Análisis de Riesgos

[G3] Proyecto 10 Bastionado - G3

14.5.2024

1 Introducción

Documento para anexar a la documentación de seguridad del sistema que se presenta para conseguir la aprobación o autorización de la autoridad responsable del sistema de información.

Datos del sistema sujeto a análisis:

Código: G3

Nombre: Proyecto 10 Bastionado - G3

1.1 Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [DP] Datos personales

2 Dominios de seguridad

dominios de seguridad

- [base] Base

2.1 Valoración de los activos

capa: [B] Activos esenciales

activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[DP]**
[SRW] Server Web	[10]	[M+]	[B]	[A]	[A]	[A]

[SRE] Server Email	[M]	[A-]	[A]	[A]	[M]	[A]
[SRFB] Server Files y Backup	[10]	[10]	[9]	[9]	[10]	[10]
[SRA] Server Aplicaciones	[M]	[A+]	[0]	[A+]	[A+]	[0]
[EC] Equipos del Dpt de Compras	[9]	[10]	[M]	[10]	[A-]	[10]
[MOVCA] Móvil de Empresa C.Administración	[M-]	[A]	[10]	[10]	[A]	[10]
[EFyV] Equipo del Dpt. Facturación y Ventas	[10]	[9]	[10]	[A]	[9]	[10]
[C. Administración] C. Administración	[A]	[A]	[10]	[9]	[A+]	[10]

capa: [E] Equipamiento

activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[DP]**
[ETIC] Equipos del Dpt TIC	[A]	[A]	[10]	[A]	[A-]	[10]
[ERRHH] Equipos del Dpt RRHH	[A+]	[9]	[10]	[10]	[A-]	[10]
[EDev] Equipos del Dpt Delivery	[9]	[A+]	[10]	[A+]	[A+]	[10]
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[B]	[A+]	[B]	[9]	[B+]	[10]
[EL] Equipos del Dpt Legal	[A+]	[10]	[10]	[10]	[10]	[10]
[MOVE] Móvil de Empresa de Empleados	[M]	[A]	[A]	[A-]	[A-]	[10]

[TELIP] Telefonía IP	[0]	[0]	[0]	[0]	[0]	[0]
[RO] Router	[10]	[9]	[A-]	[A+]	[9]	[0]
[ROV] Router VLANS	[10]	[9]	[A+]	[9]	[9]	[0]

capa: [L] Instalaciones

activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[DP]**
[SE1] Sede 1	[10]	[0]	[0]	[0]	[0]	[0]
[SE2] Sede 2	[M+]	[0]	[0]	[0]	[0]	[0]

capa: [P] Personal

activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[DP]**
[EMRRHH] Empleados del Dpt. RRHH	[A]	[A+]	[10]	[9]	[A+]	[10]
[EMTIC] Empleados de TIC	[A+]	[A+]	[10]	[9]	[A+]	[10]
[EM] Empleados Mantenimiento	[M+]	[A+]	[10]	[9]	[M]	[10]
[EMFyV] Empleados Facturación y Ventas	[A]	[A+]	[10]	[9]	[A+]	[10]

[EmCRRSS] Empleados Comunicación y RRSS	[M-]	[A+]	[10]	[9]	[M-]	[10]
[EDEL] Empleados Delivery	[A+]	[A+]	[10]	[9]	[9]	[10]

2.2 Valoración de los dominios

dominio de seguridad	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[DP]**
[base] Base	[10]	[10]	[10]	[10]	[10]	[10]

3 Riesgo acumulado

Se presentan los principales riesgos en cada dominio de seguridad del sistema en las diferentes fases de trabajo.

amenaza

presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella

D – dimensión

se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto

se muestra el máximo impacto causado por esta amenaza en algún activo del sistema

R – riesgo

se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

Fase: [current] situación actual

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, A	[9]	{7,8}
[A.25] Robo de equipos	D, C	[10]	{7,7}
[E.25] Pérdida de equipos	D	[10]	{7,4}

Fase: [target] situación objetivo

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A+]	{7,0}
[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6,5}

Fase: [PILAR] recomendación

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A-]	{5,6}
[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}

Fase: [PILAR] recomendación

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A-]	{5,6}
[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}

Fase: [PILAR] recomendación

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A-]	{5,6}
[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}

Fase: [ENS] Esquema Nacional de Seguridad

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A-]	{5,4}
[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{4,8}

Fase: [B]

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A+]	{6, 9}
[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6, 4}

Fase: [M]

[base] Base

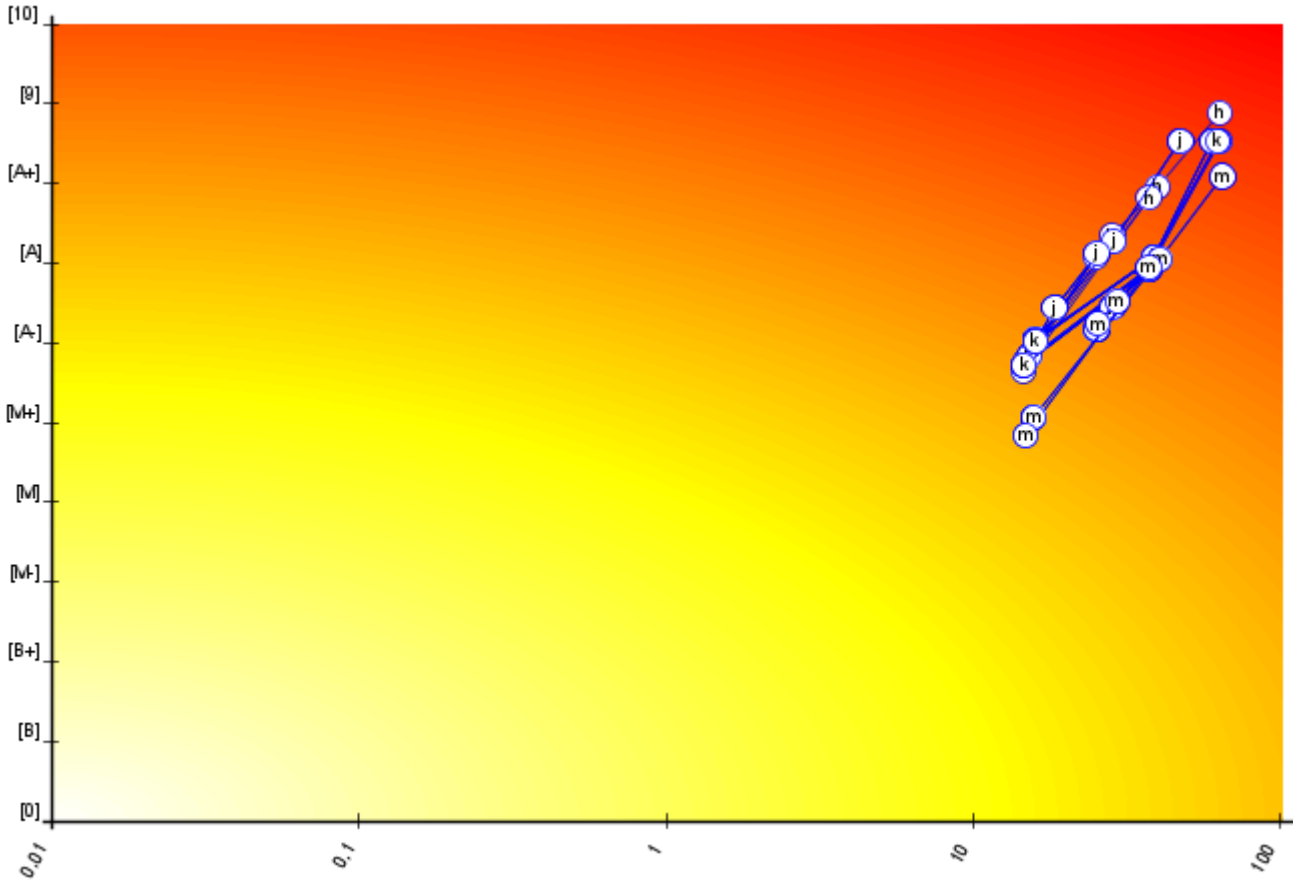
amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A]	{6,5}
[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6,1}

