países considerados seguros para las transferencias de datos:

- \* Paises de la Unión Europea
- \* Andorra
- \* Argentina
- \* Canadá (Sector privado)
- \* Suiza

Este gráfico vincula la necesidad de seguridad con la infraestructura tecnológica. Muestra que nuestros servidores y aplicaciones actuales requieren una capa de autenticación robusta que hoy no tienen.

# CONTEXTO - CICLO DE VIDA

Datos del proyecto > RGPD

RGPD

- roles
- necesidad
- ciclo de vida
- necesidad y proporcionalidad

[btw001] Implementación de Bitwarden

Ciclo de vida de los datos

1 Captura de datos

Actividades del proceso

Se deben detallar qué actividades, tareas o acciones se han llevado a cabo con la finalidad de recabar los datos necesarios para el tratamiento.

Datos tratados

Se debe listar las categorías de datos que se han recolectado para el tratamiento.

Intervinientes involucrados

Si los datos han sido proporcionados únicamente por el interesado, por la misma entidad o si hay terceros que hayan aportado información.

Tecnologías interviniéntes

Elaborar un listado completo de las tecnologías utilizadas para recabar los datos a tratar del interesado.

2 Clasificación / Almacenamiento

Actividades del proceso

Se debe enumerar las actividades que se pretenden llevar a cabo en el proceso de almacenaje de la información.

Datos tratados

Realizar un inventario de los tipos de datos del interesado que se van a almacenar

Intervinientes involucrados

Si en los procesos de clasificación, los datos del interesado son gestionados únicamente por el responsable del tratamiento o existen terceros involucrados en el proceso.

Tecnologías interviniéntes

Proporcionar el nombre de las tecnologías que hayan podido ser utilizadas en el proceso de clasificación o almacenaje de los datos del interesado.

3 Uso / Tratamiento

Actividades del proceso

Detallar qué acciones o labores se desempeñan en el momento de hacer uso de los datos del interesado.

Datos tratados

Listar qué categorías de datos se utilizan en el proceso del tratamiento

Intervinientes involucrados

El tratamiento lo realiza el encargado y/o se ven involucrados terceros adicionalmente en este proceso.

Tecnologías interviniéntes

Listar qué tecnologías son utilizadas para el proceso de tratamiento.

4 Cesión o transferencia de los datos a un tercero para su tratamiento

Actividades del proceso

Se debe enumerar las actividades que se pretenden llevar a cabo en el proceso de cesión o transferencia de la información.

Datos tratados

Realizar un listado de las categorías de datos que se van a ceder a los terceros.

Intervinientes involucrados

Enumerar los terceros a los que se van a realizar las cesiones de datos.

Analizamos la vida de una credencial: Creación, Uso, Almacenamiento, Transmisión y Destrucción. El gráfico resalta que actualmente fallamos en la **Transmisión** (envío inseguro) y **Destrucción** (archivos Excel eternos). Bitwarden asegura el ciclo completo.

# ANÁLISIS DE NECESIDAD Y PROPORCIONALIDAD

Este es un análisis de costo-beneficio. El gráfico demuestra que el valor de los activos (datos financieros, accesos ERP) es infinitamente superior al costo de implementar Bitwarden. Valida que la inversión es **proporcional** y necesaria; no estamos 'matando moscas a cañonazos'

P Datos del proyecto > RGPD

[btw001] Implementación de Bitwarden

Análisis de la necesidad y proporcionalidad del tratamiento

1 Legitimación

- Consentimiento
- Relación contractual
- Intereses vitales del interesado o de otras personas
- Obligación legal del responsable
- Interés público o ejercicio de poderes públicos
- Intereses legítimos prevalentes del responsable o de terceros

Legitimación

El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- \* el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos
- \* el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontratadas
- \* el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento
- \* el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física. El considerando 46 establece como ejemplos de intereses vitales y de interés público, aquellos relativos al tratamiento necesario para fines humanitarios (incluido el control de epidemias y su propagación) y situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.
- \* el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento
- \* el tratamiento es necesario para la salufacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

2 Evaluación del interés legítimo ( cumplimiento si anteriormente se ha seleccionado 'Interés legítimo')

¿El tratamiento es conforme a la legislación nacional y de la UE?

¿Existe la posibilidad de que algún aspecto del tratamiento a realizar entre en conflicto con alguna Ley de la UE? En tal caso, detallarlo

¿El tratamiento representa un interés real y actual de la entidad?

Los intereses de la empresa no pueden prevalecer sobre los de los interesados. La finalidad del tratamiento debe verse amparada bajo legitimación.

¿Existen otros medios menos invasivos para alcanzar la finalidad prevista del tratamiento y satisfacer el interés legítimo del responsable del tratamiento?

Debe adoptarse la vía en la que la intimidad del interesado, así como la de sus datos, se vea menos afectada.

¿Cuál es la naturaleza del interés de la entidad?

Describir detalladamente la razón y alcance del tratamiento que se va a hacer de los datos del interesado.

¿Cuál es el perjuicio que el responsable del tratamiento, los terceros o la comunidad en general puedan sufrir si no se realiza el tratamiento de datos?

Detallar las acciones o consecuencias que puede acarrear al responsable del tratamiento la no realización del tratamiento de datos.

¿Existe un desequilibrio entre la situación del interesado y la del responsable del tratamiento?

Ejemplos de personas que pueden considerarse vulnerables: menores, personas mayores, discapacitados, refugiados y/o solicitantes de asilo, etc.

¿El interesado ha sido debidamente informado sobre las actividades del tratamiento?

Se debe informar de las acciones, labores y tareas que se van a llevar a cabo con los datos del interesado, así como el alcance de las mismas.

¿Qué perjuicios pueden ocasionarse al interesado?

Detallar las acciones o consecuencias que puede experimentar el interesado tras la realización del tratamiento.

¿Se trata de un tratamiento normalizado en el sector?

Existen precedentes en el mercado y es una práctica común.

3 Evaluación de la necesidad y proporcionalidad de las operaciones de Tratamiento

Los datos recogidos se van a usar exclusivamente para la finalidad declarada y no para ninguna otra no informada ni incompatible con la legitimidad de su uso (principio de limitación de la finalidad).

El tratamiento de los datos se reduce únicamente a la finalidad establecida en el momento de su recogida.

La finalidad que se pretende cubrir requiere de todos los datos a recabar y para todas las personas/interesados afectados (principio de minimización de datos).

Los datos personales han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados

Las tecnologías empleadas para el tratamiento son adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios fundamentales de la privacidad.

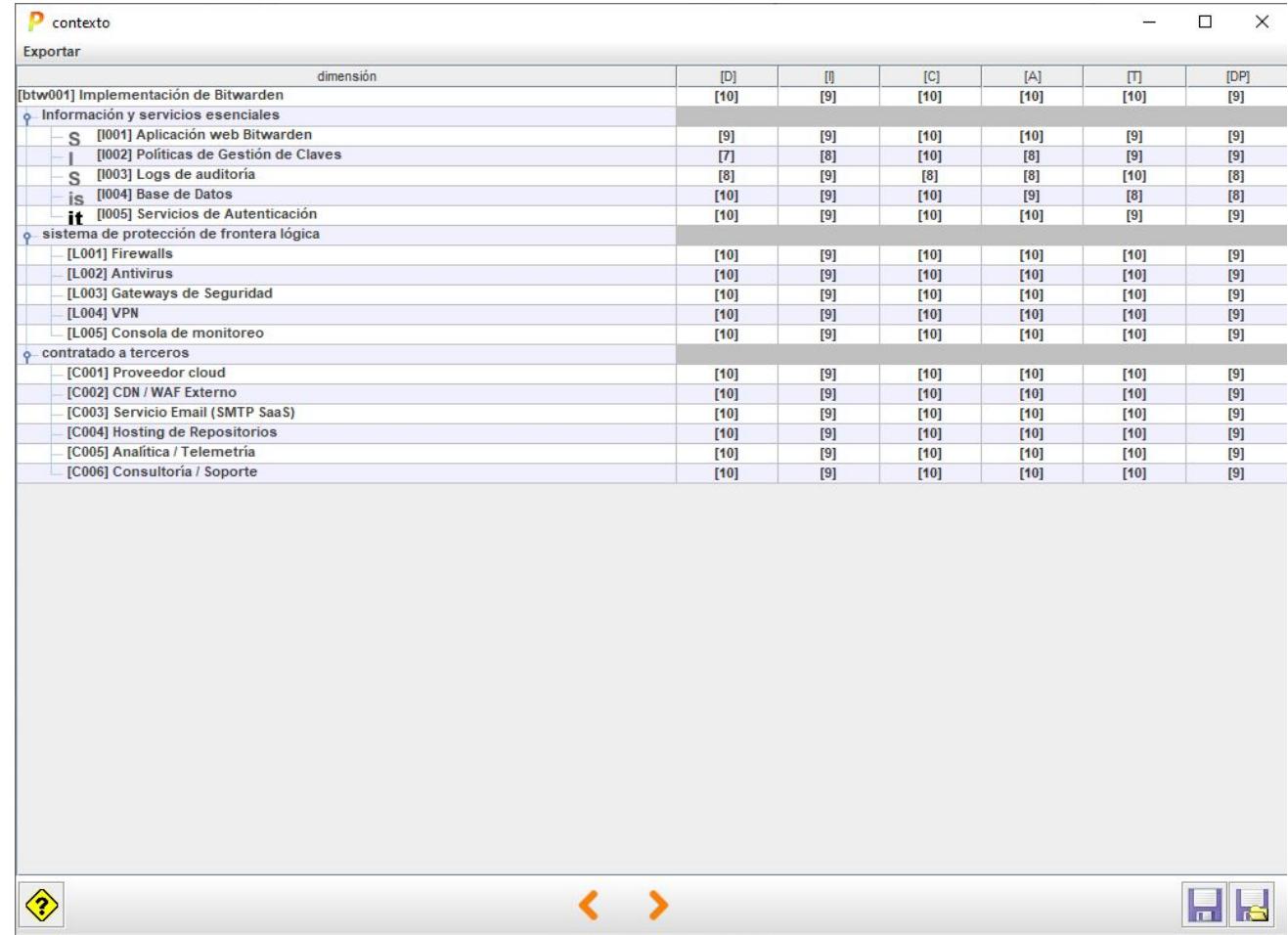
No deben utilizarse herramientas o tecnologías que comprometen la privacidad del interesado. A modo de ejemplo, el envío de sms masivos se considera intruso.

