ANEJO 02: CUMPLIMIENTO ISO/IEC 27002

Cumplimiento ISO/IEC 27002:2013

[GIM] Gimnasio

23.6.2019

Introducción

Código: GIM

Nombre: Gimnasio

Datos administrativos:

- Descripción: GIMNASIO XXX
- Fecha: 1.06.2019

Dominios de seguridad

[base] red corporativa

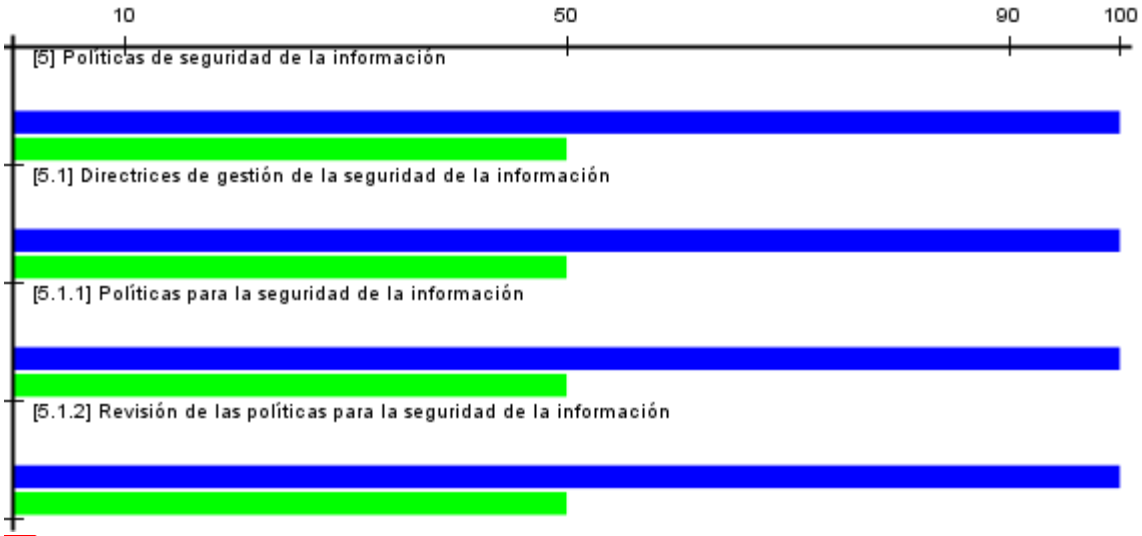
- clase: [ENS] sujeto al ENS

Controles

Niveles de madurez

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

[5] Políticas de seguridad



[current] situación actual

[target] situación objetivo

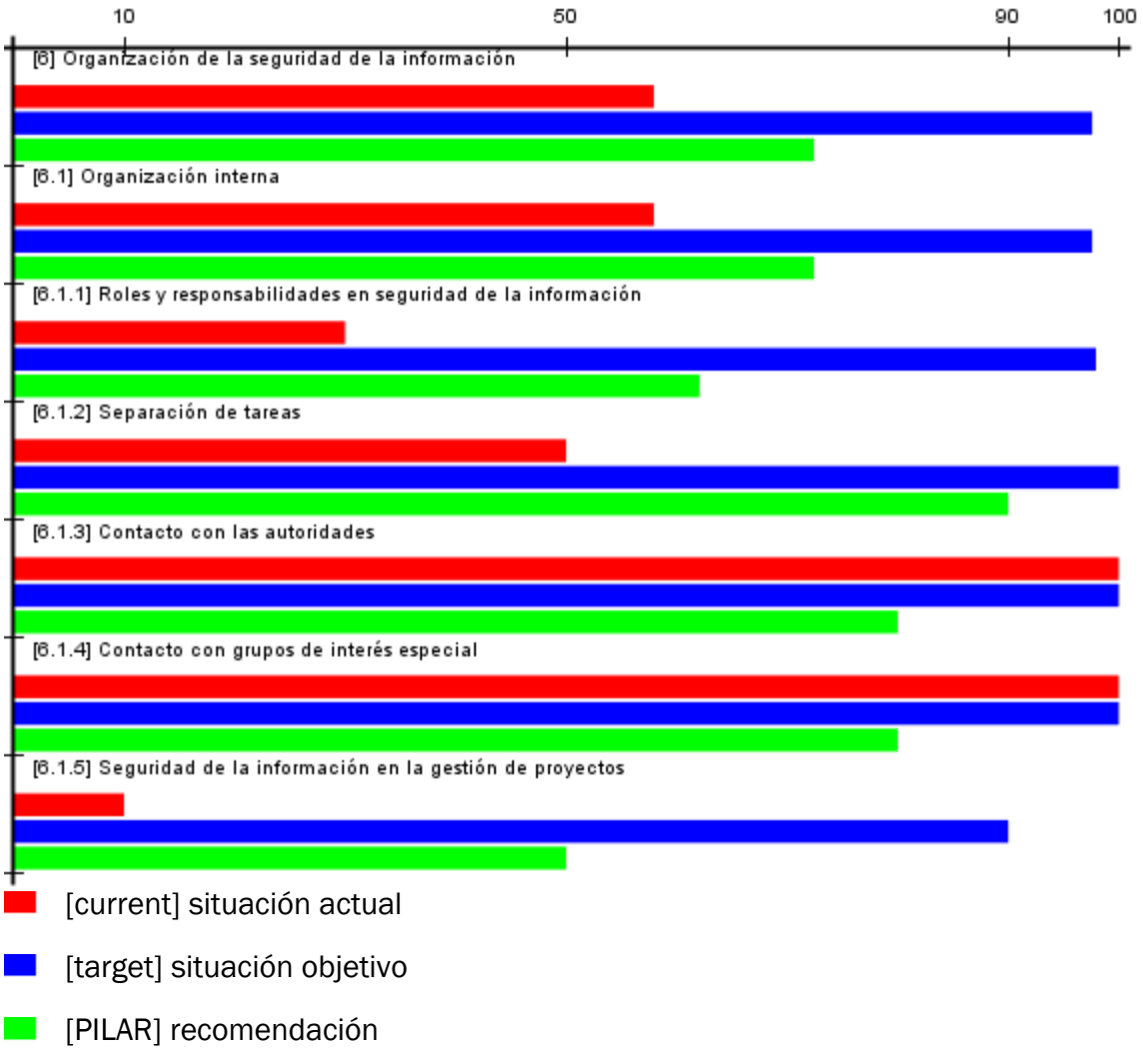
[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[5] Políticas de seguridad de la información	sí	L0	L5	L2
[5.1] Directrices de gestión de la seguridad de la información	sí	L0	L5	L2

[5.1.1] Políticas para la seguridad de la información	sí	L0	L5	L2
[5.1.2] Revisión de las políticas para la seguridad de la información	sí	L0	L5	L2

[6] Organización de la seguridad de la información



dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR

[6] Organización de la seguridad de la información	sí	L0-L5	L4-L5	L2-L4
[6.1] Organización interna	sí	L0-L5	L4-L5	L2-L4
[6.1.1] Roles y responsabilidades en seguridad de la información	sí	L0-L5	L4-L5	L2-L3
[6.1.2] Separación de tareas	sí	L2	L5	L4
[6.1.3] Contacto con las autoridades	sí	L5	L5	L3
[6.1.4] Contacto con grupos de interés especial	sí	L5	L5	L3
[6.1.5] Seguridad de la información en la gestión de proyectos	sí	L1	L4	L2
[6.2] Los dispositivos móviles y el teletrabajo	n.a.	n.a.	n.a.	n.a.