Fase: [A]

[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	I, C, A	[A]	{6,3}
[A.3] Manipulación de los registros de actividad (log)	I	[A-]	{5,8}
[A.24] Denegación de servicio	D	[A]	{5,5}
[A.25] Robo de equipos	D	[A]	{5,5}
[E.25] Pérdida de equipos	D	[A]	{5,5}

3.1 Evolución del riesgo



- a. C, A: EDev * A.11
- b. C, A: ROV * A.11
- c. C, A: RO * A.11
- d. C, A: MOVCA * A.11
- e. C, A: EL * A.11
- f. A: ECRRSS * A.11
- g. A: ERRHH * A.11
- h. I: SRFB * A.11
- i. C, A: ETIC * A.11
- j. A: EC * A.11

- k. C, A: EFyV * A.11
- l. I: ROV * A.3
- m. I: RO * A.3

4 Riesgo repercutido

Se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema en cada fase de trabajo.

activo

presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza

amenaza

presenta la amenaza dentro del catálogo de PILAR.

D – dimensión

se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto

se muestra el máximo impacto causado por esta amenaza sobre el activo esencial

R – riesgo

se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

Fase: [current] situación actual

[base] Base

activo	amenaza	D	I	R
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[9]	{7,8}

[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	D, I, A	[10]	{7,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[10]	{7,7}
[SE1] Sede 1	[A.25] Robo de equipos	C	[10]	{7,7}
[SE2] Sede 2	[A.25] Robo de equipos	C	[10]	{7,7}
[SRW] Server Web	[A.25] Robo de equipos	D	[10]	{7,4}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[10]	{7,4}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D, C	[10]	{7,4}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D, C	[10]	{7,4}
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[9]	{7,4}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[9]	{7,4}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D, C	[10]	{7,4}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[9]	{7,4}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[9]	{7,4}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[9]	{7,4}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[9]	{7,4}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[9]	{7,4}

[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[9]	{7,4}
[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[10]	{7,4}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D, C	[10]	{7,4}
[RO] Router	[E.25] Pérdida de equipos	D, C	[10]	{7,4}
[RO] Router	[A.25] Robo de equipos	D, C	[10]	{7,4}
[RO] Router	[A.11] Acceso no autorizado	C, A	[9]	{7,4}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[10]	{7,4}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D, C	[10]	{7,4}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[9]	{7,4}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[A+]	{7,3}
[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[A+]	{7,3}
[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[A+]	{7,3}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[9]	{7,1}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[9]	{7,1}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[9]	{7,1}

[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[9]	{7,1}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[9]	{7,1}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[9]	{7,1}
[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[9]	{7,1}
[RO] Router	[A.24] Denegación de servicio	D	[9]	{7,1}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[9]	{7,1}
[SRW] Server Web	[A.24] Denegación de servicio	D	[9]	{7,0}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[9]	{7,0}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I, C, A	[9]	{7,0}
[EC] Equipos del Dpt de Compras	[A.5] Suplantación de la identidad	I, A	[10]	{7,0}
[MOVCA] Móvil de Empresa C.Administración	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.5] Suplantación de la identidad	I, C, A, T	[9]	{7,0}
[ETIC] Equipos del Dpt TIC	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}
[ERRHH] Equipos del Dpt RRHH	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}
[EDev] Equipos del Dpt Delivery	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}

[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}
[EL] Equipos del Dpt Legal	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}
[RO] Router	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}
[ROV] Router VLANS	[A.5] Suplantación de la identidad	C, A	[9]	{7,0}
[EC] Equipos del Dpt de Compras	[E.25] Pérdida de equipos	D, I, A	[9]	{6, 9}
[SRFB] Server Files y Backup	[A.15] Modificación de la información	I	[9]	{6, 8}
[EC] Equipos del Dpt de Compras	[A.19] Revelación de información	I, A	[9]	{6, 8}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.19] Revelación de información	C	[9]	{6, 8}
[C. Administración] C. Administración	[A.19] Revelación de información	C	[9]	{6, 8}
[TELIP] Telefonía IP	[A.5] Suplantación de la identidad	C, A	[10]	{6, 8}
[RO] Router	[A.19] Revelación de información	C	[9]	{6, 8}
[ROV] Router VLANS	[A.19] Revelación de información	C	[9]	{6, 8}
[EMTIC] Empleados de TIC	[A.19] Revelación de información	C	[9]	{6, 8}
[SRFB] Server Files y Backup	[A.5] Suplantación de la identidad	I, A	[A+]	{6,7}
[EC] Equipos del Dpt de Compras	[A.6] Abuso de privilegios de acceso	I, A	[A+]	{6,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.3] Manipulación de los registros de actividad (log)	I, T	[A]	{6,7}

[EFyV] Equipo del Dpt. Facturación y Ventas	[A.6] Abuso de privilegios de acceso	C	[A+]	{6,7}
[RO] Router	[A.6] Abuso de privilegios de acceso	C	[A+]	{6,7}
[ROV] Router VLANS	[A.6] Abuso de privilegios de acceso	C	[A+]	{6,7}
[SRW] Server Web	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[SRFB] Server Files y Backup	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[N.1] Fuego	D	[10]	{6, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[I.1] Fuego	D	[10]	{6, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[I.2] Daños por agua	D	[10]	{6, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[I.*] Desastres industriales	D	[10]	{6, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[N.2] Daños por agua	D	[10]	{6, 6}
[ETIC] Equipos del Dpt TIC	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[ERRHH] Equipos del Dpt RRHH	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[EDev] Equipos del Dpt Delivery	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}

[ECRRSS] Equipos del Dpt Comunicación y RRSS	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[EL] Equipos del Dpt Legal	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[TELIP] Telefonía IP	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[TELIP] Telefonía IP	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[RO] Router	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[RO] Router	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[ROV] Router VLANS	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[ROV] Router VLANS	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6, 6}
[SE1] Sede 1	[I.1] Fuego	D	[10]	{6, 6}
[SE1] Sede 1	[N.1] Fuego	D	[10]	{6, 6}
[SE1] Sede 1	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[SE1] Sede 1	[I.*] Desastres industriales	D	[10]	{6, 6}
[SE1] Sede 1	[I.2] Daños por agua	D	[10]	{6, 6}
[SE1] Sede 1	[N.2] Daños por agua	D	[10]	{6, 6}
[SE2] Sede 2	[N.1] Fuego	D	[10]	{6, 6}

[SE2] Sede 2	[I.2] Daños por agua	D	[10]	{6, 6}
[SE2] Sede 2	[I.*] Desastres industriales	D	[10]	{6, 6}
[SE2] Sede 2	[N.2] Daños por agua	D	[10]	{6, 6}
[SE2] Sede 2	[I.1] Fuego	D	[10]	{6, 6}
[SE2] Sede 2	[A.27] Ocupación enemiga	D	[10]	{6, 6}
[SRW] Server Web	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6,5}
[SRFB] Server Files y Backup	[E.24] Caída del sistema por agotamiento de recursos	D	[A+]	{6,5}
[EC] Equipos del Dpt de Compras	[A.24] Denegación de servicio	D	[A+]	{6,5}
[MOVCA] Móvil de Empresa C.Administración	[A.6] Abuso de privilegios de acceso	C	[A+]	{6,5}
[SRW] Server Web	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[SRW] Server Web	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[SRFB] Server Files y Backup	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[SRFB] Server Files y Backup	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[EFyV] Equipo del Dpt. Facturación y Ventas	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}