Los datos se mantienen más tiempo del necesario para las finalidades del tratamiento (principio de limitación del plazo de conservación).

Los datos no serán mantenidos más allá del requerimiento regulatorio pertinente ni de la finalidad con la que fueron recogidos.

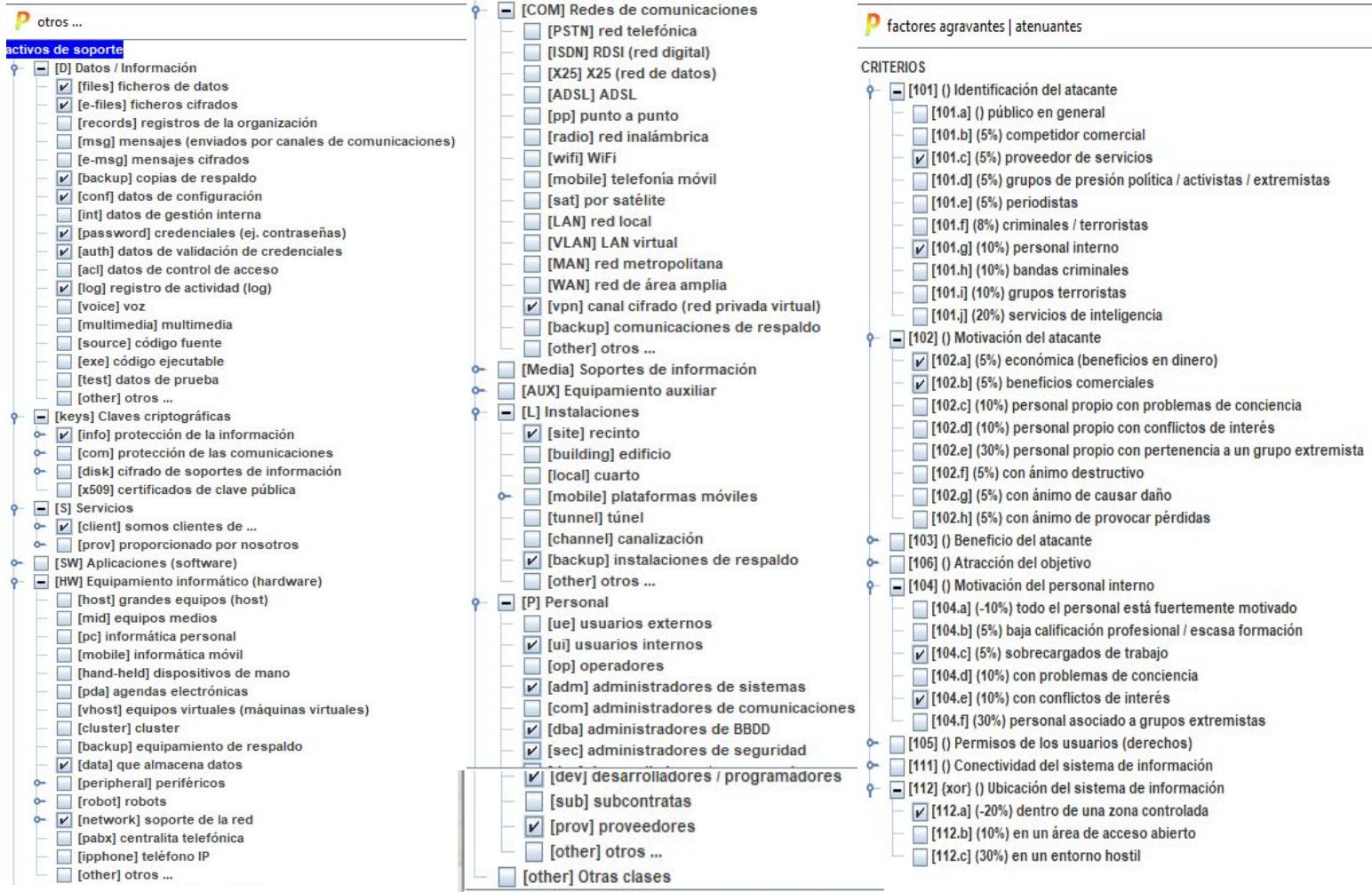
# Implementación de Bitwarden

Aquí mapeamos la solución técnica sobre los activos. Muestra visualmente qué partes de la organización serán cubiertas por la bóveda centralizada. Es el alcance funcional del proyecto



# Activos de Soporte vs Criterios

Árbol de dependencias de MAGERIT.  
Muestra que la **Información (Datos)** depende del **Servicio (Bitwarden)**, que a su vez depende del **Equipo (Servidor/Docker)**. Esto prueba que debemos proteger el servidor (hardening) para proteger el dato (herencia de riesgo).



# Tratamiento de los riesgos

---

## P tratamiento de los riesgos (opciones)

---

PILAR: salvaguardas

NIST SP800-53

[27002:2022] Control de la seguridad de la información

[27701:2019] Extensión de las Normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de provacidad de la información

[27002:2013] Código de prácticas para los controles de seguridad de la información

[BPS\_IP:2023]

[GDPR:2016] Reglamento relativo al tratamiento de datos personales

Resumen estratégico. Muestra qué riesgos vamos a **Mitigar** (con Bitwarden), cuáles vamos a **Transferir** (ej. seguros), cuáles vamos a **Eliminar** (borrar Excels) y cuáles **Aceptamos** (riesgo residual).

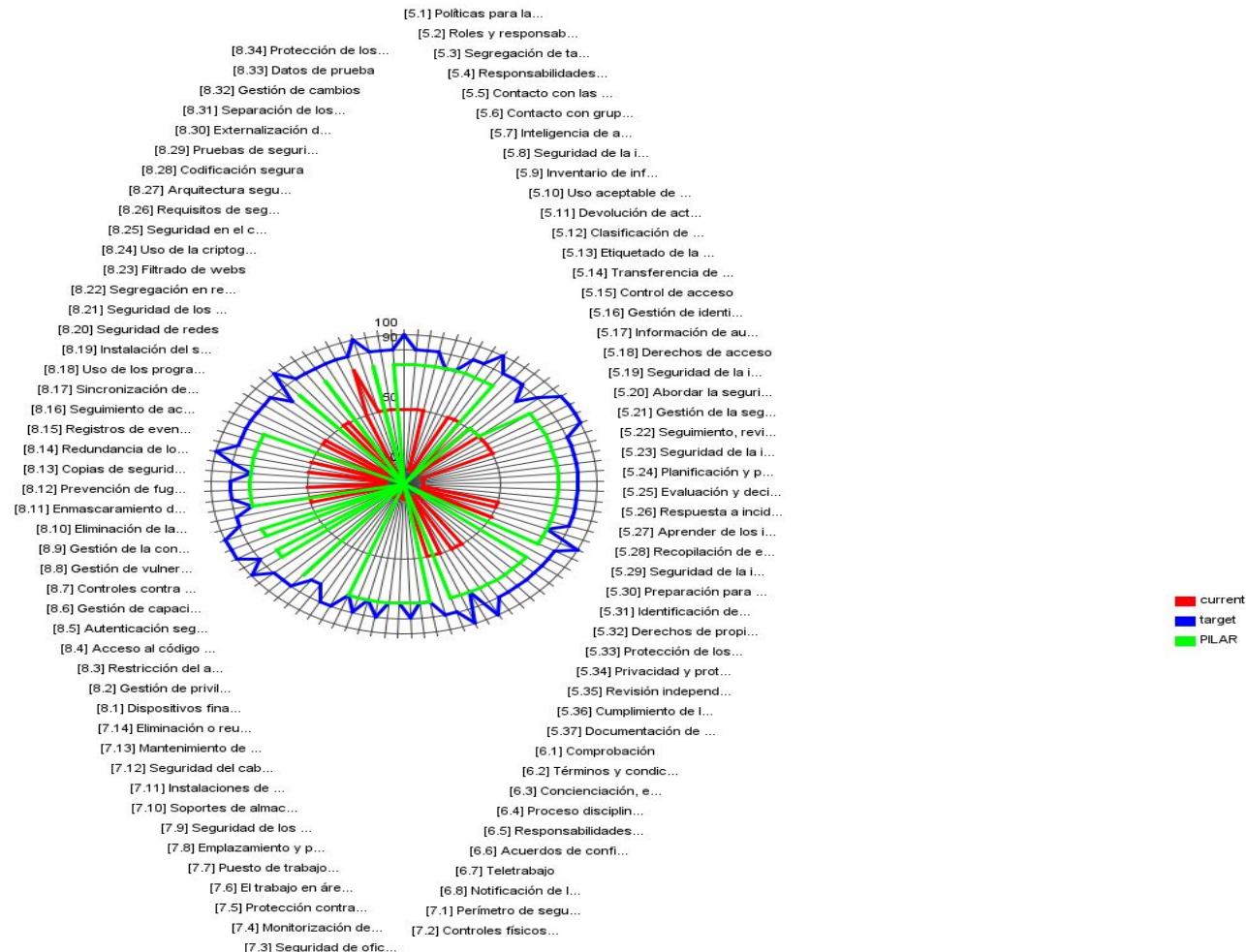
# Control de la seguridad de la información



Visión global de cumplimiento. Muestra el estado actual de inseguridad frente al estado objetivo seguro.