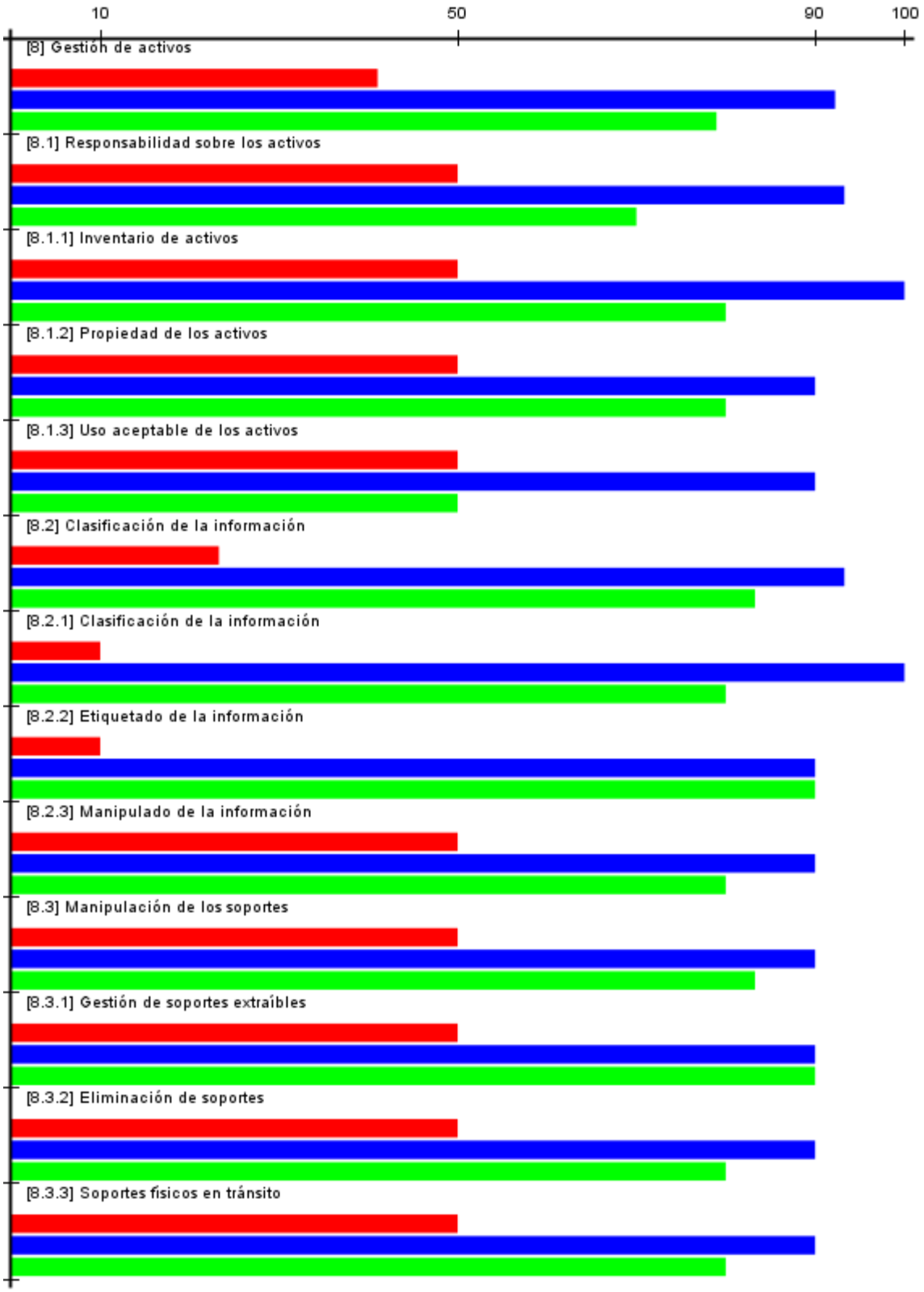
[7] Seguridad relativa a los recursos humanos

- [current] situación actual
- [target] situación objetivo
- [PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[7] Seguridad relativa a los recursos humanos	n.a.	n.a.	n.a.	n.a.