[EFyV] Equipo del Dpt. Facturación y Ventas	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[ETIC] Equipos del Dpt TIC	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[ETIC] Equipos del Dpt TIC	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[ETIC] Equipos del Dpt TIC	[A.6] Abuso de privilegios de acceso	C	[A+]	{6, 4}
[ERRHH] Equipos del Dpt RRHH	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[ERRHH] Equipos del Dpt RRHH	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[ERRHH] Equipos del Dpt RRHH	[A.6] Abuso de privilegios de acceso	C	[A+]	{6, 4}
[EDev] Equipos del Dpt Delivery	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[EDev] Equipos del Dpt Delivery	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[EDev] Equipos del Dpt Delivery	[A.6] Abuso de privilegios de acceso	C	[A+]	{6, 4}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.6] Abuso de privilegios de acceso	C	[A+]	{6, 4}
[EL] Equipos del Dpt Legal	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}

[EL] Equipos del Dpt Legal	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[EL] Equipos del Dpt Legal	[A.6] Abuso de privilegios de acceso	C	[A+]	{6, 4}
[TELIP] Telefonía IP	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[TELIP] Telefonía IP	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[RO] Router	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[RO] Router	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[ROV] Router VLANS	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[9]	{6, 4}
[ROV] Router VLANS	[I.6] Corte del suministro eléctrico	D	[9]	{6, 4}
[SRW] Server Web	[I.1] Fuego	D	[9]	{6,3 }
[SRW] Server Web	[I.2] Daños por agua	D	[9]	{6,3 }
[SRW] Server Web	[I.*] Desastres industriales	D	[9]	{6,3 }
[SRW] Server Web	[A.26] Ataque destructivo	D	[9]	{6,3 }
[SRW] Server Web	[N.1] Fuego	D	[9]	{6,3 }
[SRW] Server Web	[N.2] Daños por agua	D	[9]	{6,3 }
[SRFB] Server Files y Backup	[N.1] Fuego	D	[9]	{6,3 }

[SRFB] Server Files y Backup	[A.26] Ataque destructivo	D	[9]	{6,3}
[SRFB] Server Files y Backup	[I.2] Daños por agua	D	[9]	{6,3}
[SRFB] Server Files y Backup	[N.2] Daños por agua	D	[9]	{6,3}
[SRFB] Server Files y Backup	[I.*] Desastres industriales	D	[9]	{6,3}
[SRFB] Server Files y Backup	[I.1] Fuego	D	[9]	{6,3}
[SRA] Server Aplicaciones	[A.11] Acceso no autorizado	A	[A]	{6,3}
[EC] Equipos del Dpt de Compras	[A.29] Extorsión	I, A	[9]	{6,3}
[EFyV] Equipo del Dpt. Facturación y Ventas	[N.*] Desastres naturales	D	[10]	{6,3}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.26] Ataque destructivo	D	[9]	{6,3}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.29] Extorsión	C	[9]	{6,3}
[C. Administración] C. Administración	[A.29] Extorsión	C	[9]	{6,3}
[TELIP] Telefonía IP	[N.1] Fuego	D	[9]	{6,3}
[TELIP] Telefonía IP	[I.*] Desastres industriales	D	[9]	{6,3}
[TELIP] Telefonía IP	[I.2] Daños por agua	D	[9]	{6,3}
[TELIP] Telefonía IP	[A.26] Ataque destructivo	D	[9]	{6,3}
[TELIP] Telefonía IP	[N.2] Daños por agua	D	[9]	{6,3}
[TELIP] Telefonía IP	[I.1] Fuego	D	[9]	{6,3}

[RO] Router	[N.2] Daños por agua	D	[9]	{6,3}
[RO] Router	[I.1] Fuego	D	[9]	{6,3}
[RO] Router	[I.2] Daños por agua	D	[9]	{6,3}
[RO] Router	[A.26] Ataque destructivo	D	[9]	{6,3}
[RO] Router	[I.*] Desastres industriales	D	[9]	{6,3}
[RO] Router	[N.1] Fuego	D	[9]	{6,3}
[RO] Router	[A.29] Extorsión	I, C	[9]	{6,3}
[ROV] Router VLANS	[I.1] Fuego	D	[9]	{6,3}
[ROV] Router VLANS	[I.*] Desastres industriales	D	[9]	{6,3}
[ROV] Router VLANS	[N.1] Fuego	D	[9]	{6,3}
[ROV] Router VLANS	[I.2] Daños por agua	D	[9]	{6,3}
[ROV] Router VLANS	[A.26] Ataque destructivo	D	[9]	{6,3}
[ROV] Router VLANS	[N.2] Daños por agua	D	[9]	{6,3}
[ROV] Router VLANS	[A.29] Extorsión	I, C	[9]	{6,3}
[SE1] Sede 1	[N.*] Desastres naturales	D	[10]	{6,3}
[SE2] Sede 2	[N.*] Desastres naturales	D	[10]	{6,3}
[EMTIC] Empleados de TIC	[A.29] Extorsión	I, C	[9]	{6,3}

Fase: [target] situación objetivo

[base] Base

activo	amenaza	D	I	R
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[A+]	{7,0}
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A]	{6,5}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[A]	{6,5}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A]	{6,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[A]	{6,5}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A]	{6,5}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A]	{6,5}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A]	{6,5}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A]	{6,5}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A]	{6,5}
[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6,5}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A]	{6,5}

[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6,5}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A]	{6,5}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A+]	{6,3}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D, C	[A+]	{6,3}
[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	D, I, A	[A+]	{6,3}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A+]	{6,3}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D, C	[A+]	{6,3}
[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A+]	{6,3}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D, C	[A+]	{6,3}
[RO] Router	[E.25] Pérdida de equipos	D, C	[A+]	{6,3}
[RO] Router	[A.25] Robo de equipos	D, C	[A+]	{6,3}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A+]	{6,3}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D, C	[A+]	{6,3}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A+]	{6,3}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A+]	{6,3}
[SRW] Server Web	[A.25] Robo de equipos	D	[A+]	{6,2}

[SRFB] Server Files y Backup	[A.25] Robo de equipos	D, C	[A+]	{6,2}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I, C	[A+]	{6,2}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A+]	{6,1}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A+]	{6,1}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A+]	{6,1}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A+]	{6,1}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A+]	{6,1}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A+]	{6,1}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A+]	{6,1}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A+]	{6,1}
[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A+]	{6,1}
[RO] Router	[A.24] Denegación de servicio	D	[A+]	{6,1}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A+]	{6,1}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.3] Manipulación de los registros de actividad (log)	I, T	[A-]	{5,9}
[SRFB] Server Files y Backup	[A.15] Modificación de la información	I	[A]	{5,8}
[EC] Equipos del Dpt de Compras	[A.19] Revelación de información	I, A	[A]	{5,8}

[EFyV] Equipo del Dpt. Facturación y Ventas	[A.19] Revelación de información	C	[A]	{5,8}
[C. Administración] C. Administración	[A.19] Revelación de información	C	[A]	{5,8}
[RO] Router	[A.19] Revelación de información	C	[A]	{5,8}
[ROV] Router VLANS	[A.19] Revelación de información	C	[A]	{5,8}
[EMTIC] Empleados de TIC	[A.19] Revelación de información	C	[A]	{5,8}
[EC] Equipos del Dpt de Compras	[E.25] Pérdida de equipos	D, I, A	[A]	{5,7}
[EC] Equipos del Dpt de Compras	[A.6] Abuso de privilegios de acceso	I, A	[A]	{5,7}
[EC] Equipos del Dpt de Compras	[A.5] Suplantación de la identidad	I, A	[A]	{5,7}
[MOVCA] Móvil de Empresa C.Administración	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[MOVCA] Móvil de Empresa C.Administración	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[ETIC] Equipos del Dpt TIC	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[ETIC] Equipos del Dpt TIC	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[ERRHH] Equipos del Dpt RRHH	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[ERRHH] Equipos del Dpt RRHH	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}