# Control de la seguridad de la información

"Gráfico de madurez  
(Spider Chart) enfocado  
en políticas. Muestra  
cómo pasamos de un  
nivel bajo a uno alto en  
'Gestión de Identidades'  
y 'Concientización'



# [27002:2022]Control de la seguridad de la información

recomendación	nivel	control	dudas	aplica	comentario	current	target
		[27002:2022] Control de la seguridad de la información				L0-L3	L3-L5
4	4	♀ [5] Organización /PR CR DC			...	L1-L2 (L1-L3)	L3-L5
4	4	o- [5.1] Políticas para la seguridad de la información /PR			Existe política general per...	L2	L5 (L4)
4	4	o- [5.2] Roles y responsabilidades en seguridad de la información /PR			Roles definidos pero falta ...	L2	L4
4	4	o- [5.3] Segregación de tareas /PR			Aplicar separación para acc...	L2 (L2-L3)	L4 (L4-L5)
4	4	o- [5.4] Responsabilidades de la dirección /PR			KPI y dashboard al Comité d...	L2 (L1)	L4
4	4	o- [5.5] Contacto con las autoridades /PR CR			Incluir en playbooks y cont...	L1 (L2)	L3 (L4)
4	4	o- [5.6] Contacto con grupos de interés especial /PR CR			Recomendar suscribir al me...	L1 (L2)	L3 (L4)
4	4	o- [5.7] Inteligencia de amenazas /PR CR DC			Enriquecer SIEM con feeds d...	L1 (L1-L2)	L4 (L3-L4)
4	4	o- [5.8] Seguridad de la información en la gestión de proyectos /PR			Integrar checklist security...	L2	L4 (L4-L5)
4	4	o- [5.9] Inventario de información y otros activos asociados /PR			Añadir tag "managed by thir...	L2 (L1-L3)	L5 (L4-L5)
4	4	o- [5.10] Uso aceptable de la información y activos asociados /PR			Aforzar acuerdos de uso y sa...	L2 (L1-L3)	L4 (L4-L5)
4	4	o- [5.11] Desvolvención de activos /PR			Procedimiento de revocación...	L1	L4
2	2	o- [5.12] Clasificación de la información /PR			Clasificar PII/Secret/Restr...	L2 (L1)	L4
2	2	o- [5.13] Etiquetado de la información /PR			Etiquetado automático en pi...	L1 (L1-L2)	L3 (L4)
2	2	o- [5.14] Transferencia de la información /PR			Requerir cifrado, MTA-STIS y...	L2 (L2-L3)	L4 (L4-L5)
4	4	o- [5.15] Control de acceso /PR			Implementar JIT, roles y re...	L2	L5
4	4	o- [5.16] Gestión de identidad /PR			Owner corporativo siempre d...	L2	L5
4	4	o- [5.17] Información de autenticación /PR			SSO + MFA obligatorio + rot...	L2	L5 (L4-L5)
4	4	o- [5.18] Derechos de acceso /PR			Workflows de approval y tim...	L2	L5
3	3	o- [5.19] Seguridad de la información en las relaciones con los proveedores /PR			SAST/DAST reportes de prove...	L1 (L2)	L4
3	3	o- [5.20] Abordar la seguridad de la información dentro de los acuerdos de proveedores /PR			Requerir SBOM y SLSA mínimo...	L1 (L1-L3)	L4 (L4-L5)
3	3	o- [5.21] Gestión de la seguridad de la información en la cadena de suministro de las TIC /PR			Integrar en riesgo empresar...	L1 (L1-L2)	L4
3	3	o- [5.22] Seguimiento, revisión y gestión del cambio de los servicios de proveedores /PR			Unificar procesos y evidenc...	L1 (L1-L2)	L4
3	3	o- [5.23] Seguridad de la información para el uso de servicios en la nube /PR			L1 (L1-L3)	L4 (L4-L5)	
4	4	o- [5.24] Planificación y preparación de la gestión de incidentes de seguridad de la información /CR			Pruebas anuales y plan de f...	L1 (L1-L2)	L4
4	4	o- [5.25] Evaluación y decisión sobre los eventos de seguridad de la información /DC			L1 (L2)	L4	
4	4	o- [5.26] Respuesta a incidentes de seguridad de la información /CR			Simulacros conjuntos y comu...	L1 (L1-L2)	L4
4	4	o- [5.27] Aprender de los incidentes de seguridad de la información /PR			L1 (L2)	L4	
4	4	o- [5.28] Recopilación de evidencias /CR			Requerir acceso read-only a...	L2	L4
4	4	o- [5.29] Seguridad de la información durante la interrupción /PR CR			L2	L4 (L3-L4)	
4	4	o- [5.30] Preparación para las TIC para la continuidad del negocio /CR			L1 (L1-L2)	L3 (L3-L4)	
3	3	o- [5.31] Identificación de requisitos legales, reglamentarios y contractuales /PR			Mapeo por territorio y serv...	L2 (L3)	L5
4	4	o- [5.32] Derechos de propiedad intelectual (DPI) /PR			Cláusula de propiedad y uso...	L1 (L3)	L4 (L5)
4	4	o- [5.33] Protección de los registros /PR			Retention policy contractua...	L1 (L3)	L4 (L5)
4	4	o- [5.34] Privacidad y protección de datos de carácter personal (DCP) /PR			Pseudonimización, cifrado y...	L1 (L3)	L4 (L5)
4	4	o- [5.35] Revisión independiente de la seguridad de la información /CR			L1 (L3)	L4 (L5)	
4	4	o- [5.36] Cumplimiento de las políticas y normas de seguridad de la información /PR			L1 (L3)	L4 (L5)	
4	4	o- [5.37] Documentación de procedimientos operacionales /PR CR			L1 (L1-L2)	L4	
4	4	♀ [6] Controles de personal /PR CR DC			...	L1-L2 (L1-L3)	L3-L5 (L4-L5)
3	3	o- [6.1] Compromiso y motivación /PR			Exigir screening ampliado p...	L2 (L1)	L4
4	4	o- [6.2] Normas y condiciones de contratación /PR			Reforzar NDA sobre manejo d...	L2 (L1-L3)	L4 (L4-L5)
4	4	o- [6.3] Concienciación, educación y formación en seguridad de la información /PR			Incluir módulos de: MFA, va...	L2 (L1)	L5 (L4)
4	4	o- [6.4] Proceso disciplinario /PR CR			Añadir política explícita...	L1	L3
4	4	o- [6.5] Responsabilidades ante la finalización o cambio /PR			Offboarding automático + ki...	L2 (L1-L3)	L5 (L4-L5)
4	4	o- [6.6] Acuerdos de confidencialidad o no divulgación /PR			Actualizar NDAs a formato 2...	L2 (L3)	L4 (L5)
4	4	o- [6.7] Teletrabajo /PR			Exigir dispositivos corpora...	L2	L4
4	4	o- [6.8] Notificación de los eventos de seguridad de la información /DC			PMO debe incorporar RACI y ...	L1 (L2)	L3 (L4)
4	4	♀ [7] Controles físicos /PR DC			...	L0-L1 (L0-L2)	L3-L4
3	3	o- [7.1] Perímetro de seguridad física /PR			Los proveedores manipulan a...	L1 (L4-L2)	L3
4	4	o- [7.2] Controles físicos de entrada /PR			El control de visitas es ma...	L1 (L2)	L4 (L3)
4	4	o- [7.3] Seguridad de oficinas, despachos y recursos /PR			Áreas sensibles no siempre ...	L1 (L2)	L3
4	4	o- [7.4] Monitoreo de la seguridad física /PR DC			Cámaras sin auditoría ni re...	L1	L3
4	4	o- [7.5] Protección contra las amenazas externas y ambientales /PR			Falta inventario y respuesta...	L1 (L2)	L4 (L3)
4	4	o- [7.6] El trabajo en áreas seguras /PR			No siempre se valida el pro...	L1 (L2)	L3
4	4	o- [7.7] Puesto de trabajo despejado y pantalla limpia /PR			Contratistas dejan equipos ...	L0 (L0-L2)	L4 (L3-L4)
4	4	o- [7.8] Empalmamiento y protección de equipos /PR			Dispersión de laptops y ser...	L1 (L2)	L3
4	4	o- [7.9] Seguridad de los equipos fuera de las instalaciones /PR			No hay trazabilidad adecuad...	L1 (L2)	L4 (L3)
4	4	o- [7.10] Soportes de almacenamiento /PR			No existe control de cifrad...	L1 (L1-L2)	L4 (L3-L4)
4	4	o- [7.11] Instalaciones de suministro /PR DC			Sin protocolos formales de ...	L1 (L2)	L3
4	4	o- [7.12] Seguridad del cableado /PR			No siempre hay supervisión ...	L1 (L2)	L3
3	3	o- [7.13] Mantenimiento de los equipos /PR			Falta validación de identid...	L1 (L1-L2)	L4
4	4	o- [7.14] Eliminación o reutilización segura de los equipos /PR			Contratistas eliminan hardw...	L1 (L1-L2)	L4 (L3-L4)
4	4	♀ [8] Controles tecnológicos /PR CR DC			...	L0-L3 (L1-L3)	L3-L5
4	4	o- [8.1] Dispositivos finales de usuario /PR			No existe gestión completa ...	L1 (L2)	L4 (L3-L4)
3	3	o- [8.2] Gestión de privilegios de acceso * /PR			Los accesos admin se compar...	L0 (L2)	L5
4	4	o- [8.3] Restricción del acceso a la información /PR			Roles difusos, accesos otor...	L1 (L2)	L4 (L5)
4	4	o- [8.4] Acceso al código fuente /PR			Guardias credenciales en arc...	L0 (L2)	L5
4	4	o- [8.5] Autenticación segura /PR			Autenticación simple, sin c...	L1 (L2)	L5
4	4	o- [8.6] Gestión de capacidades /PR DC			L1 (L2)	L5 (L4)	
4	4	o- [8.7] Controles contra el código malicioso /PR CR DC			Antivirus no corporativo.	L0 (L2)	L4
4	4	o- [8.8] Gestión de vulnerabilidades técnicas /PR			Parcheo inconsistente en eq...	L2 (L2-L3)	L4 (L3-L4)
4	4	o- [8.9] Gestión de la configuración /PR			Configuraciones ad hoc.	L2	L3 (L3-L4)
3	3	o- [8.10] Eliminación de la información /PR			L1 (L1-L2)	L4	
4	4	o- [8.11] Enmascaramiento de datos /PR			L2	L4	
3	3	o- [8.12] Prevención de fugas de datos /PR DC			Sin herramientas robustas n...	L1 (L1-L3)	L4 (L3-L5)
3	3	o- [8.13] Copias de seguridad de la información * /CR			L1 (L2)	L3 (L4)	
4	4	o- [8.14] Redundancia de los recursos de tratamiento de la información /PR			L2	L4	