[8] Gestión de activos

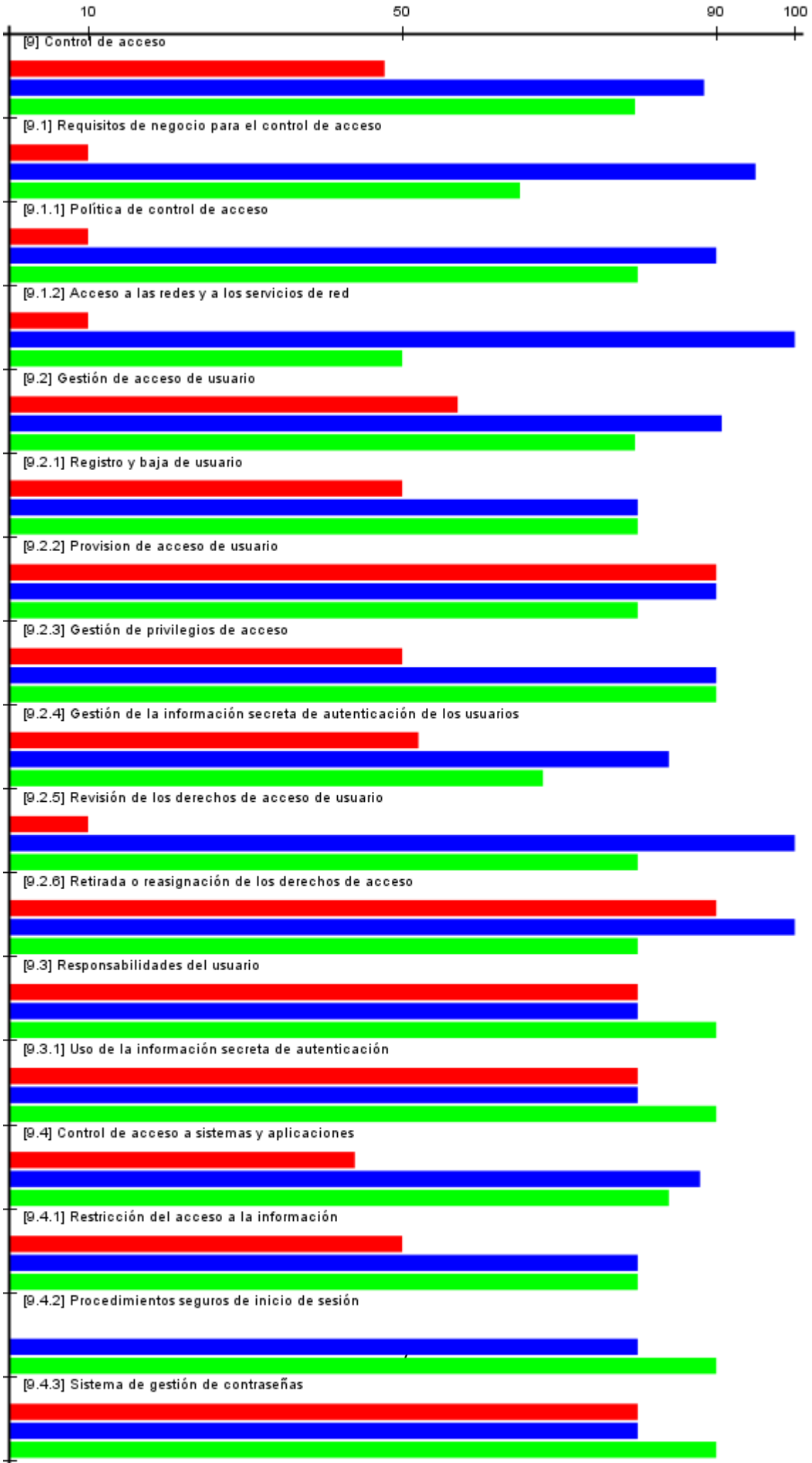

10
50
90
100
[8] Gestión de activos
[8.1] Responsabilidad sobre los activos
[8.1.1] Inventario de activos
[8.1.2] Propiedad de los activos
[8.1.3] Uso aceptable de los activos
[8.2] Clasificación de la información
[8.2.1] Clasificación de la información
[8.2.2] Etiquetado de la información
[8.2.3] Manipulado de la información
[8.3] Manipulación de los soportes
[8.3.1] Gestión de soportes extraíbles
[8.3.2] Eliminación de soportes
[8.3.3] Soportes físicos en tránsito
[current] situación actual
[target] situación objetivo
[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[8] Gestión de activos	sí	L1-L2	L4-L5	L2-L4
[8.1] Responsabilidad sobre los activos	sí	L2	L4-L5	L2-L3
[8.1.1] Inventario de activos	sí	L2	L5	L3
[8.1.2] Propiedad de los activos	sí	L2	L4	L3
[8.1.3] Uso aceptable de los activos	sí	L2	L4	L2
[8.1.4] Devolución de activos	n.a.	n.a.	n.a.	n.a.
[8.2] Clasificación de la información	sí	L1-L2	L4-L5	L3-L4
[8.2.1] Clasificación de la información	sí	L1	L5	L3
[8.2.2] Etiquetado de la información	sí	L1	L4	L4
[8.2.3] Manipulado de la información	sí	L2	L4	L3
[8.3] Manipulación de los soportes	sí	L2	L4	L3-L4
[8.3.1] Gestión de soportes extraíbles	sí	L2	L4	L4
[8.3.2] Eliminación de soportes	sí	L2	L4	L3
[8.3.3] Soportes físicos en tránsito	sí	L2	L4	L3

[9] Control de acceso

CUMPLIMIENTO ISO/IEC 27002



[current] situación actual

[target] situación objetivo

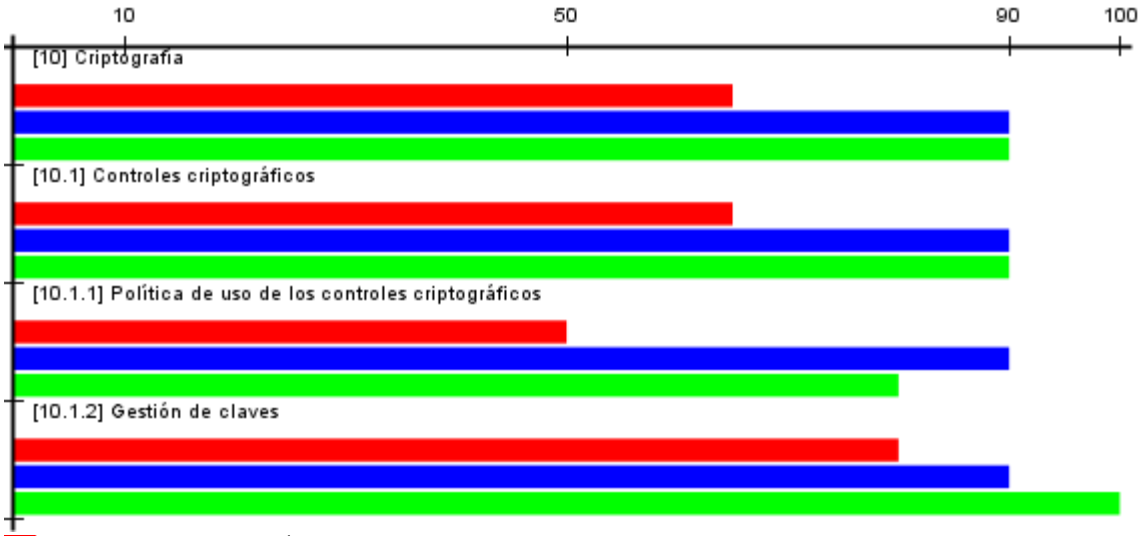
[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[9] Control de acceso	sí	L0-L4	L3-L5	L2-L4
[9.1] Requisitos de negocio para el control de acceso	sí	L1	L4-L5	L2-L3
[9.1.1] Política de control de acceso	sí	L1	L4	L3
[9.1.2] Acceso a las redes y a los servicios de red	sí	L1	L5	L2
[9.2] Gestión de acceso de usuario	sí	L0-L4	L3-L5	L2-L4
[9.2.1] Registro y baja de usuario	sí	L2	L3	L3
[9.2.2] Provision de acceso de usuario	sí	L4	L4	L3
[9.2.3] Gestión de privilegios de acceso	sí	L2	L4	L4
[9.2.4] Gestión de la información secreta de autenticación de los usuarios	sí	L0-L3	L3-L5	L2-L3
[9.2.5] Revisión de los derechos de acceso de usuario	sí	L1	L5	L3
[9.2.6] Retirada o reasignación de los derechos de acceso	sí	L4	L5	L3
[9.3] Responsabilidades del usuario	sí	L3	L3	L4
[9.3.1] Uso de la información secreta de autenticación	sí	L3	L3	L4
[9.4] Control de acceso a sistemas y aplicaciones	sí	L0-L3	L3-L5	L3-L4
[9.4.1] Restricción del acceso a la información	sí	L2	L3	L3
[9.4.2] Procedimientos seguros de inicio de sesión	sí	L0	L3	L4
[9.4.3] Sistema de gestión de contraseñas	sí	L3	L3	L4
[9.4.4] Uso de utilidades con privilegios del sistema	sí	L3	L5	L3