[EDev] Equipos del Dpt Delivery	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[EDev] Equipos del Dpt Delivery	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[EL] Equipos del Dpt Legal	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[EL] Equipos del Dpt Legal	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[RO] Router	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[RO] Router	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[ROV] Router VLANS	[A.5] Suplantación de la identidad	C, A	[A]	{5,7}
[ROV] Router VLANS	[A.6] Abuso de privilegios de acceso	C	[A]	{5,7}
[SRW] Server Web	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[SRFB] Server Files y Backup	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[SRFB] Server Files y Backup	[A.5] Suplantación de la identidad	I	[A]	{5,6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[ETIC] Equipos del Dpt TIC	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}

[ERRHH] Equipos del Dpt RRHH	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[EDev] Equipos del Dpt Delivery	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[EL] Equipos del Dpt Legal	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[TELIP] Telefonía IP	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[RO] Router	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}
[ROV] Router VLANS	[E.24] Caída del sistema por agotamiento de recursos	D	[A]	{5,6}

Fase: [PILAR] recomendación

[base] Base

activo	amenaza	D	I	R
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A-]	{5,6}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}

[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[A-]	{5,5}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[A-]	{5,4}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[M+]	{5,0}
[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}
[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}
[EC] Equipos del Dpt de Compras	[A.5] Suplantación de la identidad	I, A	[A-]	{4,8}
[MOVCA] Móvil de Empresa C.Administración	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.5] Suplantación de la identidad	C, A	[A-]	{4,8}
[ETIC] Equipos del Dpt TIC	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ERRHH] Equipos del Dpt RRHH	[A.5] Suplantación de la identidad	A	[A-]	{4,8}

[EDev] Equipos del Dpt Delivery	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EL] Equipos del Dpt Legal	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[RO] Router	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ROV] Router VLANS	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	I, A	[A-]	{4,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[RO] Router	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[SRW] Server Web	[A.25] Robo de equipos	D	[A-]	{4, 6}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I	[A-]	{4, 6}

[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[RO] Router	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[RO] Router	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A-]	{4, 6}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.13] Repudio (negación de actuaciones)	T	[A-]	{4,5}

Fase: [PILAR] recomendación

[base] Base

activo	amenaza	D	I	R
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A-]	{5,6}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[A-]	{5,5}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[A-]	{5,4}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[M+]	{5,0}
[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}

[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}
[EC] Equipos del Dpt de Compras	[A.5] Suplantación de la identidad	I, A	[A-]	{4,8}
[MOVCA] Móvil de Empresa C.Administración	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.5] Suplantación de la identidad	C, A	[A-]	{4,8}
[ETIC] Equipos del Dpt TIC	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ERRHH] Equipos del Dpt RRHH	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EDev] Equipos del Dpt Delivery	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EL] Equipos del Dpt Legal	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[RO] Router	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ROV] Router VLANS	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	I, A	[A-]	{4,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[RO] Router	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A-]	{4,7}

[SRW] Server Web	[A.25] Robo de equipos	D	[A-]	{4, 6}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I	[A-]	{4, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[RO] Router	[E.25] Pérdida de equipos	D	[A-]	{4, 6}

[RO] Router	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A-]	{4, 6}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.13] Repudio (negación de actuaciones)	T	[A-]	{4,5}

Fase: [PILAR] recomendación

[base] Base

activo	amenaza	D	I	R
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A-]	{5,6}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A-]	{5,6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[A-]	{5,5}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}

[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A-]	{5,5}
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[A-]	{5,4}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[M+]	{5,0}
[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}
[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{5,0}
[EC] Equipos del Dpt de Compras	[A.5] Suplantación de la identidad	I, A	[A-]	{4,8}
[MOVCA] Móvil de Empresa C.Administración	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.5] Suplantación de la identidad	C, A	[A-]	{4,8}
[ETIC] Equipos del Dpt TIC	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ERRHH] Equipos del Dpt RRHH	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EDev] Equipos del Dpt Delivery	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EL] Equipos del Dpt Legal	[A.5] Suplantación de la identidad	A	[A-]	{4,8}

[RO] Router	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[ROV] Router VLANS	[A.5] Suplantación de la identidad	A	[A-]	{4,8}
[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	I, A	[A-]	{4,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[RO] Router	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A-]	{4,7}
[SRW] Server Web	[A.25] Robo de equipos	D	[A-]	{4, 6}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I	[A-]	{4, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A-]	{4, 6}

[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[RO] Router	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[RO] Router	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A-]	{4, 6}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D	[A-]	{4, 6}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A-]	{4, 6}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A-]	{4, 6}
[SRFB] Server Files y Backup	[A.13] Repudio (negación de actuaciones)	T	[A-]	{4,5}

Fase: [ENS] Esquema Nacional de Seguridad

[base] Base

activo	amenaza	D	I	R

[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A-]	{5,4}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A-]	{5,4}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A-]	{5,4}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A-]	{5,4}
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[A-]	{5,3}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[A-]	{5,3}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A-]	{5,3}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A-]	{5,3}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A-]	{5,3}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A-]	{5,3}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A-]	{5,3}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[M+]	{4,8}
[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{4,8}
[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[M+]	{4,8}
[EC] Equipos del Dpt de Compras	[A.5] Suplantación de la identidad	I, A	[A-]	{4,6}

[RO] Router	[A.5] Suplantación de la identidad	A	[A-]	{4, 6}
[ROV] Router VLANS	[A.5] Suplantación de la identidad	A	[A-]	{4, 6}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A-]	{4,5}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D	[A-]	{4,5}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I	[A-]	{4,5}
[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	I, A	[A-]	{4,5}
[MOVCA] Móvil de Empresa C.Administración	[A.5] Suplantación de la identidad	A	[A-]	{4,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D	[A-]	{4,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A-]	{4,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.5] Suplantación de la identidad	C, A	[A-]	{4,5}
[ETIC] Equipos del Dpt TIC	[A.5] Suplantación de la identidad	A	[A-]	{4,5}
[ERRHH] Equipos del Dpt RRHH	[A.5] Suplantación de la identidad	A	[A-]	{4,5}
[EDev] Equipos del Dpt Delivery	[A.5] Suplantación de la identidad	A	[A-]	{4,5}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.5] Suplantación de la identidad	A	[A-]	{4,5}
[EL] Equipos del Dpt Legal	[A.5] Suplantación de la identidad	A	[A-]	{4,5}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D	[A-]	{4,5}

[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A-]	{4,5}
[RO] Router	[E.25] Pérdida de equipos	D	[A-]	{4,5}
[RO] Router	[A.25] Robo de equipos	D, C	[A-]	{4,5}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D	[A-]	{4,5}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A-]	{4,5}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A-]	{4,5}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A-]	{4,5}
[SRW] Server Web	[A.25] Robo de equipos	D	[A-]	{4,4}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A-]	{4,4}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A-]	{4,4}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D	[A-]	{4,4}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A-]	{4,4}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A-]	{4,4}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A-]	{4,4}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A-]	{4,4}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A-]	{4,4}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A-]	{4,4}

[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A-]	{4, 4}
[RO] Router	[A.24] Denegación de servicio	D	[A-]	{4, 4}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A-]	{4, 4}

Fase: [B]

[base] Base

activo	amenaza	D	I	R
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[A+]	{6, 9}
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A]	{6, 4}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[A]	{6, 4}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[A]	{6, 4}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}