# [27002:2022]Control de la seguridad de la información

## Continuación

	recomendación	nivel	control	dudas	aplica	comentario	current	target
	3		o ✓ [8.15] Registros de eventos /DC o ✓ [8.16] Seguimiento de actividades /CR DC o ✓ [8.17] Sincronización del reloj /DC o ✓ [8.18] Uso de los programas de utilidad con privilegios /PR o ✓ [8.19] Instalación del software en sistemas de producción /PR o ✓ [8.20] Seguridad de redes /PR DC			Actividades no c...	L1 (L2)	L5 (L4)
	4		o ✓ [8.21] Seguridad de los servicios de red /PR o ✓ [8.22] Segregación en redes /PR o ✓ [8.23] Filtrado de webs /PR o ✓ [8.24] Uso de la criptografía /PR			Reglas amplias y ...	L2 (L2-L3)	L4 (L4-L5)
	3		o ✓ [8.25] Seguridad en el ciclo de vida del desarrollo /PR o ✓ [8.26] Requisitos de seguridad de las aplicaciones /PR o ✓ [8.27] Arquitectura segura de sistemas y principios de ingeniería /PR o ✓ [8.28] Codificación segura /PR o ✓ [8.29] Pruebas de seguridad en desarrollo y aceptación /PR o ✓ [8.30] Externalización del desarrollo /PR DC			Equipos externo...	L1 (L2)	L3 (L3-L4)
	4		o ✓ [8.31] Separación de los entornos de desarrollo, prueba y producción /PR o ✓ [8.32] Gestión de cambios /PR o ✓ [8.33] Datos de prueba /PR o ✓ [8.34] Protección de los sistemas de información durante las pruebas de auditoría /PR			No hay cifrado de...	L1 (L2-L3)	L5
	3		[27701:2019] Extensión de las Normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de provacidad de la información				L2	L4 (L4-L5)
	3		o ✓ [6] Guía específica del SGPI relacionadas con la Norma ISO/IEC 27002				L2 (L2-L3)	L4 (L4-L5)
	3		o ✓ [6.2] Políticas de seguridad de la información			Poíticas existen ...	L1 (L2)	L3-L5
	2		o ✓ [6.3] Organización de la seguridad de la información			Estructura ISMS ...	L2 (L2-L3)	L4 (L3-L5)
	2		o ✓ [6.4] Seguridad relativa a los recursos humanos			Gestión de crede...	L1 (L1-L3)	L4 (L4-L5)
	2		o ✓ [6.5] Gestión de activos			No hay gestión cif...	L1 (L1-L3)	L4 (L3-L5)
	2		o ✓ [6.6] Control de acceso			Bitwarden mejora...	L2 (L2-L3)	L5 (L4-L5)
	2		o ✓ [6.7] Criptografía			Cifrado inconsist...	L2 (L2-L3)	L5
	2		o ✓ [6.8] Seguridad física y del entorno			Bitwarden no apli...	L2	L3 (L3-L4)
	2		o ✓ [6.9] Seguridad de las operaciones			Bitwarden aporta ...	L2	L4 (L4-L5)
	2		o ✓ [6.10] Seguridad de las comunicaciones			Bitwarden usa TL...	L3 (L2-L3)	L5 (L4-L5)
	2		o ✓ [6.11] Adquisición, desarrollo y mantenimiento de los sistemas de información			Bitwarden Secret...	L2 (L2-L3)	L5
	2		o ✓ [6.12] Relación con proveedores			Bitwarden facilita ...	L2 (L2-L3)	L4 (L4-L5)
	2		o ✓ [6.13] Gestión de incidentes de seguridad de la información			Bitwarden soport...	L2	L4
	2		o ✓ [6.14] Aspectos de la seguridad de la información para la gestión de la continuidad del negocio			Bitwarden garanti...	L2	L4
	2		o ✓ [6.15] Cumplimiento			Bitwarden ayuda ...	L3	L5
	2		o ✓ [7] Guía adicional de la Norma ISO/IEC 27002 para el responsable del tratamiento de IP			...	L1-L2	L3-L4
	2		o ✓ [7.2] Condiciones para la recogida y el tratamiento			protege los siste...	L2	L3
	2		o ✓ [7.3] Obligaciones hacia los interesados			asegura la entreg...	L1	L3
	2		o ✓ [7.4] Privacidad desde el diseño y privacidad por defecto			Bitwarden imple...	L1	L4
	2		o ✓ [7.5] Intercambio, transferencia y comunicación de IP			Bitwarden evita fil...	L2	L4
	2		o ✓ [8] Guía adicional de la Norma ISO / IEC 27002 para el encargado del tratamiento de IP			...	L1-L2	L3-L4
	2		o ✓ [8.2] Condiciones de recogida y tratamiento			El rol de Backus c...	L2	L4
	2		o ✓ [8.3] Obligaciones hacia los interesados			Bitwarden proteg...	L1	L3
	2		o ✓ [8.4] Privacidad desde el diseño y privacidad por defecto			Managing secret...	L1	L4
	2		o ✓ [8.5] Intercambio, transferencia y comunicación de IP			Bitwarden registr...	L2	L4

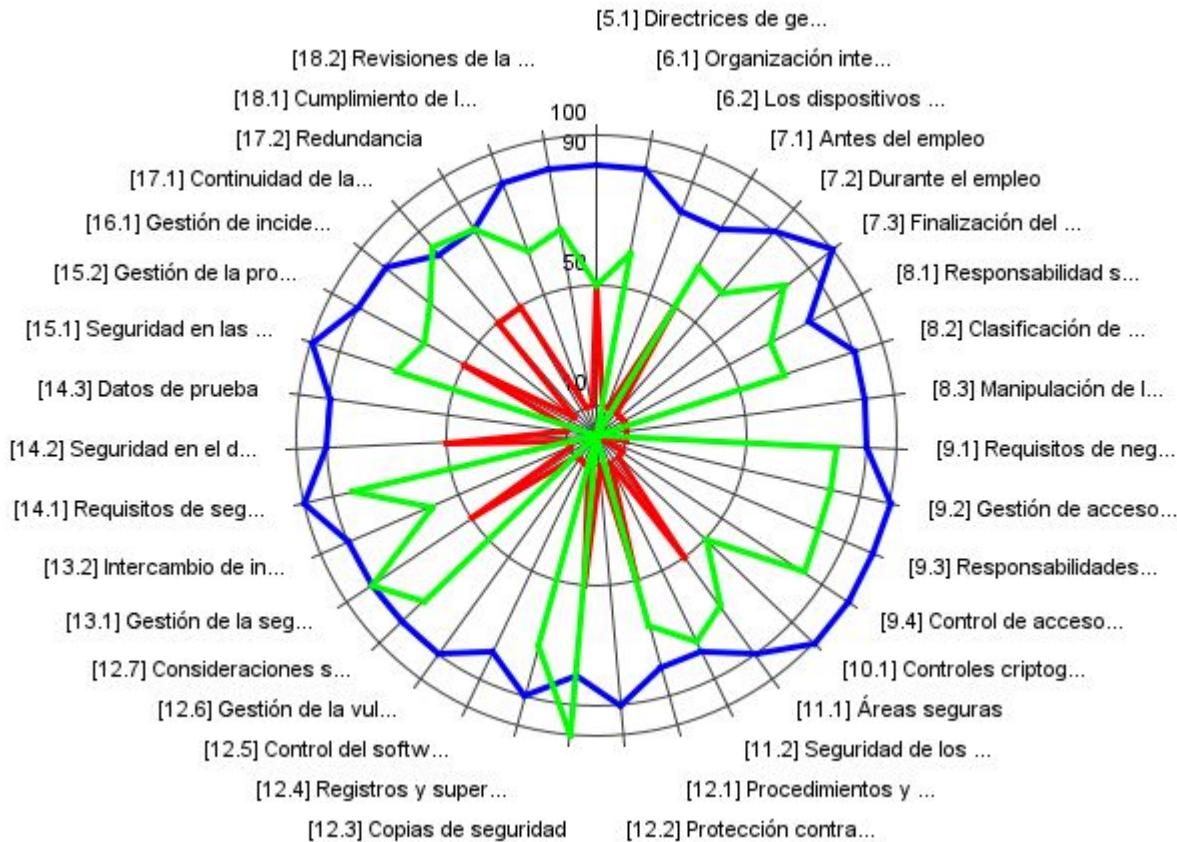
# [27002:2013]Código de prácticas para los controles de seguridad de la información

P [27002:2013] Código de prácticas para los controles de seguridad de la información