[9.4.5] Control de acceso al código fuente de los programas	sí	L1	L5	L3

[10] Criptografía



[current] situación actual

[target] situación objetivo

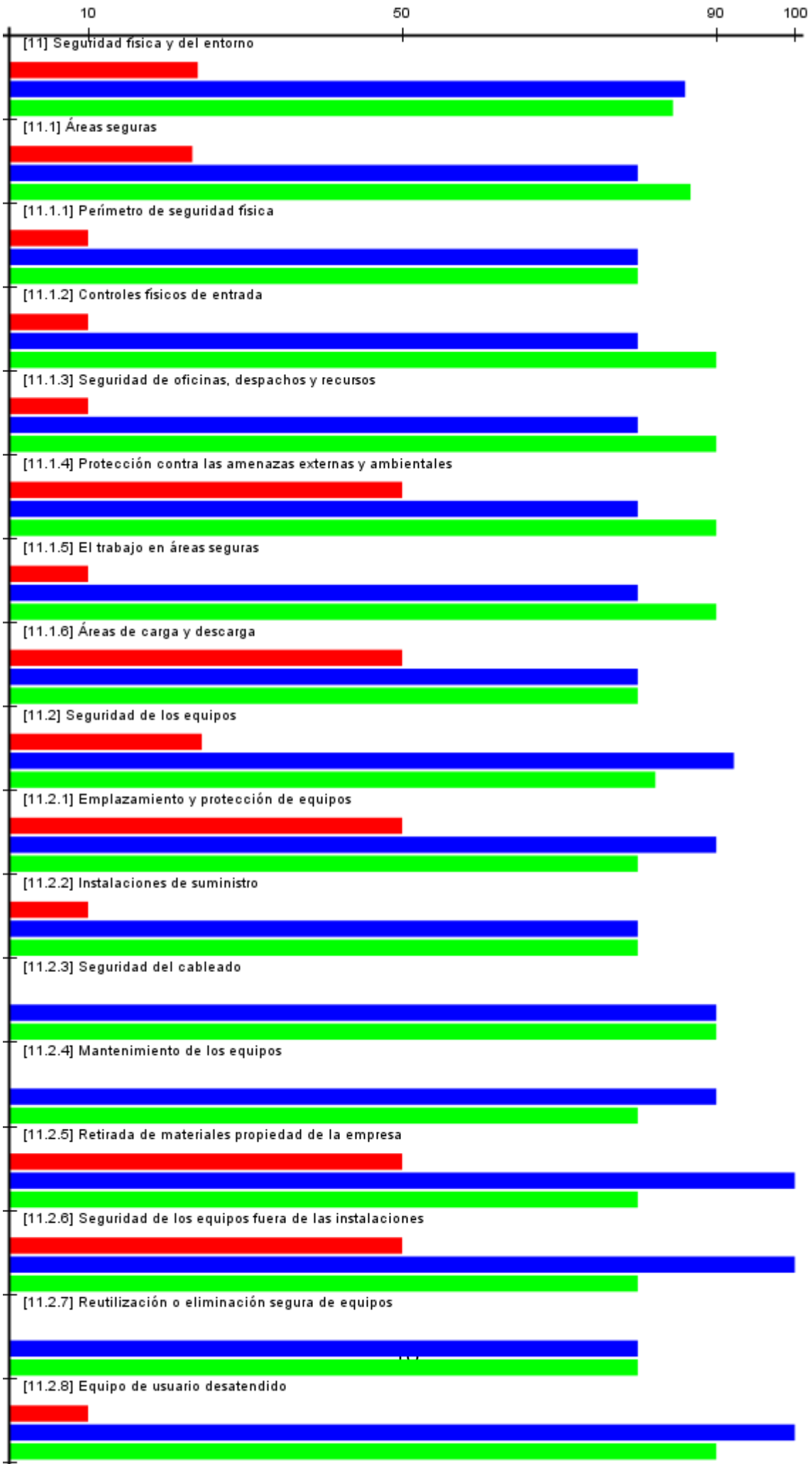
[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[10] Criptografía	sí	L2-L3	L4	L3-L5
[10.1] Controles criptográficos	sí	L2-L3	L4	L3-L5
[10.1.1] Política de uso de los controles criptográficos	sí	L2	L4	L3
[10.1.2] Gestión de claves	sí	L3	L4	L5

[11] Seguridad física y del entorno

CUMPLIMIENTO ISO/IEC 27002



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[11] Seguridad física y del entorno	sí	L0-L2	L3-L5	L3-L4
[11.1] Áreas seguras	sí	L1-L2	L3	L3-L4
[11.1.1] Perímetro de seguridad física	sí	L1	L3	L3
[11.1.2] Controles físicos de entrada	sí	L1	L3	L4
[11.1.3] Seguridad de oficinas, despachos y recursos	sí	L1	L3	L4
[11.1.4] Protección contra las amenazas externas y ambientales	sí	L2	L3	L4
[11.1.5] El trabajo en áreas seguras	sí	L1	L3	L4
[11.1.6] Áreas de carga y descarga	sí	L2	L3	L3
[11.2] Seguridad de los equipos	sí	L0-L2	L3-L5	L3-L4
[11.2.1] Emplazamiento y protección de equipos	sí	L2	L4	L3
[11.2.2] Instalaciones de suministro	sí	L1	L3	L3
[11.2.3] Seguridad del cableado	sí	L0	L4	L4
[11.2.4] Mantenimiento de los equipos	sí	L0	L4	L3
[11.2.5] Retirada de materiales propiedad de la empresa	sí	L2	L5	L3
[11.2.6] Seguridad de los equipos fuera de las instalaciones	sí	L2	L5	L3
[11.2.7] Reutilización o eliminación segura de equipos	sí	L0	L3	L3
[11.2.8] Equipo de usuario desatendido	sí	L1	L5	L4
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia	sí	L2	L5	L3