[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6, 4}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}
[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6, 4}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A]	{6, 4}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A+]	{6,1}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A+]	{6,1}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I, C	[A+]	{6,1}
[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	I, A	[A+]	{6,1}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A+]	{6,1}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A+]	{6,1}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A+]	{6,1}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A+]	{6,1}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A+]	{6,1}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A+]	{6,1}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A+]	{6,1}
[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A+]	{6,1}

[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A+]	{6,1}
[RO] Router	[A.24] Denegación de servicio	D	[A+]	{6,1}
[RO] Router	[A.25] Robo de equipos	D, C	[A+]	{6,1}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A+]	{6,1}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A+]	{6,1}
[SRW] Server Web	[A.25] Robo de equipos	D	[A+]	{6, 0}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A+]	{6, 0}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D	[A+]	{6, 0}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D	[A+]	{6, 0}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D, C	[A+]	{6, 0}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D, C	[A+]	{6, 0}
[RO] Router	[E.25] Pérdida de equipos	D, C	[A+]	{6, 0}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D, C	[A+]	{6, 0}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A+]	{6, 0}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A+]	{6, 0}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.3] Manipulación de los registros de actividad (log)	I, T	[A-]	{5,8}

[EC] Equipos del Dpt de Compras	[A.6] Abuso de privilegios de acceso	I, A	[A]	{5,6}
[EC] Equipos del Dpt de Compras	[E.25] Pérdida de equipos	I, A	[A]	{5,6}
[MOVCA] Móvil de Empresa C.Administración	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[ETIC] Equipos del Dpt TIC	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[ERRHH] Equipos del Dpt RRHH	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[EDev] Equipos del Dpt Delivery	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[EL] Equipos del Dpt Legal	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[RO] Router	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[ROV] Router VLANS	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}

Fase: [M]

[base] Base

activo	amenaza	D	I	R
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C, A	[A]	{6,5}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[A]	{6,1}

[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6,1}
[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[A]	{6,1}
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A-]	{6, 0}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A, T	[A-]	{6, 0}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A-]	{6, 0}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I, C	[A]	{5,8}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A]	{5,7}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A]	{5,7}

[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	I, A	[A]	{5,7}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A]	{5,7}
[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A]	{5,7}
[RO] Router	[A.25] Robo de equipos	D, C	[A]	{5,7}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A]	{5,7}
[SRW] Server Web	[A.25] Robo de equipos	D	[A]	{5,6}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A]	{5,6}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D	[A]	{5,6}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D	[A]	{5,6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A]	{5,6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D, C	[A]	{5,6}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A]	{5,6}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A]	{5,6}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A]	{5,6}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A]	{5,6}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A]	{5,6}
[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A]	{5,6}

[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D, C	[A]	{5,6}
[RO] Router	[E.25] Pérdida de equipos	D, C	[A]	{5,6}
[RO] Router	[A.24] Denegación de servicio	D	[A]	{5,6}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A]	{5,6}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D, C	[A]	{5,6}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A]	{5,6}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A]	{5,6}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.3] Manipulación de los registros de actividad (log)	I, T	[A-]	{5,5}
[SRFB] Server Files y Backup	[A.5] Suplantación de la identidad	I	[A-]	{5,2}
[SRFB] Server Files y Backup	[A.15] Modificación de la información	I	[A]	{5,2}
[EC] Equipos del Dpt de Compras	[A.6] Abuso de privilegios de acceso	I, A	[A]	{5,2}
[EC] Equipos del Dpt de Compras	[E.25] Pérdida de equipos	I, A	[A]	{5,2}
[EC] Equipos del Dpt de Compras	[A.19] Revelación de información	I, A	[A-]	{5,2}
[EC] Equipos del Dpt de Compras	[A.5] Suplantación de la identidad	I, A	[A-]	{5,2}
[MOVCA] Móvil de Empresa C.Administración	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}

[MOVCA] Móvil de Empresa C.Administración	[A.5] Suplantación de la identidad	C	[A-]	{5,2}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.19] Revelación de información	C	[A-]	{5,2}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.5] Suplantación de la identidad	C	[A-]	{5,2}
[C. Administración] C. Administración	[A.19] Revelación de información	C	[A-]	{5,2}
[ETIC] Equipos del Dpt TIC	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[ERRHH] Equipos del Dpt RRHH	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[EDev] Equipos del Dpt Delivery	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[EL] Equipos del Dpt Legal	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[RO] Router	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[RO] Router	[A.5] Suplantación de la identidad	C	[A-]	{5,2}
[ROV] Router VLANS	[A.5] Suplantación de la identidad	C	[A-]	{5,2}
[ROV] Router VLANS	[A.6] Abuso de privilegios de acceso	C	[A]	{5,2}
[EMTIC] Empleados de TIC	[A.19] Revelación de información	C	[A-]	{5,2}

Fase: [A]

[base] Base

activo	amenaza	D	I	R
[SRFB] Server Files y Backup	[A.11] Acceso no autorizado	I, C	[A]	{6,3}
[EC] Equipos del Dpt de Compras	[A.11] Acceso no autorizado	I, A	[A-]	{5,8}
[EC] Equipos del Dpt de Compras	[A.3] Manipulación de los registros de actividad (log)	I, A	[A-]	{5,8}
[MOVCA] Móvil de Empresa C.Administración	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.11] Acceso no autorizado	I, C, A	[A-]	{5,8}
[ETIC] Equipos del Dpt TIC	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[ERRHH] Equipos del Dpt RRHH	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[EDev] Equipos del Dpt Delivery	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[EL] Equipos del Dpt Legal	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[RO] Router	[A.3] Manipulación de los registros de actividad (log)	I	[A-]	{5,8}
[RO] Router	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[ROV] Router VLANS	[A.3] Manipulación de los registros de actividad (log)	I	[A-]	{5,8}

[ROV] Router VLANS	[A.11] Acceso no autorizado	C, A	[A-]	{5,8}
[SRW] Server Web	[A.25] Robo de equipos	D	[A]	{5,5}
[SRW] Server Web	[E.25] Pérdida de equipos	D	[A]	{5,5}
[SRW] Server Web	[A.24] Denegación de servicio	D	[A]	{5,5}
[SRFB] Server Files y Backup	[E.25] Pérdida de equipos	D	[A]	{5,5}
[SRFB] Server Files y Backup	[A.24] Denegación de servicio	D	[A]	{5,5}
[SRFB] Server Files y Backup	[A.25] Robo de equipos	D	[A]	{5,5}
[SRFB] Server Files y Backup	[A.6] Abuso de privilegios de acceso	I	[A]	{5,5}
[EC] Equipos del Dpt de Compras	[A.25] Robo de equipos	I, A	[A]	{5,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.24] Denegación de servicio	D	[A]	{5,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.25] Robo de equipos	D, C	[A]	{5,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[E.25] Pérdida de equipos	D	[A]	{5,5}
[ETIC] Equipos del Dpt TIC	[A.24] Denegación de servicio	D	[A]	{5,5}
[ERRHH] Equipos del Dpt RRHH	[A.24] Denegación de servicio	D	[A]	{5,5}
[EDev] Equipos del Dpt Delivery	[A.24] Denegación de servicio	D	[A]	{5,5}
[ECRRSS] Equipos del Dpt Comunicación y RRSS	[A.24] Denegación de servicio	D	[A]	{5,5}
[EL] Equipos del Dpt Legal	[A.24] Denegación de servicio	D	[A]	{5,5}