Expandir Operación Ver Exportar Estadísticas

recomendación	nivel	control	dudas	aplica	comentario	current	target
		[27002:2013] Código de prácticas para los controles de seguridad de la información				L0-L2 (L1-L3)	L3-L5
2		⌚ [5] Políticas de seguridad de la información	...			L2	L4
2		⌚ [5.1] Directrices de gestión de la seguridad de la información	No menciona ges...			L2	L4
5		⌚ [6] Organización de la seguridad de la información	...			L1 (L2-L3)	L3-L4 (L3-L5)
5		⌚ [6.1] Organización interna	No existe un resp...			L1 (L2-L3)	L4 (L4-L5)
6		⌚ [6.2] Los dispositivos móviles y el teletrabajo	No hay lineamient...			L1 (L2)	L3 (L3-L4)
5		⌚ [7] Seguridad relativa a los recursos humanos	...			L1-L2 (L1-L3)	L3-L5 (L4-L5)
6		⌚ [7.1] Antes del empleo	Validación incons...			L2 (L1-L3)	L3 (L4-L5)
6		⌚ [7.2] Durante el empleo	No incluye manejo...			L1	L4
5		⌚ [7.3] Finalización del empleo o cambio en el puesto de trabajo	Cuentas quedan ...			L1 (L1-L3)	L5 (L4-L5)
5		⌚ [8] Gestión de activos	...			L1 (L1-L3)	L3-L4 (L3-L5)
5		⌚ [8.1] Responsabilidad sobre los activos	Inventory de lapt...			L1 (L1-L3)	L3 (L4-L5)
5		⌚ [8.2] Clasificación de la información	Terceros tratan P...			L1 (L1-L2)	L4 (L3-L4)
5		⌚ [8.3] Manipulación de los soportes	Riesgo de USB o c...			L1 (L1-L3)	L4 (L3-L5)
6		⌚ [9] Control de acceso	...			L0-L1 (L2-L3)	L4-L5
3		⌚ [9.1] Requisitos de negocio para el control de acceso	No hay segmenta...			L1 (L2-L3)	L4 (L5)
4		⌚ [9.2] Gestión de acceso de usuario	Cuentas comparti...			L1 (L2)	L5 (L4-L5)
5		⌚ [9.3] Responsabilidades del usuario	Guardan en What...			L0 (L2)	L5
6		⌚ [9.4] Control de acceso a sistemas y aplicaciones	Usuario/contrase...			L1 (L2)	L5
2		⌚ [10] Criptografía	...			L1 (L2-L3)	L5
2		⌚ [10.1] Controles criptográficos	No se exige form...			L1 (L2-L3)	L5
5		⌚ [11] Seguridad física y del entorno	...			L1-L2 (L2)	L3-L4
5		⌚ [11.1] Áreas seguras	No tiene supe...			L2	L4 (L3)
5		⌚ [11.2] Seguridad de los equipos	Laptops externas...			L1 (L2)	L3 (L3-L4)
9		⌚ [12] Seguridad de las operaciones	...			L1-L2 (L2)	L3-L4 (L4-L5)
3		⌚ [12.1] Procedimientos y responsabilidades operacionales	Depende del prov...			L2	L3 (L4-L5)
5		⌚ [12.2] Protección contra el software malicioso (malware)	...			L1 (L2)	L4
9		⌚ [12.3] Copias de seguridad	...			L2	L3 (L4)
4		⌚ [12.4] Registros y supervisión	Falta registro de ...			L1 (L2)	L4
		⌚ [12.5] Control del software en explotación	Riegos de softwa...			L1 (L2)	L3 (L4-L5)
		⌚ [12.6] Gestión de la vulnerabilidad técnica	...			L1 (L2)	L4 (L4-L5)
4		⌚ [12.7] Consideraciones sobre la auditoría de sistemas de información	...			L1 (L2)	L4
8		⌚ [13] Seguridad de las comunicaciones	...			L1-L2 (L2-L3)	L4 (L4-L5)
8		⌚ [13.1] Gestión de la seguridad de redes	Reglas amplias.			L2 (L2-L3)	L4 (L4-L5)
4		⌚ [13.2] Intercambio de información	Envíos por correo...			L1 (L2-L3)	L4 (L4-L5)
6		⌚ [14] Adquisición, desarrollo y mantenimiento de los sistemas de información	...			L1-L2 (L2-L3)	L4-L5 (L5)
6		⌚ [14.1] Requisitos de seguridad en sistemas de información	No se exige vaulti...			L1 (L2-L3)	L5
5		⌚ [14.2] Seguridad en el desarrollo y en los procesos de soporte	Manejo inseguro ...			L2 (L2-L3)	L4 (L5)
5		⌚ [14.3] Datos de prueba	Mal práctica frecu...			L1 (L2)	L4 (L5)
5		⌚ [15] Relación con proveedores	...			L1-L2 (L2-L3)	L4-L5
5		⌚ [15.1] Seguridad en las relaciones con proveedores	No se exige almac...			L1 (L2-L3)	L5 (L4-L5)
3		⌚ [15.2] Gestión de la provisión de servicios del proveedor	Gestión reactiva.			L2	L4
5		⌚ [16] Gestión de incidentes de seguridad de la información	...			L1 (L2)	L4
5		⌚ [16.1] Gestión de incidentes de seguridad de la información y mejoras	No hay SLA de no...			L1 (L2)	L4
7		⌚ [17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio	...			L2	L3 (L3-L4)
7		⌚ [17.1] Continuidad de la seguridad de la información	No se verifican ni ...			L2	L3 (L3-L4)
5		⌚ [17.2] Redundancia	Single points of f...			L2	L3 (L4)
5		⌚ [18] Cumplimiento	...			L1 (L2)	L4 (L5)
3		⌚ [18.1] Cumplimiento de los requisitos legales y contractuales	No monitoreo Pil...			L1 (L2)	L4 (L5)
5		⌚ [18.2] Revisiones de la seguridad de la información	No existe revisió...			L1 (L2)	L4 (L5)

# [27002:2013]Código de prácticas para los controles de seguridad de la información

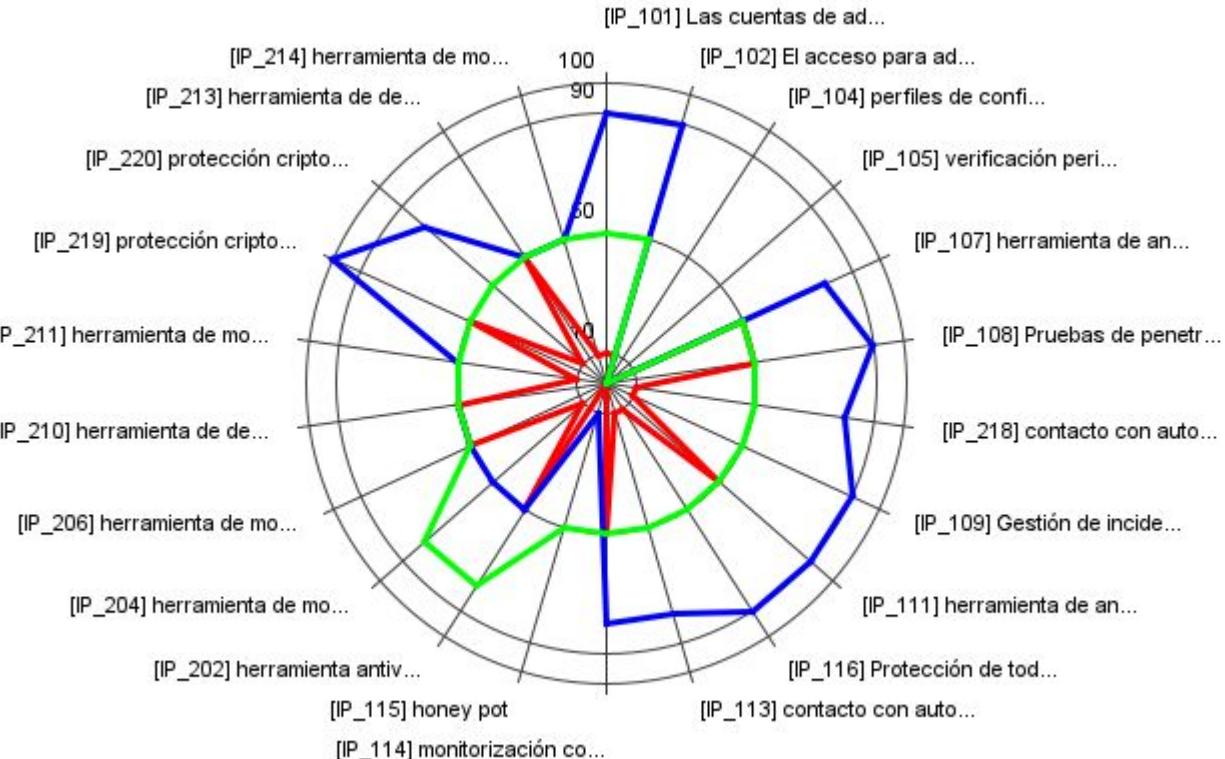


# BPS\_IP:2023

## [IP]Sistema de protección de frontera lógica /PR AD

 [BPS\_IP:2023]

	recomendación	nivel	control	dudas	aplica	comentario	current	target
			[BPS_IP:2023]				L0-L2	L1-L5
	4		♀  [IP] Sistema de protección de frontera lógica /PR AD		...	...	L0-L2	L1-L5
	4		♀  [IP_100] Administración /AD		...	...	L0-L2	L1-L4
	2		♀  [IP_101] Las cuentas de administración están bajo estricto control			Bitwarden Enterp...	L1	L4
	2		♀  [IP_102] El acceso para administración es seguro			Sin Bitwarden hay...	L1	L4
	4		♀  [IP_103] Gestión segura de la configuración			Se fortalece con v...	L1	L4
			(i) perfiles de configuración autorizados					
			(i) verificación periódica					
	2		♀  [IP_106] Gestión de vulnerabilidades /MN		...	...	L1-L2	L3-L4
	2		?	?		Escaneos requier...	L2	L3
	2		?	?		Mejora la segurid...	L2	L4
	2		?	?		Bitwarden facilita ...	L1	L3
	2		?	?		Bitwarden propor...	L1	L4
	2		?	?		...	L1-L2	L4
	2		?	?		Permite integrars...	L2	L4
	2		?	?		Vault cifrado y se...	L1	L4
	2		?	?		...	L0-L2	L1-L3
	2		?	?		Compartir creden...	L1	L3
	2		?	?		Bitwarden contrib...	L2	L3
	2		?	?		No relacionado di...	L0	L1
	4		♀  [IP_112] Inteligencia de amenazas /PR		...	...	L1-L2	L2-L5
	4		♀  [IP_113] contacto con autoridades, CERTs y fabricantes			No es función de ...	L2	L2
	4		?	?		Sin relación	L2	L2
	4		♀  [IP_203] Se inspecciona el contenido /DC			No aplica directa...	L1	L2
	4		?	?		Se alinea a secret...	L1	L2
	2		?	?		Protección de cre...	L2	L2
	2		?	?		No es parte de Bit...	L2	L2
	2		?	?	n.a.	Sin relación		
	2		?	?	n.a.			
	2		?	?	n.a.			
	2		?	?	...	...	L1-L2	L2-L5
	2		?	?		No aplica directa...	L2	L2
	2		?	?		Bitwarden mejora...	L1	L2
	2		?	?		Bitwarden cifrado...	L2	L5
	2		?	?		No nativo pero pr...	L1	L3
	2		?	?	n.a.			
	2		?	?	...	...	L1-L2	L2
	2		?	?		L2	L2	
	2		?	?		L1	L2	
	2		?	?	n.a.			