[12] Seguridad de las operaciones

CUMPLIMIENTO ISO/IEC 27002

[current] situación actual

[target] situación objetivo

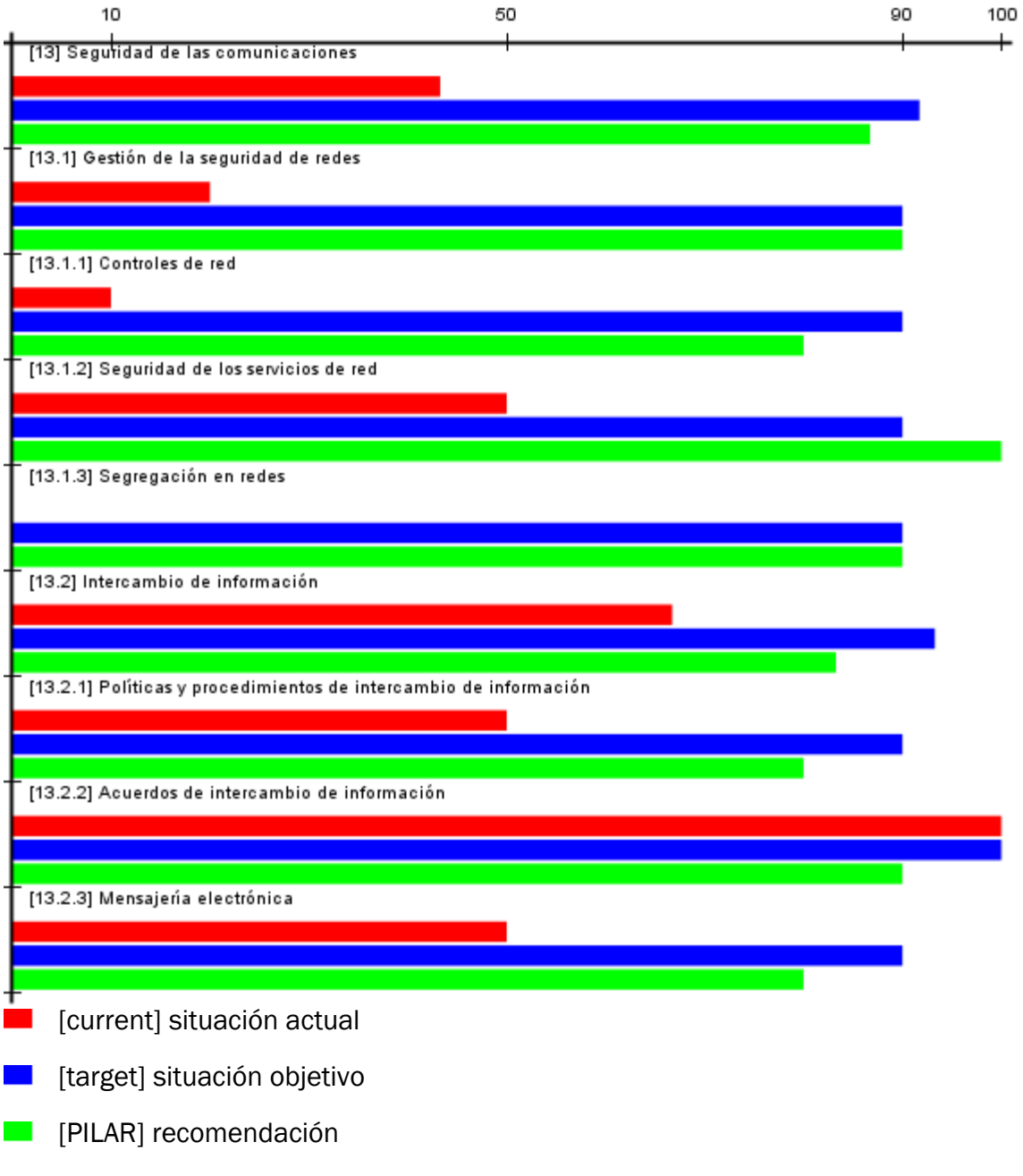
[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[12] Seguridad de las operaciones	sí	L0-L5	L3-L5	L2-L5
[12.1] Procedimientos y responsabilidades operacionales	sí	L0-L2	L3-L5	L2-L3
[12.1.1] Documentación de los procedimientos de operación	sí	L0-L2	L3-L4	L2-L3
[12.1.2] Gestión de cambios	sí	L2	L5	L3
[12.1.3] Gestión de capacidades	sí	L1	L3	L3
[12.1.4] Separación de los recursos de desarrollo, prueba y operación	sí	L1	L5	L3
[12.2] Protección contra el software malicioso (malware)	sí	L3	L3	L5
[12.2.1] Controles contra el código malicioso	sí	L3	L3	L5
[12.3] Copias de seguridad	sí	L3	L5	L5
[12.3.1] Copias de seguridad de la información	sí	L3	L5	L5
[12.4] Registros y supervisión	sí	L2-L5	L5	L2-L4
[12.4.1] Registro de eventos	sí	L3	L5	L3
[12.4.2] Protección de la información de registro	sí	L2	L5	L3
[12.4.3] Registros de administración y operación	sí	L5	L5	L2
[12.4.4] Sincronización del reloj	sí	L5	L5	L4
[12.5] Control del software en explotación	sí	L1	L5	L4
[12.5.1] Instalación del software en explotación	sí	L1	L5	L4
[12.6] Gestión de la vulnerabilidad técnica	sí	L1	L5	L3-L4
[12.6.1] Gestión de las vulnerabilidades técnicas	sí	L1	L5	L4

[12.6.2] Restricción en la instalación de software	sí	L1	L5	L3
[12.7] Consideraciones sore la auditoría de sistemas de información	sí	L1	L3	L3
[12.7.1] Controles de auditoría de sistemas de información	sí	L1	L3	L3

[13] Seguridad de las comunicaciones



dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[13] Seguridad de las comunicaciones	sí	L0-L5	L4-L5	L3-L5
[13.1] Gestión de la seguridad de redes	sí	L0-L2	L4	L3-L5
[13.1.1] Controles de red	sí	L1	L4	L3
[13.1.2] Seguridad de los servicios de red	sí	L2	L4	L5
[13.1.3] Segregación en redes	sí	L0	L4	L4
[13.2] Intercambio de información	sí	L2-L5	L4-L5	L3-L4
[13.2.1] Políticas y procedimientos de intercambio de información	sí	L2	L4	L3
[13.2.2] Acuerdos de intercambio de información	sí	L5	L5	L4
[13.2.3] Mensajería electrónica	sí	L2	L4	L3
[13.2.4] Acuerdos de confidencialidad o no revelación	n.a.	n.a.	n.a.	n.a.