[TELIP] Telefonía IP	[A.24] Denegación de servicio	D	[A]	{5,5}
[TELIP] Telefonía IP	[A.25] Robo de equipos	D, C	[A]	{5,5}
[TELIP] Telefonía IP	[E.25] Pérdida de equipos	D	[A]	{5,5}
[RO] Router	[E.25] Pérdida de equipos	D	[A]	{5,5}
[RO] Router	[A.24] Denegación de servicio	D	[A]	{5,5}
[RO] Router	[A.25] Robo de equipos	D, C	[A]	{5,5}
[ROV] Router VLANS	[A.25] Robo de equipos	D, C	[A]	{5,5}
[ROV] Router VLANS	[A.24] Denegación de servicio	D	[A]	{5,5}
[ROV] Router VLANS	[E.25] Pérdida de equipos	D	[A]	{5,5}
[SE1] Sede 1	[A.25] Robo de equipos	C	[A]	{5,5}
[SE2] Sede 2	[A.25] Robo de equipos	C	[A]	{5,5}
[EFyV] Equipo del Dpt. Facturación y Ventas	[A.3] Manipulación de los registros de actividad (log)	I, T	[M+]	{5,3}

5 Activos

Relación de activos identificados en el sistema de información.

dominio de seguridad: [base] Base

- Activos esenciales
  - [B] Activos esenciales
    - [SRV] Servidores
      - [SRW] Server Web
      - [SRE] Server Email
      - [SRFB] Server Files y Backup
      - [SRA] Server Aplicaciones
    - [EC] Equipos del Dpt de Compras
    - [MOVCA] Móvil de Empresa C.Administración
    - [EFyV] Equipo del Dpt. Facturación y Ventas
    - [C. Administración] C. Administración
- activos
  - [E] Equipamiento
    - [HW] Equipos
      - [ETIC] Equipos del Dpt TIC
      - [ERRHH] Equipos del Dpt RRHH
      - [EDev] Equipos del Dpt Delivery
      - [ECRRSS] Equipos del Dpt Comunicación y RRSS
      - [EL] Equipos del Dpt Legal
    - [DR] Dispositivos de Red
      - [RO] Router
      - [ROV] Router VLANS
  - [L] Instalaciones

- [SE1] Sede 1
- [SE2] Sede 2

- [P] Personal
  - [EMRRHH] Empleados del Dpt. RRHH
  - [EMTIC] Empleados de TIC
  - [EM] Empleados Mantenimiento
  - [EMFyV] Empleados Facturación y Ventas
  - [EmCRRSS] Empleados Comunicación y RRSS
  - [EDEL] Empleados Delivery

5.1 Descripción

Detalle de los activos identificados en el sistema de información.

dominio de seguridad: [base] Base

[SRV] Servidores

Dominio de seguridad

[base] Base

Clases de activos

[SRW] Server Web

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [D.files] ficheros de datos
  - [D.multimedia] multimedia
  - [S.prov.www] world wide web
  - [HW.host] grandes equipos (host)
  - [HW.data] que almacena datos
  - [COM.VLAN] LAN virtual
  - [COM.WAN] red de área amplia
  - [AUX.power] fuentes de alimentación
  - [AUX.ups] sai - sistemas de alimentación ininterrumpida
  - [AUX.ac] equipos de climatización
  - [L.local] cuarto

[SRE] Server Email

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [D.msg] mensajes (enviados por canales de comunicaciones)
  - [D.e-msg] mensajes cifrados
  - [D.int] datos de gestión interna
  - [D.password] credenciales (ej. contraseñas)
  - [D.auth] datos de validación de credenciales
  - [D.multimedia] multimedia
  - [S.prov.email] correo electrónico
  - [HW.host] grandes equipos (host)

- [COM.VLAN] LAN virtual
- [COM.WAN] red de área amplia
- [AUX.power] fuentes de alimentación
- [AUX.ups] sai - sistemas de alimentación ininterrumpida
- [AUX.ac] equipos de climatización
- [L.local] cuarto

[SRFB] Server Files y Backup

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [D.files] ficheros de datos
  - [D.backup] copias de respaldo
  - [S.prov.ft] transferencia de ficheros
  - [S.prov.backup] servicio de copias de respaldo (backup)
  - [HW.host] grandes equipos (host)
  - [HW.backup] equipamiento de respaldo
  - [HW.data] que almacena datos
  - [COM.VLAN] LAN virtual
  - [AUX.power] fuentes de alimentación
  - [AUX.ups] sai - sistemas de alimentación ininterrumpida
  - [AUX.ac] equipos de climatización
  - [L.local] cuarto

[SRA] Server Aplicaciones

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [D.files] ficheros de datos
  - [D.conf] datos de configuración
  - [D.multimedia] multimedia
  - [D.source] código fuente
  - [D.exe] código ejecutable
  - [S.prov.file] almacenamiento de ficheros
- [SW] Aplicaciones (software)
  - [SW.prp] desarrollo propio (in house)
  - [SW.sub] desarrollo a medida (subcontratado)
  - [SW.std] estándar (off the shelf)
  - [HW.host] grandes equipos (host)
  - [COM.VLAN] LAN virtual
  - [AUX.power] fuentes de alimentación
  - [AUX.ups] sai - sistemas de alimentación ininterrumpida
  - [AUX.ac] equipos de climatización
  - [L.local] cuarto

[EC] Equipos del Dpt de Compras

Dominio de seguridad

[base] Base

Clases de activos

- [essential.info.biz] datos de interés para el negocio
- [essential.info.com] datos de interés comercial
- [D.files] ficheros de datos
- [D.e-files] ficheros cifrados
- [D.records] registros de la organización
- [D.msg] mensajes (enviados por canales de comunicaciones)
- [D.e-msg] mensajes cifrados
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [D.source] código fuente
- [D.exe] código ejecutable
- [HW.pc] informática personal
- [COM.VLAN] LAN virtual

[MOVCA] Móvil de Empresa C.Administración

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [D.msg] mensajes (enviados por canales de comunicaciones)
  - [D.password] credenciales (ej. contraseñas)
  - [D.auth] datos de validación de credenciales
  - [D.voice] voz
  - [D.multimedia] multimedia

- [HW.mobile] informática móvil
- [COM.X25] X25 (red de datos)
- [COM.wifi] WiFi
- [COM.mobile] telefonía móvil
- [P.ui] usuarios internos

[EFyV] Equipo del Dpt. Facturación y Ventas

Dominio de seguridad

[base] Base

Clases de activos

- [essential.info.biz] datos de interés para el negocio
- [essential.info.com] datos de interés comercial
- [essential.bp] proceso de negocio
- [essential.ppd] tratamiento de datos personales
- [D.e-files] ficheros cifrados
- [D.records] registros de la organización
- [D.msg] mensajes (enviados por canales de comunicaciones)
- [D.e-msg] mensajes cifrados
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [HW.pc] informática personal
- [COM.VLAN] LAN virtual

[C. Administración] C. Administración

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [P.adm] administradores de sistemas

[HW] Equipos

Dominio de seguridad

[base] Base

Clases de activos

[ETIC] Equipos del Dpt TIC

Dominio de seguridad

[base] Base

Clases de activos

- [D.files] ficheros de datos
- [D.e-files] ficheros cifrados
- [D.records] registros de la organización
- [D.msg] mensajes (enviados por canales de comunicaciones)
- [D.e-msg] mensajes cifrados
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales

- [D.source] código fuente
- [D.exe] código ejecutable
- [HW.pc] informática personal
- [COM.VLAN] LAN virtual

[ERRHH] Equipos del Dpt RRHH

Dominio de seguridad

[base] Base

Clases de activos

- [D.files] ficheros de datos
- [D.e-files] ficheros cifrados
- [D.records] registros de la organización
- [D.msg] mensajes (enviados por canales de comunicaciones)
- [D.e-msg] mensajes cifrados
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [D.source] código fuente
- [D.exe] código ejecutable
- [HW.pc] informática personal
- [COM.VLAN] LAN virtual