P por dominios: BPS\_IP:2023 X

dominio de seguridad			IP	total
[base]	Base		42	42
control	base	total		
IP	42	42		
TOTAL	42	42		

índice de madurez				
dominio de seguridad			current	target
[base]	Base		26%	69%

índice de cumplimiento				
dominio de seguridad			current	target
[base]	Base		0%	0%

# [GDPR:2016]Reglamento relativo al tratamiento de datos personales

P [GDPR:2016] Reglamento relativo al tratamiento de datos personales

Expandir Operación Ver Exportar Estadísticas

	recomendación	nivel	control	dudas	GDPR	aplica	comentario	current	target
			[GDPR:2016] Reglamento relativo al tratamiento de datos personales					L1-L2	L1-L5
	2		o- ✓ [A5] Artículo 5 - Principios relativos al tratamiento				Falta estandariz...	L2	L4
	2		o- ✓ [A6] Artículo 6 - Licitud del tratamiento				Cumple base le...	L2	L3
	2		o- ✓ [A7] Artículo 7 - Condiciones para el consentimiento				Consentimiento...	L1	L2
			o- ✓ [A8] Artículo 8 - Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información				No aplica al con...	L2	L4
			o- ✓ [A9] Artículo 9 - Tratamiento de categorías especiales de datos personales				Datos sensible...	L2	L4
			o- ✓ [A10] Artículo 10 - Tratamiento de datos personales relativos a condenas e infracciones penales				No aplica.	L1	L1
	2		o- ✓ [A11] Artículo 11 - Tratamiento que no requiere identificación				Control poco re...	L1	L1
	2		o- ✓ [A12] Artículo 12 - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado				Repositorios d...	L2	L3
	2		o- ✓ [A13] Artículo 13 - Información que deberá facilitarse cuando los datos personales se obtengan del interesado				Proceso corpor...	L2	L3
	2		o- ✓ [A14] Artículo 14 - Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado				Igual que A13, ...	L2	L3
	2		o- ✓ [A15] Artículo 15 - Derecho de acceso del interesado				Bitwarden ayud...	L1	L2
	2		o- ✓ [A16] Artículo 16 - Derecho de rectificación				Depende del si...	L2	L3
	2		o- ✓ [A17] Artículo 17 - Derecho de supresión («el derecho al olvido»)				Requiere proce...	L1	L3
	2		o- ✓ [A18] Artículo 18 - Derecho a la limitación del tratamiento				Necesita polític...	L1	L2
	2		o- ✓ [A19] Artículo 19 - Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento				Requiere auto...	L1	L2
	2		o- ✓ [A20] Artículo 20 - Derecho a la portabilidad de los datos				No impactado p...	L1	L2
	2		o- ✓ [A21] Artículo 21 - Derecho de oposición				Gestión manual.	L1	L2
	2		o- ✓ [A22] Artículo 22 - Decisiones individuales automatizadas, incluida la elaboración de perfiles			n.a.			
	2		o- ✓ [A24] Artículo 24 - Responsabilidad del responsable del tratamiento				Control fuerte; ...	L2	L4
	2		o- ✓ [A25] Artículo 25 - Protección de datos desde el diseño y por defecto				Bitwarden apor...	L2	L5
	2		o- ✓ [A26] Artículo 26 - Corresponsables del tratamiento				Aplica cuando h...	L1	L2
	2		o- ✓ [A28] Artículo 28 - Encargado del tratamiento				Bitwarden se c...	L2	L4
	2		o- ✓ [A29] Artículo 29 - Tratamiento bajo la autoridad del responsable o del encargado del tratamiento				Bitwarden fort...	L2	L5
	2		o- ✓ [A30] Artículo 30 - Registro de las actividades de tratamiento				Independiente ...	L2	L3
	2		o- ✓ [A31] Artículo 31 - Cooperación con la autoridad de control				Sin relación Bit...	L2	L3
	2		o- ✓ [A32] Artículo 32 - Seguridad del tratamiento				Bitwarden apor...	L2	L5
	2		o- ✓ [A33] Artículo 33 - Notificación de una violación de la seguridad de los datos personales a la autoridad de control				Bitwarden mejor...	L2	L3
	2		o- ✓ [A34] Artículo 34 - Comunicación de una violación de la seguridad de los datos personales al interesado				No relacionado ...	L1	L2
	2		o- ✓ [A35] Artículo 35 - Evaluación de impacto relativa a la protección de datos				Bitwarden facil...	L1	L3
	2		o- ✓ [A36] Artículo 36 - Consulta previa			n.a.			
	2		o- ✓ [A37] Artículo 37 - Designación del delegado de protección de datos				No afectado por...	L2	L3
	2		o- ✓ [A38] Artículo 38 - Posición del delegado de protección de datos				No impacta Bit...	L2	L3
	2		o- ✓ [A39] Artículo 39 - Funciones del delegado de protección de datos				No impacta Bit...	L2	L3
	2		o- ✓ [A45] Artículo 45 - Transferencias basadas en una decisión de adecuación			n.a.			
	2		o- ✓ [A46] Artículo 46 - Transferencias mediante garantías adecuadas				Bitwarden facili...	L2	L5
	2		o- ✓ [A47] Artículo 47 - Normas corporativas vinculantes				Independiente ...	L2	L3
	2		o- ✓ [A48] Artículo 48 - Transferencias o comunicaciones no autorizadas por el Derecho de la Unión				Control legal; Bi...	L2	L3
	2		o- ✓ [A49] Artículo 49 - Excepciones para situaciones específicas				Sin relación co...	L1	L1

# RIESGOS(POTENCIAL Y CURRENT)

P riesgos

Exportar

potencial current target PILAR

	activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS		{7,3}	{7,5}	{8,1}	{8,1}	{8,1}	{6,7}
S [I001] Aplicación web Bitwarden		{6,7}	{7,5}	{8,1}	{8,1}	{7,5}	
I [I002] Políticas de Gestión de Claves		{5,6}	{7,0}	{8,1}	{7,0}	{7,5}	
S [I003] Logs de auditoría		{6,2}	{7,5}	{7,0}	{7,0}	{8,1}	
is [I004] Base de Datos		{7,3}	{7,5}	{8,1}	{7,5}	{7,0}	
it [I005] Servicios de Autenticación		{7,3}	{7,5}	{8,1}	{8,1}	{7,5}	{6,7}

P riesgos

Exportar

potencial current target PILAR

	activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS		{5,5}	{5,9}	{6,5}	{6,5}	{6,3}	{4,4}
S [I001] Aplicación web Bitwarden		{4,9}	{5,9}	{6,5}	{6,5}	{5,7}	
I [I002] Políticas de Gestión de Claves		{3,8}	{5,3}	{6,5}	{5,3}	{5,7}	
S [I003] Logs de auditoría		{4,4}	{5,9}	{5,3}	{5,3}	{6,3}	
is [I004] Base de Datos		{5,5}	{5,9}	{6,5}	{5,9}	{5,1}	
it [I005] Servicios de Autenticación		{5,5}	{5,9}	{6,5}	{6,5}	{5,7}	{4,4}

# RIESGOS(TARGET Y PILAR)

P riesgos

Exportar

	potencial	current	target	PILAR			
	activo						
<input type="checkbox"/>	ACTIVOS	[D]	[I]	[C]	[A]	[T]	[DP]
<input type="checkbox"/>	o S [I001] Aplicación web Bitwarden	{2,8}	{2,6}	{3,2}	{3,1}	{3,2}	{2,4}
<input type="checkbox"/>	o I [I002] Políticas de Gestión de Claves	{2,2}	{2,6}	{3,2}	{3,1}	{2,6}	
<input type="checkbox"/>	o S [I003] Logs de auditoría	{1,0}	{2,0}	{3,2}	{2,0}	{2,6}	
<input type="checkbox"/>	o is [I004] Base de Datos	{1,6}	{2,6}	{2,1}	{2,0}	{3,2}	
<input type="checkbox"/>	o it [I005] Servicios de Autenticación	{2,8}	{2,6}	{3,2}	{2,6}	{2,0}	
<input type="checkbox"/>		{2,8}	{2,6}	{3,2}	{3,1}	{2,6}	{2,4}

P riesgos

Exportar

	potencial	current	target	PILAR			
	activo						
<input type="checkbox"/>	ACTIVOS	[D]	[I]	[C]	[A]	[T]	[DP]
<input type="checkbox"/>	o S [I001] Aplicación web Bitwarden	{3,9}	{4,1}	{4,7}	{4,7}	{4,7}	{3,8}
<input type="checkbox"/>	o I [I002] Políticas de Gestión de Claves	{3,3}	{4,1}	{4,7}	{4,7}	{4,1}	
<input type="checkbox"/>	o S [I003] Logs de auditoría	{2,1}	{3,5}	{4,7}	{3,5}	{4,1}	
<input type="checkbox"/>	o is [I004] Base de Datos	{2,7}	{4,1}	{3,5}	{3,5}	{4,7}	
<input type="checkbox"/>	o it [I005] Servicios de Autenticación	{3,9}	{4,1}	{4,7}	{4,1}	{3,5}	
<input type="checkbox"/>		{3,9}	{4,1}	{4,7}	{4,7}	{4,1}	{3,8}