[14] Adquisición, desarrollo y mantenimiento de sistemas de información

CUMPLIMIENTO ISO/IEC 27002

[current] situación actual

[target] situación objetivo

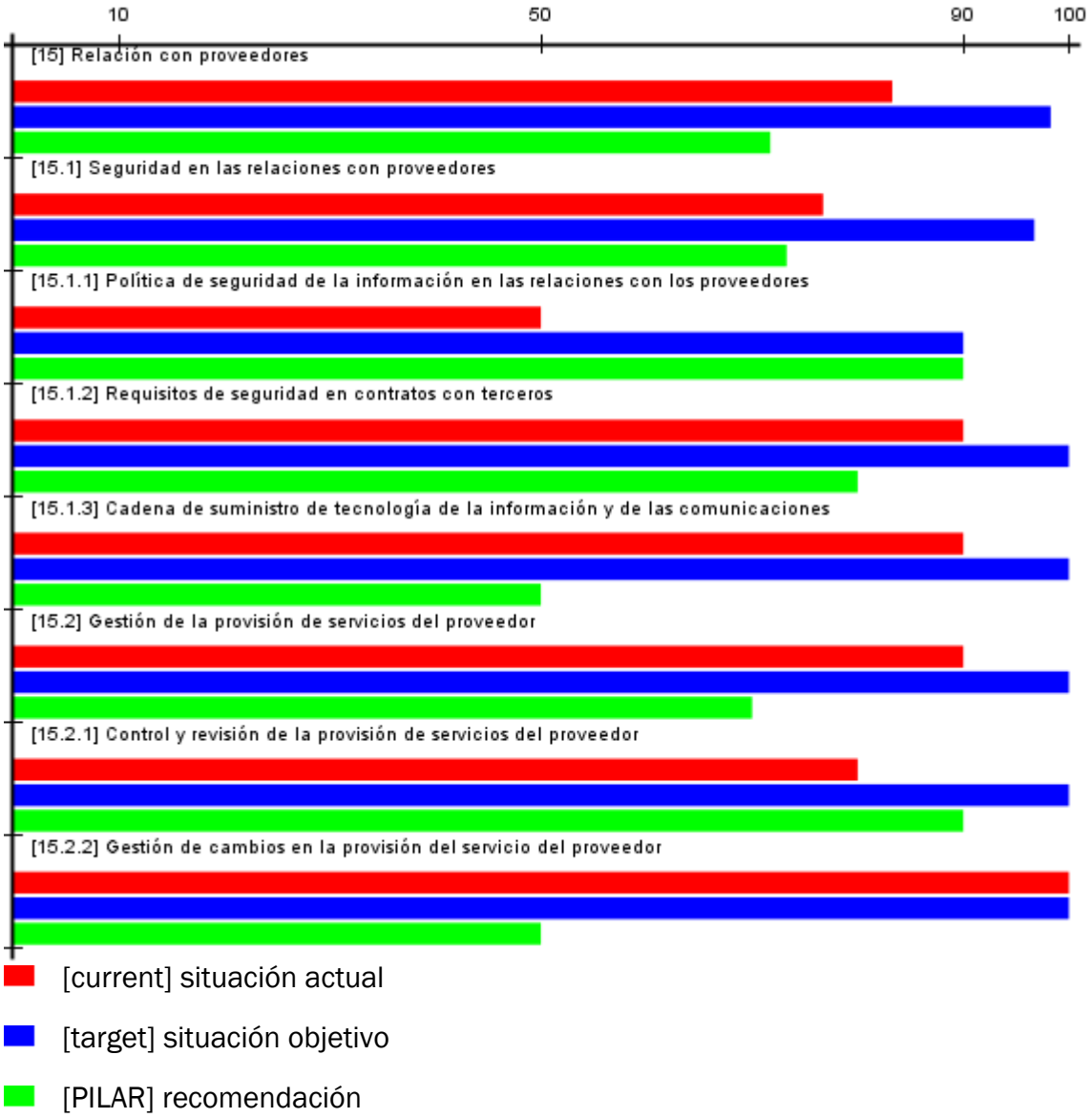
[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	sí	L0-L3	L4-L5	L2-L4
[14.1] Requisitos de seguridad en sistemas de información	sí	L0-L3	L4-L5	L3-L4
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información	sí	L0-L2	L5	L3
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas	sí	L3	L4	L3
[14.1.3] Protección de las transacciones de servicios de aplicaciones	sí	L3	L4	L4
[14.2] Seguridad en el desarrollo y en los procesos de soporte	sí	L0-L3	L5	L2-L3
[14.2.1] Política de desarrollo seguro	sí	L1	L5	L3
[14.2.2] Procedimiento de control de cambios en sistemas	sí	L3	L5	L3
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	sí	L2	L5	L3
[14.2.4] Restricciones a los cambios en los paquetes de software	sí	L2	L5	L2
[14.2.5] Principios de ingeniería de sistemas seguros	sí	L2	L5	L3
[14.2.6] Entorno de desarrollo seguro	sí	L1	L5	L3
[14.2.7] Externalización del desarrollo de software	sí	L1	L5	L3
[14.2.8] Pruebas funcionales de seguridad de sistemas	sí	L1	L5	L3

[14.2.9] Pruebas de aceptación de sistemas	sí	L0	L5	L3
[14.3] Datos de prueba	sí	L1	L5	L3
[14.3.1] Protección de los datos de prueba	sí	L1	L5	L3