[EDev] Equipos del Dpt Delivery

Dominio de seguridad

[base] Base

Clases de activos

- [D.files] ficheros de datos
- [D.e-files] ficheros cifrados
- [D.records] registros de la organización
- [D.msg] mensajes (enviados por canales de comunicaciones)
- [D.e-msg] mensajes cifrados
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [HW.pc] informática personal
- [COM.VLAN] LAN virtual

[ECRRSS] Equipos del Dpt Comunicación y RRSS

Dominio de seguridad

[base] Base

Clases de activos

- [D.files] ficheros de datos
- [D.e-files] ficheros cifrados
- [D.records] registros de la organización
- [D.msg] mensajes (enviados por canales de comunicaciones)
- [D.e-msg] mensajes cifrados
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [HW.pc] informática personal

- [COM.VLAN] LAN virtual

[EL] Equipos del Dpt Legal

Dominio de seguridad

[base] Base

Clases de activos

- [D.files] ficheros de datos
- [D.e-files] ficheros cifrados
- [D.records] registros de la organización
- [D.msg] mensajes (enviados por canales de comunicaciones)
- [D.e-msg] mensajes cifrados
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [HW.pc] informática personal
- [COM.VLAN] LAN virtual

[TEL] Telefonía

Dominio de seguridad

[base] Base

Clases de activos

[MOVE] Móvil de Empresa de Empleados

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [D.msg] mensajes (enviados por canales de comunicaciones)
  - [D.password] credenciales (ej. contraseñas)
  - [D.auth] datos de validación de credenciales
  - [D.voice] voz
  - [D.multimedia] multimedia
  - [HW.mobile] informática móvil
  - [COM.X25] X25 (red de datos)
  - [COM.wifi] WiFi
  - [COM.mobile] telefonía móvil
  - [P.ui] usuarios internos

[TELIP] Telefonía IP

Dominio de seguridad

[base] Base

Clases de activos

- [HW.ipphone] teléfono IP
- [COM.PSTN] red telefónica
- [L.local] cuarto
- [P.ui] usuarios internos

[DR] Dispositivos de Red

Dominio de seguridad

[base] Base

Clases de activos

[RO] Router

Dominio de seguridad

[base] Base

Clases de activos

- [D.log] registro de actividad (log)
- [HW.other] otros ...
- [COM.wifi] WiFi
- [COM.WAN] red de área amplia
- [L.local] cuarto
- [P.adm] administradores de sistemas

[ROV] Router VLANS

Dominio de seguridad

[base] Base

Clases de activos

- [D.log] registro de actividad (log)
- [HW.other] otros ...
- [COM.wifi] WiFi

- [COM.VLAN] LAN virtual
- [L.local] cuarto
- [P.adm] administradores de sistemas

[SE1] Sede 1

Dominio de seguridad

[base] Base

Clases de activos

- [L.building] edificio

[SE2] Sede 2

Dominio de seguridad

[base] Base

Clases de activos

- [L.building] edificio

[EMRRHH] Empleados del Dpt. RRHH

Dominio de seguridad

[base] Base

Clases de activos

- [P.ui] usuarios internos

[EMTIC] Empleados de TIC

Dominio de seguridad

[base] Base

Clases de activos

- [P.adm] administradores de sistemas

[EM] Empleados Mantenimiento

Dominio de seguridad

[base] Base

Clases de activos

- [P.ui] usuarios internos

[EMFyV] Empleados Facturación y Ventas

Dominio de seguridad

[base] Base

Clases de activos

- [P.ui] usuarios internos

[EmCRRSS] Empleados Comunicación y RRSS

Dominio de seguridad

[base] Base

Clases de activos

- [P.ui] usuarios internos

[EDEL] Empleados Delivery

Dominio de seguridad

[base] Base

Clases de activos

- [P.ui] usuarios internos

6 Comentarios adicionales

Con ayuda de la herramienta PILAR, hemos podido comprobar que existen distintos aspectos que podríamos mejorar de nuestra empresa, además de comprender e identificar de manera mucho más precisa qué activos son claves para el buen funcionamiento y nuestra seguridad.

Al tratarse nuestra empresa de una consultora con una página web, con información de nuestros distintos clientes y ventas, resulta al final muy coherente que los activos con más riesgo y los más importantes sean:

- **El servidor web**
- **El servidor de archivos**
- **Equipos del departamento de compras y ventas**
- **Sedes**

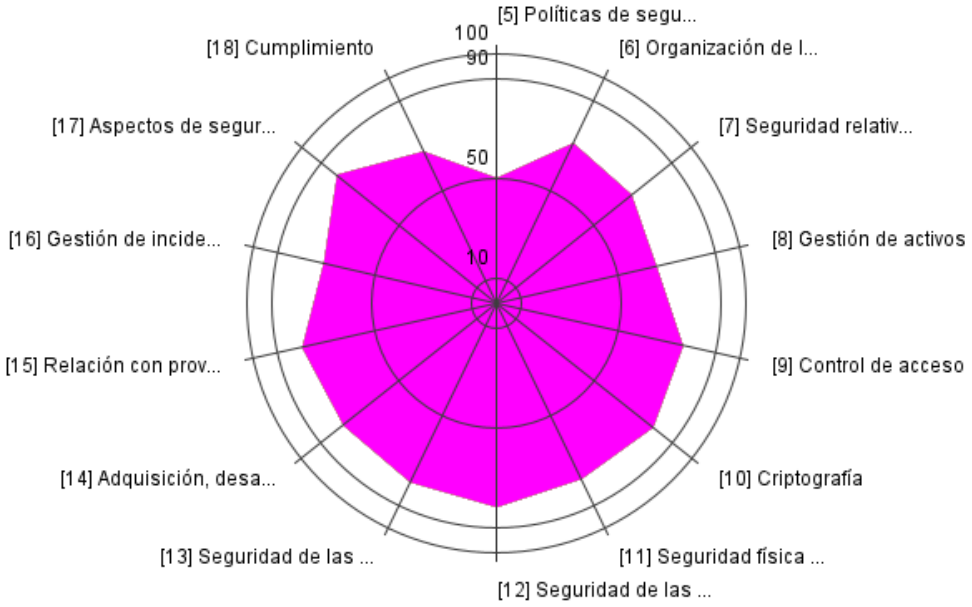
Esto se debe a que la lógica de negocio de nuestra empresa depende fundamentalmente de que nuestra web esté operativa, de que los datos de nuestros clientes estén bajo seguro y ocurre lo mismo para los datos de nuestras operaciones y datos críticos.

Es por ello que los equipos de los departamentos de compras y ventas se incluyen, ya que contienen información de clientes y proveedores crítica, así como de transacciones y ciertas operaciones, como los

servidores de archivos y web, de los que depende nuestra web para funcionar o están conectados a nivel de red y la vulneración de uno podría impactar en el otro.

PILAR nos ofrece también un análisis de madurez que puede resultarnos muy útil para saber dónde centrarnos y qué prioridad darle.

Podemos ver en el siguiente gráfico el nivel de madurez actual de la empresa:



Se puede apreciar cómo los apartados [5] *PolÍticas de Seguridad,* [8] *Gestión de activos* y [16] *Gestión de Incidentes* tienen un nivel de madurez bajo, y además son bastante esenciales.

Existen también niveles bajos en los apartados [7] Seguridad relativa a los recursos humanos, y [6] Organización de la gestión de la información, pero se considera que en cuanto al control [6], mejorará con la implementación de medidas de mitigación en otros controles y la seguridad relativa a los recursos humanos es menos prioritaria que [5], [8] y [16].

Teniendo esto en cuenta, se proponen las siguientes medidas y buenas prácticas:

Políticas de Seguridad de la Información

1. Creación del Plan Director de Seguridad

- **Desarrollo del Plan**: Elabora un plan director de ciberseguridad que incluya objetivos a largo plazo, responsabilidades, recursos necesarios y un cronograma de implementación.