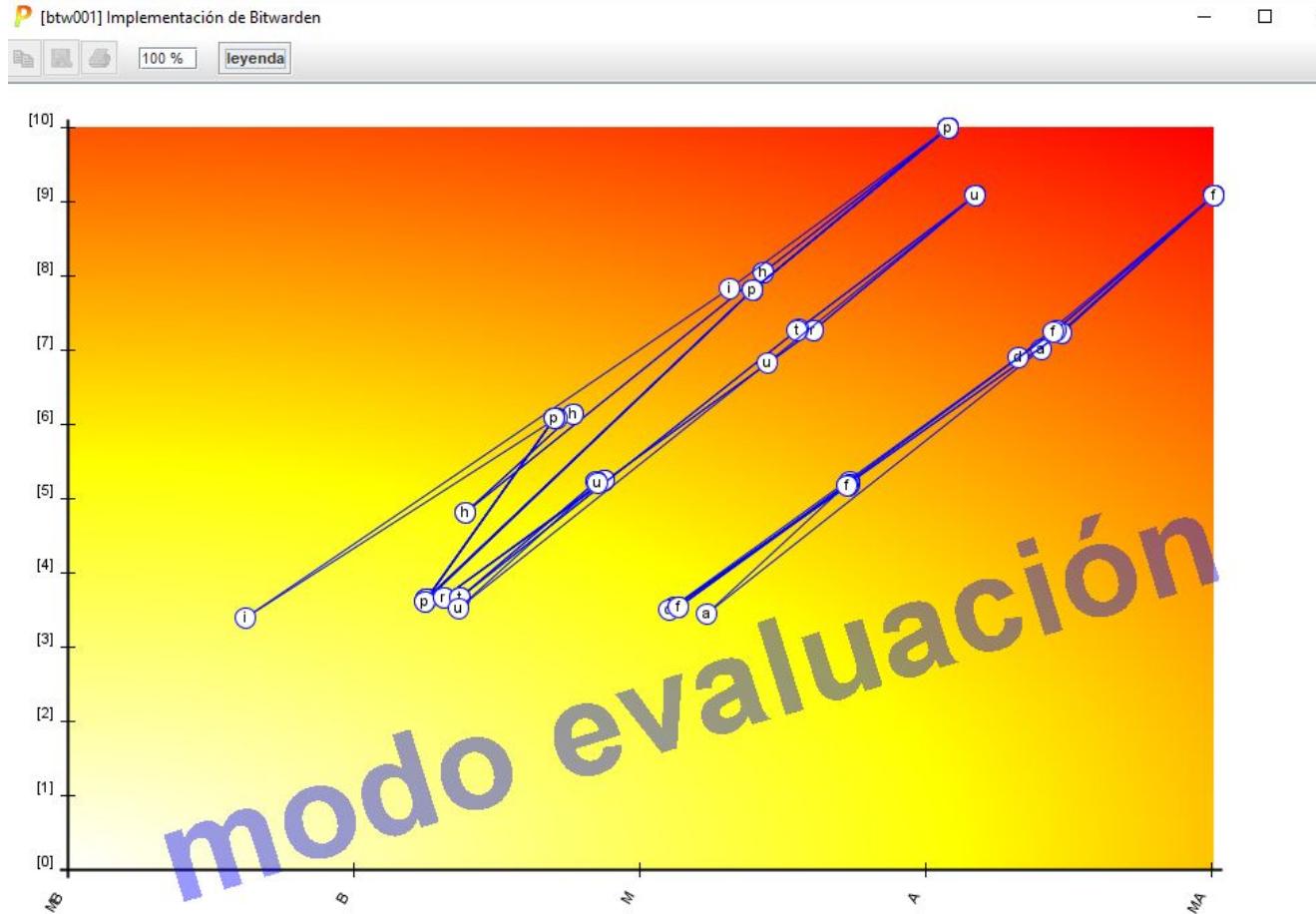
# TOP 10: FASE POTENCIAL

P top 10

Fase: potencial Exportar

	potencial	current	target	PILAR	resumen (impacto)	resumen (riesgo)	D	V	VA	D	I	N	R
	activo				amenaza								
[D.password] credenciales (ej. contra...	[A.11] Acceso no autorizado				[C]			[10]		50%	[9]	MA	{8,1}
[D.e-files] ficheros cifrados	[A.11] Acceso no autorizado				[C]			[10]		50%	[9]	MA	{8,1}
[D.backup] copias de respaldo	[A.11] Acceso no autorizado				[C]			[10]		50%	[9]	MA	{8,1}
[D.files] ficheros de datos	[A.11] Acceso no autorizado				[C]			[10]		50%	[9]	MA	{8,1}
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de...				[I]			[10]		50%	[9]	MA	{8,1}
[keys.info] protección de la información	[A.11] Acceso no autorizado				[C]			[10]		50%	[9]	MA	{8,1}
[L.backup] instalaciones de respaldo	[A.25] Robo de equipos				[C]			[10]		100%	[10]	A	{7,8}
[L.site] recinto	[A.25] Robo de equipos				[C]			[10]		100%	[10]	A	{7,8}
[D.files] ficheros de datos	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[D.auth] datos de validación de creden...	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[D.e-files] ficheros cifrados	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[D.password] credenciales (ej. contra...	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[D.conf] datos de configuración	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[keys.info] protección de la información	[A.5] Suplantación de la identidad				[A]			[10]		100%	[10]	A	{7,8}
[D.e-files] ficheros cifrados	[A.6] Abuso de privilegios de acceso				[C]			[10]		50%	[9]	A	{7,3}
[D.password] credenciales (ej. contra...	[A.6] Abuso de privilegios de acceso				[C]			[10]		50%	[9]	A	{7,3}
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso				[C]			[10]		50%	[9]	A	{7,3}
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso				[C]			[10]		50%	[9]	A	{7,3}
[COM.vpn] canal cifrado (red privada vi...	[A.24] Denegación de servicio				[D]			[10]		50%	[9]	A	{7,3}

# TOP 10: FASE POTENCIAL- MAPA DE CALOR



# TOP 10: FASE CURRENT

P top 10

Fase: potencial Exportar

	potencial	current	target	PILAR	resumen (impacto)	resumen (riesgo)				
	activo	amenaza	D	V	VA	D	I	N	R	
[D.password] credenciales (ej. contra...	[A.11] Acceso no autorizado	[C]		[10]	50%	[7]	A	{6,5}		
[D.e-files] ficheros cifrados	[A.11] Acceso no autorizado	[C]		[10]	50%	[7]	A	{6,5}		
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]		[10]	50%	[7]	A	{6,5}		
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]		[10]	50%	[7]	A	{6,5}		
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de...	[I]		[10]	50%	[7]	A	{6,3}		
[keys.info] protección de la información	[A.11] Acceso no autorizado	[C]		[10]	50%	[7]	A	{6,2}		
[L.backup] instalaciones de respaldo	[A.25] Robo de equipos	[C]		[10]	100%	[8]	M	{6,1}		
[L.site] recinto	[A.25] Robo de equipos	[C]		[10]	100%	[8]	M	{6,1}		
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,9}		
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,9}		
[D.auth] datos de validación de creden...	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,9}		
[D.e-files] ficheros cifrados	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,9}		
[D.password] credenciales (ej. contra...	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,9}		
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,9}		
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,9}		
[D.e-files] ficheros cifrados	[A.6] Abuso de privilegios de acceso	[C]		[10]	50%	[7]	A	{5,8}		
[D.password] credenciales (ej. contra...	[A.6] Abuso de privilegios de acceso	[C]		[10]	50%	[7]	A	{5,8}		
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[A]		[10]	100%	[8]	M	{5,8}		
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso	[C]		[10]	50%	[7]	A	{5,7}		
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso	[C]		[10]	50%	[7]	A	{5,7}		
[COM.vpn] canal cifrado (red privada vi...	[A.24] Denegación de servicio	[D]		[10]	50%	[7]	M	{5,4}		

# TOP 10: FASE TARGET

P top 10

Fase: potencial Exportar

	potencial	current	target	PILAR	resumen (impacto)	resumen (riesgo)				
	activo	amenaza		D	V	VA	D	I	N	R
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de...	[I]		[10]		50%	[3]	M	{3,2}	
[L.backup] instalaciones de respaldo	[A.25] Robo de equipos	[C]		[10]		100%	[5]	B	{3,2}	
[L.site] recinto	[A.25] Robo de equipos	[C]		[10]		100%	[5]	B	{3,2}	
[D.password] credenciales (ej. contra...	[A.11] Acceso no autorizado	[C]		[10]		50%	[4]	M	{3,1}	
[D.e-files] ficheros cifrados	[A.11] Acceso no autorizado	[C]		[10]		50%	[4]	M	{3,1}	
[keys.info] protección de la información	[A.11] Acceso no autorizado	[C]		[10]		50%	[4]	M	{3,1}	
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]		[10]		50%	[4]	M	{3,1}	
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]		[10]		50%	[4]	M	{3,1}	
[D.e-files] ficheros cifrados	[A.6] Abuso de privilegios de acceso	[C]		[10]		50%	[4]	B	{2,5}	
[D.password] credenciales (ej. contra...	[A.6] Abuso de privilegios de acceso	[C]		[10]		50%	[4]	B	{2,5}	
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso	[C]		[10]		50%	[4]	B	{2,5}	
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso	[C]		[10]		50%	[4]	B	{2,5}	
[COM.vpn] canal cifrado (red privada vi...	[A.24] Denegación de servicio	[D]		[10]		50%	[4]	B	{2,5}	
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]		[10]		100%	[4]	B	{2,4}	
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]		[10]		100%	[4]	B	{2,4}	
[D.auth] datos de validación de creden...	[A.5] Suplantación de la identidad	[A]		[10]		100%	[4]	B	{2,4}	
[D.e-files] ficheros cifrados	[A.5] Suplantación de la identidad	[A]		[10]		100%	[4]	B	{2,4}	
[D.password] credenciales (ej. contra...	[A.5] Suplantación de la identidad	[A]		[10]		100%	[4]	B	{2,4}	
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]		[10]		100%	[4]	B	{2,4}	
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad	[A]		[10]		100%	[4]	B	{2,4}	
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[A]		[10]		100%	[3]	B	{1,7}	

# TOP 10: FASE PILAR

P top 10



Fase: potencial Exportar

potencial	current	target	PILAR	resumen (impacto)	resumen (riesgo)	D	V	VA	D	I	N	R
			activo	amenaza								
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de...			[I]			[10]		50%	[5]	A	{4,7}
[D.password] credenciales (ej. contra...	[A.11] Acceso no autorizado			[C]			[10]		50%	[5]	A	{4,7}
[D.e-files] ficheros cifrados	[A.11] Acceso no autorizado			[C]			[10]		50%	[5]	A	{4,7}
[keys.info] protección de la información	[A.11] Acceso no autorizado			[C]			[10]		50%	[5]	A	{4,6}
[D.backup] copias de respaldo	[A.11] Acceso no autorizado			[C]			[10]		50%	[5]	A	{4,6}
[D.files] ficheros de datos	[A.11] Acceso no autorizado			[C]			[10]		50%	[5]	A	{4,6}
[L.backup] instalaciones de respaldo	[A.25] Robo de equipos			[C]			[10]		100%	[6]	M	{4,4}
[L.site] recinto	[A.25] Robo de equipos			[C]			[10]		100%	[6]	M	{4,4}
[keys.info] protección de la información	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.files] ficheros de datos	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.auth] datos de validación de creden...	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.e-files] ficheros cifrados	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.password] credenciales (ej. contra...	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.conf] datos de configuración	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad			[A]			[10]		100%	[6]	M	{4,3}
[D.e-files] ficheros cifrados	[A.6] Abuso de privilegios de acceso			[C]			[10]		50%	[5]	M	{3,9}
[D.password] credenciales (ej. contra...	[A.6] Abuso de privilegios de acceso			[C]			[10]		50%	[5]	M	{3,9}
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso			[C]			[10]		50%	[5]	M	{3,9}
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso			[C]			[10]		50%	[5]	M	{3,9}
[COMvpn] canal cifrado (red privada vi...	[A.24] Denegación de servicio			[D]			[10]		50%	[5]	M	{3,9}