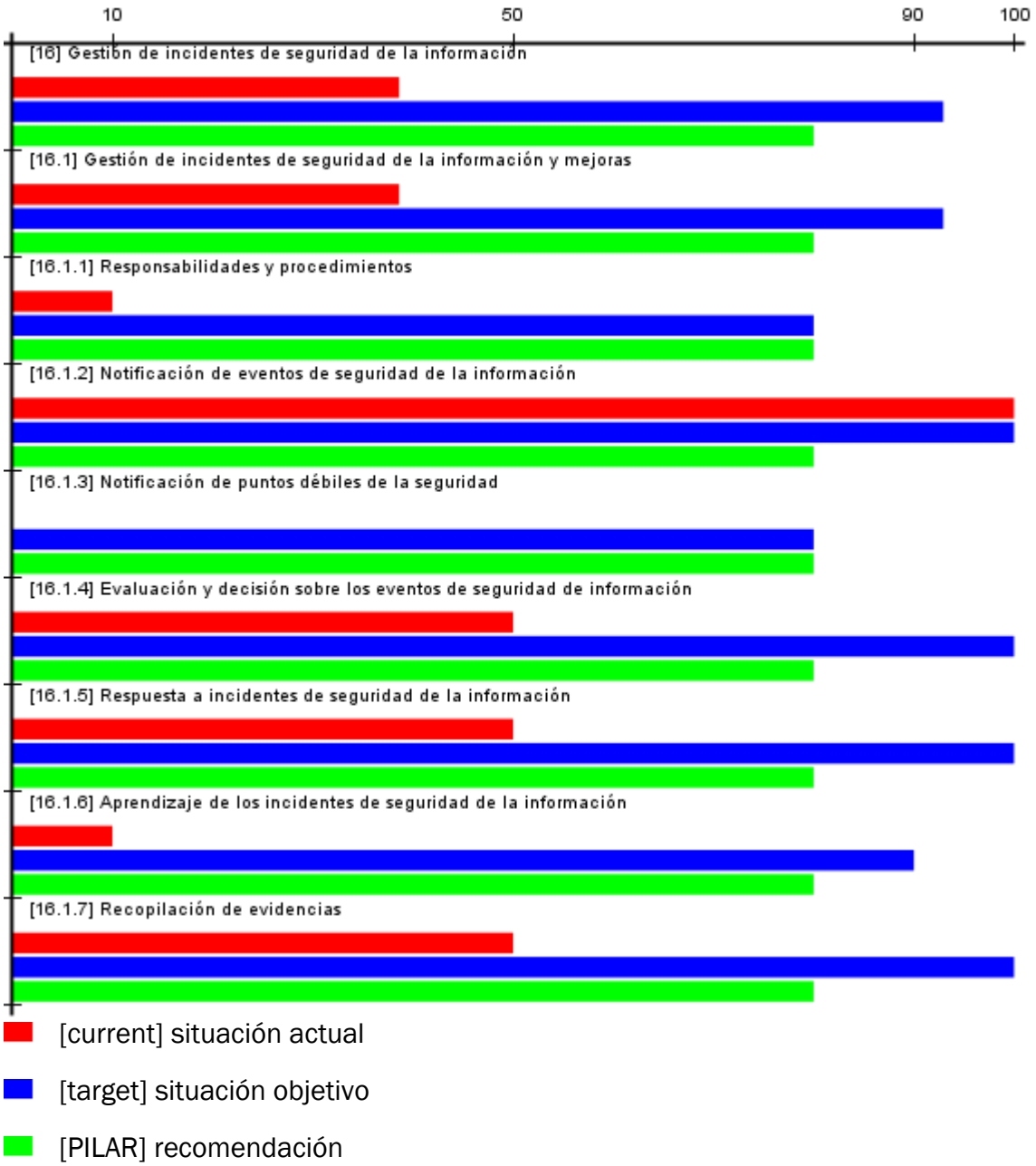
[15] Relación con proveedores



dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[15] Relación con proveedores	sí	L2-L5	L4-L5	L2-L4
[15.1] Seguridad en las relaciones con proveedores	sí	L2-L4	L4-L5	L2-L4
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores	sí	L2	L4	L4
[15.1.2] Requisitos de seguridad en contratos con terceros	sí	L4	L5	L3
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones	sí	L4	L5	L2
[15.2] Gestión de la provisión de servicios del proveedor	sí	L3-L5	L5	L2-L4
[15.2.1] Control y revisión de la provisión de servicios del proveedor	sí	L3	L5	L4
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor	sí	L5	L5	L2

[16] Gestión de incidentes de seguridad de la información

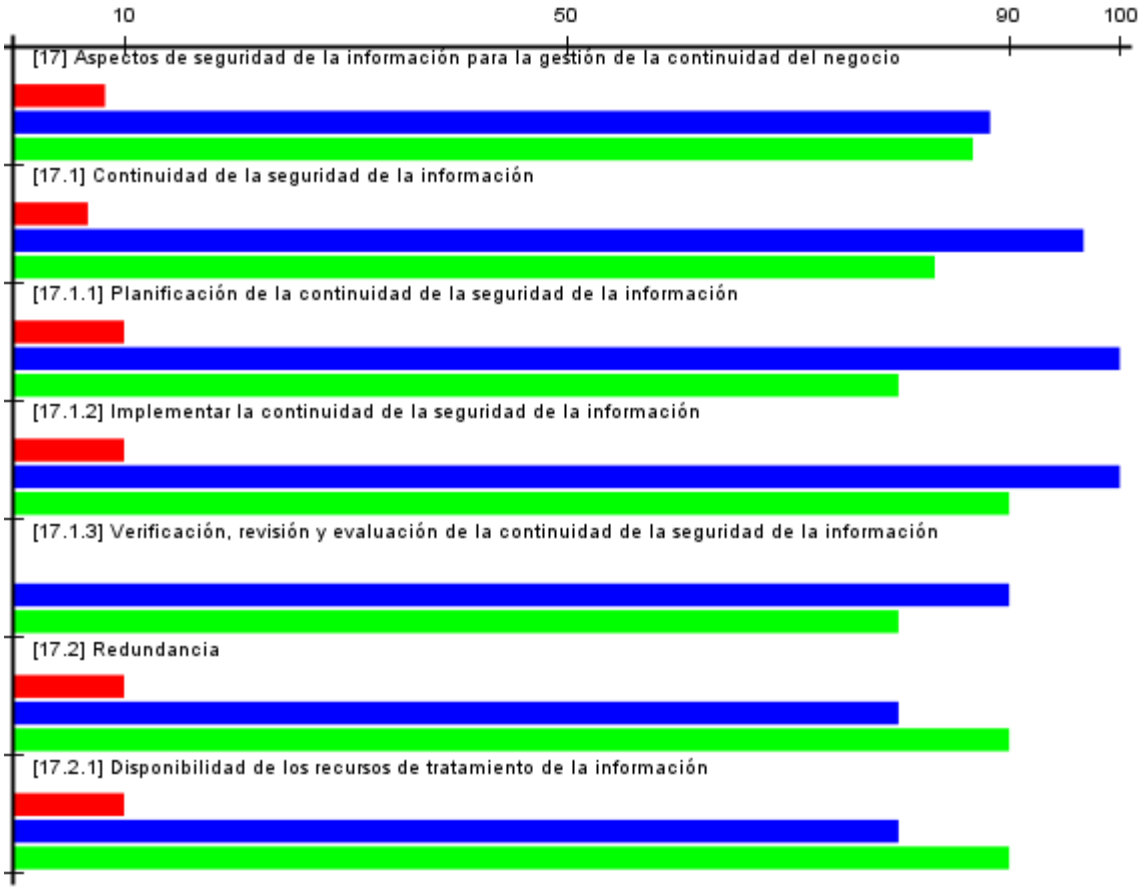


dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[16] Gestión de incidentes de seguridad de la información	sí	L0-L5	L3-L5	L3
[16.1] Gestión de incidentes de seguridad de la información y mejoras	sí	L0-L5	L3-L5	L3
[16.1.1] Responsabilidades y procedimientos	sí	L1	L3	L3
[16.1.2] Notificación de eventos de seguridad de	sí	L5	L5	L3