- **Alineación Estratégica**: Asegura que el plan esté alineado con los objetivos estratégicos de la organización y con las normativas vigentes (como GDPR, ISO 27001, NIST).

- **Proceso de Aprobación:** Define un proceso claro para la aprobación del plan, que incluya revisiones por parte de los departamentos relevantes y la aprobación final por parte de la alta dirección.

- **Adaptación y Actualización:** Revisa y actualiza el plan director de seguridad al menos una vez al año o cuando ocurran cambios significativos en el entorno de amenazas o en la estructura de la organización.

2. Difusión y Capacitación

- **Acceso a Políticas:** Almacena todas las políticas en un repositorio accesible para todos los empleados (por ejemplo, una intranet corporativa).

- **Programas de Capacitación**: Organiza sesiones de capacitación periódicas (al menos anualmente) para todos los empleados y sesiones adicionales para nuevos empleados.

- **Materiales de Capacitación**: Crea materiales didácticos, como manuales, videos y cuestionarios, para facilitar la comprensión de las políticas.

3. Cumplimiento y Monitoreo

- **Auditorías Internas**: Programa auditorías internas trimestrales para verificar el cumplimiento de las políticas de seguridad.

- **Métricas de Cumplimiento**: Define KPIs para medir el cumplimiento, como el número de incidentes relacionados con el incumplimiento de políticas.

Gestión de Incidentes de Seguridad de la Información

1. Plan de Respuesta a Incidentes

- **Estructura del Plan**: Elabora un plan que incluya identificación, contención, erradicación, recuperación y lecciones aprendidas.

- **Procedimientos Detallados**: Documenta procedimientos específicos para diferentes tipos de incidentes (malware, violaciones de datos, ataques DDoS).

- **Contacto de Emergencia**: Incluye una lista de contactos de emergencia internos y externos (proveedores de servicios, autoridades).

2. Equipos de Respuesta a Incidentes

- **Definición de Roles**: Define claramente los roles y responsabilidades de cada miembro del equipo de respuesta a incidentes (IRT).

- **Capacitación del IRT**: Organiza capacitaciones especializadas y ejercicios de simulación de incidentes regularmente.

- **Disponibilidad**: Asegura la disponibilidad 24/7 del equipo de respuesta a incidentes mediante turnos y alertas automáticas.

3. Herramientas y Tecnologías

- **SIEM**: Implementa un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) para la centralización y análisis de logs. Es de considerar por ejemplo el stack ELK como opción interesante.

- **EDR**: Utiliza herramientas de detección y respuesta en endpoints (EDR) para una respuesta rápida y eficaz a incidentes.

- **Sistemas de Alerta**: Configura alertas automáticas para incidentes críticos que requieran atención inmediata, como por ejemplo Snort o Suricata.

4. Simulacros y Ejercicios

- **Simulaciones Regulares**: Realiza simulacros de incidentes al menos dos veces al año para evaluar la preparación del equipo.

- **Revisión de Resultados**: Después de cada simulacro, revisa los resultados y ajusta el plan de respuesta según sea necesario.

- **Informe de Lecciones Aprendidas**: Documenta las lecciones aprendidas de cada simulacro e incidente real y comparte los conocimientos con todo el equipo.

Gestión de Activos

1. Inventario de Activos

- **Automatización**: Utiliza herramientas de gestión de inventarios automatizadas para detectar y registrar todos los activos como por ejemplo SpiceWorks o Assets Sonar.

- **Actualización Continua**: Establece procesos para la actualización continua del inventario cada vez que se adquiere, cambia o elimina un activo. Posibilidad de automatización de este sistema.

2. Políticas de Manejo de Activos

- **Ciclo de Vida del Activo**: Desarrolla políticas que cubran todo el ciclo de vida de los activos, desde la adquisición hasta la disposición segura.

- **Controles de Acceso**: Implementa controles de acceso basados en roles (RBAC) para limitar el acceso a activos sensibles.

- **Mantenimiento**: Establece procedimientos regulares de mantenimiento y auditoría para asegurar que los activos se mantengan en condiciones óptimas.

3. Monitoreo y Auditoría

- **Auditorías Regulares**: Programa auditorías de activos trimestrales para verificar la precisión del inventario y el cumplimiento de las políticas.

- **Informes de Auditoría**: Genera informes detallados de las auditorías y utiliza los resultados para mejorar la gestión de activos.

Buenas Prácticas Generales para Mejorar el Plan de Madurez

1. Evaluación Continua

- **Utilización de Marcos de Referencia**: Adopta marcos de referencia reconocidos como NIST, ISO 27001 para evaluar la madurez de seguridad.

- **Análisis de Brechas**: Realiza análisis de brechas para identificar áreas de mejora y desarrollar planes de acción específicos.

2. Gobernanza de Seguridad

- **Comité de Seguridad**: Establece un comité de gobernanza de seguridad que incluya representantes de todas las áreas clave de la organización.

- **Reuniones Regulares:** Programa reuniones regulares del comité para revisar el estado de la seguridad y la implementación de nuevas medidas.

3. Capacitación y Concienciación

- **Programas de Capacitación Específicos**: Desarrolla programas de capacitación específicos para diferentes roles dentro de la organización.

- **Evaluación de la Conciencia de Seguridad**: Realiza encuestas y pruebas periódicas para evaluar el nivel de conciencia de seguridad entre los empleados.

4. Tecnología y Automatización

- **Inversión en Herramientas Avanzadas**: Invertir en tecnologías avanzadas de seguridad como inteligencia artificial, machine learning, y blockchain para mejorar la ciberseguridad.

- **Automatización de Procesos**: Automatizar procesos de detección y respuesta a incidentes para reducir el tiempo de reacción.

5. Gestión de Riesgos

- **Evaluaciones de Riesgos**: Realiza evaluaciones de riesgos periódicas para identificar, evaluar y mitigar riesgos de seguridad.

- **Registro de Riesgos**: Mantén un registro actualizado de todos los riesgos identificados y las medidas de mitigación implementadas.

6. Mejora Continua

- **Ciclo PDCA (Plan-Do-Check-Act)**: Implementa el ciclo PDCA para la mejora continua de todos los procesos de seguridad.

- **Métricas y KPIs:** Define y monitorea KPIs específicos para medir el desempeño de las iniciativas de seguridad y ajusta las estrategias en función de los resultados.

Medidas Adicionales para Mejorar el Plan de Madurez

Integración y Sinergia de Controles

- **Mejora Colateral junto a los Demás Controles**: Asegura que todas las políticas y medidas de seguridad trabajen en conjunto de manera sinérgica para fortalecer el sistema de seguridad general. Esto incluye la integración de diversas herramientas y prácticas de seguridad para maximizar su efectividad y cobertura.

Gestión de Incidentes de Seguridad de la Información

- **Elaboración del Plan de Respuesta a Incidentes**: Establece un plan de respuesta detallado que incluya todos los pasos necesarios para manejar un incidente de seguridad desde la detección hasta la recuperación y el aprendizaje posterior.

- **Implementación de SIEM**: Adopta un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) para mejorar la capacidad de detectar, analizar y responder a incidentes de seguridad en tiempo real.

- **Equipo de Respuesta a Incidentes (CSIRT)**: Forma un equipo especializado en la respuesta a incidentes (CSIRT) que esté preparado y equipado para manejar situaciones de emergencia de manera eficiente y efectiva.

Gestión de Activos

- **Elaboración de un Inventario General**: Desarrolla un inventario exhaustivo de todos los activos de la organización, incluyendo hardware, software, datos y otros recursos críticos.

- **Implementación de Herramientas de Gestión**: Utiliza herramientas de gestión de activos como Spiceworks o Asset Sonar para mantener el inventario actualizado, facilitar el seguimiento de los activos y mejorar la eficiencia en la gestión de estos