# TOP 10: FASE RESUMEN(IMPACTO)

P top 10

Fase: potencial Exportar

	potencial	current	target	PILAR	resumen (impacto)	resumen (riesgo)			
	activo	amenaza	dimensión	impacto	current	target			PILAR
[L.backup]	instalaciones de respaldo	[A.25] Robo de equipos	[C]	[10]	[8]	[5]			[6]
[L.site]	recinto	[A.25] Robo de equipos	[C]	[10]	[8]	[5]			[6]
[keys.info]	protección de la información	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[3]			[6]
[D.files]	ficheros de datos	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[4]			[6]
[D.backup]	copias de respaldo	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[4]			[6]
[D.auth]	datos de validación de credenciales	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[4]			[6]
[D.e-files]	ficheros cifrados	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[4]			[6]
[D.password]	credenciales (ej. contraseñas)	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[4]			[6]
[D.conf]	datos de configuración	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[4]			[6]
[D.log]	registro de actividad (log)	[A.5] Suplantación de la identidad	[A]	[10]	[8]	[4]			[6]
[D.log]	registro de actividad (log)	[A.3] Manipulación de los registros de acti...	[I]	[9]	[7]	[3]			[5]
[D.password]	credenciales (ej. contraseñas)	[A.11] Acceso no autorizado	[C]	[9]	[7]	[4]			[5]
[D.e-files]	ficheros cifrados	[A.11] Acceso no autorizado	[C]	[9]	[7]	[4]			[5]
[keys.info]	protección de la información	[A.11] Acceso no autorizado	[C]	[9]	[7]	[4]			[5]
[D.backup]	copias de respaldo	[A.11] Acceso no autorizado	[C]	[9]	[7]	[4]			[5]
[D.files]	ficheros de datos	[A.11] Acceso no autorizado	[C]	[9]	[7]	[4]			[5]
[D.e-files]	ficheros cifrados	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[4]			[5]
[D.password]	credenciales (ej. contraseñas)	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[4]			[5]
[D.backup]	copias de respaldo	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[4]			[5]
[D.files]	ficheros de datos	[A.6] Abuso de privilegios de acceso	[C]	[9]	[7]	[4]			[5]
[COM.vpn]	canal cifrado (red privada virtual)	[A.24] Denegación de servicio	[D]	[9]	[7]	[4]			[5]

# TOP 10: FASE RESUMEN(RIESGO)

P top 10

Fase: potencial Exportar

	potencial	current	target	PILAR	resumen (impacto)	resumen (riesgo)			
	activo	amenaza	dimensión	riesgo	current	target			PILAR
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de acti...	[I]	{8,1}	{6,3}	{3,2}	{4,7}			
[D.password] credenciales (ej. contraseñas)	[A.11] Acceso no autorizado	[C]	{8,1}	{6,5}	{3,1}	{4,7}			
[D.e-files] ficheros cifrados	[A.11] Acceso no autorizado	[C]	{8,1}	{6,5}	{3,1}	{4,7}			
[keys.info] protección de la información	[A.11] Acceso no autorizado	[C]	{8,1}	{6,2}	{3,1}	{4,6}			
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]	{8,1}	{6,5}	{3,1}	{4,6}			
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]	{8,1}	{6,5}	{3,1}	{4,6}			
[L.backup] instalaciones de respaldo	[A.25] Robo de equipos	[C]	{7,8}	{6,1}	{3,2}	{4,4}			
[L.site] recinto	[A.25] Robo de equipos	[C]	{7,8}	{6,1}	{3,2}	{4,4}			
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,8}	{1,7}	{4,3}			
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,9}	{2,4}	{4,3}			
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,9}	{2,4}	{4,3}			
[D.auth] datos de validación de credenciales	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,9}	{2,4}	{4,3}			
[D.e-files] ficheros cifrados	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,9}	{2,4}	{4,3}			
[D.password] credenciales (ej. contraseñas)	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,9}	{2,4}	{4,3}			
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,9}	{2,4}	{4,3}			
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad	[A]	{7,8}	{5,9}	{2,4}	{4,3}			
[D.e-files] ficheros cifrados	[A.6] Abuso de privilegios de acceso	[C]	{7,3}	{5,8}	{2,5}	{3,9}			
[D.password] credenciales (ej. contraseñas)	[A.6] Abuso de privilegios de acceso	[C]	{7,3}	{5,8}	{2,5}	{3,9}			
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso	[C]	{7,3}	{5,7}	{2,5}	{3,9}			
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso	[C]	{7,3}	{5,7}	{2,5}	{3,9}			
[COMvpn] canal cifrado (red privada virtual)	[A.24] Denegación de servicio	[D]	{7,3}	{5,4}	{2,5}	{3,9}			



P sugiere

aspe...	tdp	reco...	nivel	salvaguarda	dud...	aplica	com...	curr...	enige	PILA
				SALVAGUARDAS						
G	EL	9		•  [IA] Identificación y autenticación					_L3	_L5 L2-L3
T	EL	7		•  [AC] Control de acceso lógico					_L2	_L5 L2-L3
G	PR	9		•  [D] Protección de la Información					_L3	_L5 L2-L3
G	EL	5		•  [K] Protección de claves criptográficas [SC-12]					_L2-L3	n.a.
G	PR	5		•  [S] Protección de los Servicios					_L3	_L5 L2-L3
G	PR	5		•  [SW] Protección de las Aplicaciones Informáticas (SW)					_L3	_L5 n.a.
G	PR	5		•  [HW] Protección de los Equipos Informáticos (HW)					_L3	_L5 L2-L3
G	PR	8		•  [COM] Protección de las Comunicaciones					_L3	_L5 L2-L3
G	PR	5		•  [M] Protección de los Soportes de Información					L1-L3	L3-L5 n.a.
G	PR	5		•  [AUX] Elementos Auxiliares					_L2	_L4 L2-L3
F	EL	5		•  [PPE] Protección física de los equipos					L0	L4 L3
F	PR	5		•  [L] Protección de las Instalaciones					_L2	_L4 L2-L3
P	PR	6		•  [P] Gestión del Personal					_L3	_L5 L2-L3
G	CR	6		•  [IM] Gestión de incidentes					_L2	_L4 L2-L3
T	PR	6		•  [tools] Herramientas de seguridad					_L2	_L4 L2-L3
G	CR			•  [V] Gestión de vulnerabilidades					L2	L4-L5 n.a.
T	MN	4		•  [A] Registro y auditoría					_L3	_L5 L2-L3
G	RC	3		•  [BC] Continuidad del negocio					L2	L3-L4 L2-L3
G	AD	5		•  [G] Organización					_L3	_L5 L2-L3
G	AD	5		•  [E] Relaciones Externas					L2-L3	L4-L5 L2-L3
G	AD	5		•  [NEW] Adquisición / desarrollo					_L3	_L5 L2-L3
G	PR			•  [PDS] Servicios potencialmente peligrosos					L1-L3	L3-L5 n.a.
G	PR			•  [IP] Sistema de protección de frontera lógica					L3	L5 n.a.
F	EL			•  [PPS] Protección del perímetro físico					_L2	_L3 n.a.
G	EL	1 (o)		•  [TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]						L2
T	PR	7		•  [ACB] ACCESS CONTROL [AC, ACB]						L2-L3
P	AW	2		•  [AT] AWARENESS AND TRAINING						L2
G	MN	3		•  [AU] AUDIT AND ACCOUNTABILITY						L2-L3
G	PR	3		•  [CA] ASSESSMENT, AUTHORIZATION, AND MONITORING						L3
G	PR	3		•  [CM] CONFIGURATION MANAGEMENT						L2-L3
G	PR	4		•  [CP] CONTINGENCY PLANNING						L3
T	EL	9		•  [Iab] IDENTIFICATION AND AUTHENTICATION [IA, Iab]						L3-L4
G	CR	4		•  [IR] INCIDENT RESPONSE						L2-L3
T	PR	3		•  [MA] MAINTENANCE						L3
T	PR			•  [MP] MEDIA PROTECTION						n.a.
F	PR	4		•  [PE] PHYSICAL AND ENVIRONMENTAL PROTECTION						L3
G	AD	2		•  [PL] PLANNING						L2
G	AD	2		•  [PM] PROGRAM MANAGEMENT						L2
P	PR	3		•  [PS] PERSONNEL SECURITY						L3
P	PR	3		•  [PT] PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY						L3
G	AD	2		•  [RA] RISK ASSESSMENT						L2
G	AD	2		•  [SA] SYSTEM AND SERVICES ACQUISITION						L2
T	PR	5		•  [SC] SYSTEM AND COMMUNICATIONS PROTECTION						L2-L3
T	PR	3		•  [SI] Protección de los soportes de información						L2-L3
G	PR	4		•  [SR] SUPPLY CHAIN RISK MANAGEMENT						L3

# Nuestro Equipo



**Jhonathan Pauca**

Me dedico a innovar soluciones que generen valor a través de liderar proyectos y emprendimientos comercialmente viables y que contribuyen al bienestar social y al desarrollo sostenible.



**Melissa Rodriguez**

Me dedico a analizar y desarrollar soluciones que le den valor a las áreas de negocio.



**Heber Hualpa**

Me dedico a soluciones de infraestructura



**Sihomara Ochoa**

Desarrolladora full stack especializada en soluciones digitales y análisis de datos para la industria y la minería.



**Ronald Ticona**

Senior de Proyectos  
Mine to Mill |  
Fragmentación &  
cominución |  
ML/Modelado predictivo  
(Python/R) + analítica  
tiempo real (PI System,  
Power BI) | ↑throughput,  
↓variabilidad y costos |  
Impactos 5–27 MUSD |  
+10 años Perú