la información				
[16.1.3] Notificación de puntos débiles de la seguridad	sí	L0	L3	L3
[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información	sí	L2	L5	L3
[16.1.5] Respuesta a incidentes de seguridad de la información	sí	L2	L5	L3
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	sí	L1	L4	L3
[16.1.7] Recopilación de evidencias	sí	L2	L5	L3

[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio



[current] situación actual

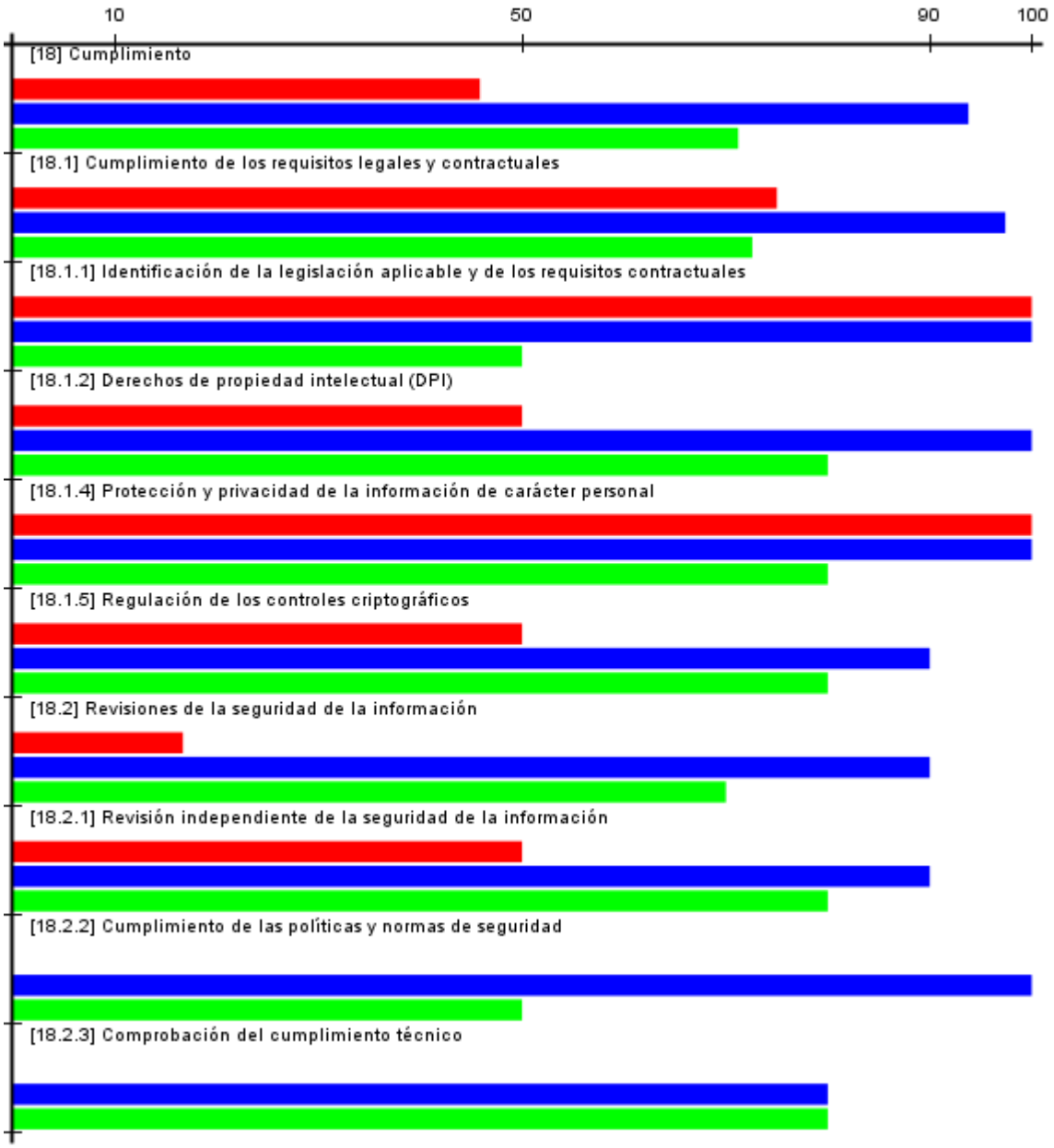
[target] situación objetivo

[PILAR] recomendación

dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio	sí	L0-L1	L3-L5	L3-L4
[17.1] Continuidad de la seguridad de la información	sí	L0-L1	L4-L5	L3-L4
[17.1.1] Planificación de la continuidad de la seguridad de la información	sí	L1	L5	L3
[17.1.2] Implementar la continuidad de la seguridad de la información	sí	L1	L5	L4
[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información	sí	L0	L4	L3
[17.2] Redundancia	sí	L1	L3	L4
[17.2.1] Disponibilidad de los recursos de tratamiento de la información	sí	L1	L3	L4

[18] Cumplimiento



dominio de seguridad: [base] red corporativa

control	aplica	current	target	PILAR
[18] Cumplimiento	sí	L0-L5	L3-L5	L2-L3
[18.1] Cumplimiento de los requisitos legales y contractuales	sí	L2-L5	L4-L5	L2-L3
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales	sí	L5	L5	L2
[18.1.2] Derechos de propiedad intelectual (DPI)	sí	L2	L5	L3
[18.1.3] Protección de los registros de la organización	n.a.	n.a.	n.a.	n.a.
[18.1.4] Protección y privacidad de la información de carácter personal	sí	L5	L5	L3
[18.1.5] Regulación de los controles criptográficos	sí	L2	L4	L3
[18.2] Revisiones de la seguridad de la información	sí	L0-L2	L3-L5	L2-L3
[18.2.1] Revisión independiente de la seguridad de la información	sí	L2	L4	L3
[18.2.2] Cumplimiento de las políticas y normas de seguridad	sí	L0	L5	L2
[18.2.3] Comprobación del cumplimiento técnico	sí	L0	L3	L3