Identificar (ID)

Control NIST	Pregunta	Respuesta (Sí/No/Parcial)	Evidencia Documental
ID.AM-1	¿Existe un inventario documentado de activos?	Sí/No	Inventario actualizado
ID.AM-2	¿Está clasificado el inventario de activos según su criticidad?	Sí/No	Documentación de clasificación
ID.BE-1	¿Está documentada la cadena de suministro de servicios críticos?	Sí/No	Acuerdos con proveedores
ID.GV-2	¿Existen políticas documentadas para la gestión de riesgos de ciberseguridad?	Sí/No	Políticas internas de ciberseguridad
ID.GV-3	¿Se revisan periódicamente las políticas de ciberseguridad?	Sí/No	Registro de revisiones de políticas
ID.RA-2	¿Se realiza una evaluación formal de riesgos al menos anualmente?	Sí/No	Informes de evaluación de riesgos
ID.RA-3	¿Se han identificado las amenazas más relevantes para la organización?	Sí/No	Análisis de amenazas
ID.RM-1	¿Existe un proceso documentado para gestionar los riesgos identificados?	Sí/No	Procedimiento de gestión de riesgos
ID.RM-2	¿Se asignan responsables para mitigar cada riesgo identificado?	Sí/No	Asignación de responsabilidades en informes

Comentarios del Auditor	Nivel de Cumplimiento (0-100%)
Descripción del inventariado	%
Detalles sobre los activos críticos	%
Riesgos identificados en la cadena de suministro	%
Necesidad de actualizaciones o revisiones	%
Frecuencia de revisiones y responsables	%
Última evaluación realizada	%
Mapa de amenazas relevante para la organización	%
Descripción del proceso y actores responsables	%
Nombre de los responsables asignados	%

Proteger (PR)

Control NIST	Pregunta	Respuesta (Sí/No/Parcial)	Evidencia Documental
PR.AC-2	¿Se aplican controles de acceso basados en roles (RBAC)?	Sí/No	Políticas de acceso
PR.AC-3	¿Se utilizan mecanismos de autenticación multifactor (MFA)?	Sí/No	Configuraciones de autenticación
PR.AC-4	¿Se desactivan o eliminan las cuentas de acceso no utilizadas?	Sí/No	Logs de auditoría de cuentas
PR.AT-1	¿Se realizan programas de capacitación en ciberseguridad para los empleados?	Sí/No	Registro de capacitaciones
PR.AT-2	¿Se adaptan los programas de capacitación según los roles y responsabilidades?	Sí/No	Contenidos de capacitaciones
PR.DS-2	¿Están encriptados los datos en tránsito y en reposo?	Sí/No	Documentación de políticas de cifrado
PR.DS-3	¿Se aplican controles adecuados para proteger los datos sensibles?	Sí/No	Informe de clasificación de datos
PR.DS-4	¿Existe un plan de retención y destrucción segura de datos?	Sí/No	Política de retención de datos
PR.IP-2	¿Se aplican actualizaciones y parches de seguridad de manera oportuna?	Sí/No	Logs de actualizaciones de software
PR.IP-3	¿Se cuenta con mecanismos de protección contra malware actualizados?	Sí/No	Configuración de software de protección
PR.MA-1	¿Se realiza mantenimiento regular de los sistemas críticos?	Sí/No	Plan de mantenimiento
PR.PT-1	¿Se han implementado controles físicos de seguridad en las instalaciones críticas?	Sí/No	Políticas de seguridad física
PR.PT-2	¿Se controlan los accesos físicos a los servidores y redes?	Sí/No	Logs de acceso físico

Comentarios del Auditor	Nivel de Cumplimiento (0-100%)
Control granular de acceso basado en roles	%
MFA activado en cuentas críticas	%
Política para inactivar cuentas inactivas	%
Frecuencia de capacitaciones y asistencia de empleados	%
Cursos específicos para roles clave	%
Descripción de las herramientas de cifrado utilizadas	%
Políticas de clasificación y protección de datos sensibles	%
Proceso documentado de eliminación segura de datos	%
Frecuencia de aplicación de parches y responsables	%
Frecuencia de actualización y monitoreo de amenazas	%
Descripción del mantenimiento y frecuencia	%
Mecanismos físicos (cámaras, acceso controlado)	%
Monitoreo y control de accesos físicos a infraestructuras críticas	%

Detectar (DE)

Control NIST	Pregunta	Respuesta (Sí/No/Parcial)	Evidencia Documental
DE.AE-2	¿Se monitorean todas las actividades y eventos en la red?	Sí/No	Logs de red y seguridad
DE.AE-3	¿Se registran los intentos de acceso no autorizados?	Sí/No	Logs de seguridad
DE.AE-4	¿Se implementa un sistema de detección de intrusos (IDS/IPS)?	Sí/No	Configuración de IDS/IPS
DE.AE-5	¿Se detectan y analizan las anomalías de comportamiento en el sistema?	Sí/No	Informes de análisis de anomalías
DE.CM-2	¿Se mantienen y revisan los registros de auditoría de seguridad?	Sí/No	Logs de auditoría
DE.DP-1	¿Se cuenta con un plan formal de respuesta ante incidentes detectados?	Sí/No	Plan de respuesta documentado
PR.DS-3	¿Se aplican controles adecuados para proteger los datos sensibles?	Sí/No	Informe de clasificación de datos
PR.DS-4	¿Existe un plan de retención y destrucción segura de datos?	Sí/No	Política de retención de datos
PR.IP-2	¿Se aplican actualizaciones y parches de seguridad de manera oportuna?	Sí/No	Logs de actualizaciones de software
PR.IP-3	¿Se cuenta con mecanismos de protección contra malware actualizados?	Sí/No	Configuración de software de protección
PR.MA-1	¿Se realiza mantenimiento regular de los sistemas críticos?	Sí/No	Plan de mantenimiento
PR.PT-1	¿Se han implementado controles físicos de seguridad en las instalaciones críticas?	Sí/No	Políticas de seguridad física
PR.PT-2	¿Se controlan los accesos físicos a los servidores y redes?	Sí/No	Logs de acceso físico

Comentarios del Auditor	Nivel de Cumplimiento (0-100%)
Alcance del monitoreo de eventos	%
Revisión de registros y auditoría	%
Estado de implementación del sistema de detección	%
Frecuencia de análisis y herramientas utilizadas	%
Frecuencia de revisiones y responsables	%
Pruebas del plan de respuesta y responsables asignados	%
Políticas de clasificación y protección de datos sensibles	%
Proceso documentado de eliminación segura de datos	%
Frecuencia de aplicación de parches y responsables	%
Frecuencia de actualización y monitoreo de amenazas	%
Descripción del mantenimiento y frecuencia	%
Mecanismos físicos (cámaras, acceso controlado)	%
Monitoreo y control de accesos físicos a infraestructuras críticas	%

Detectar (DE)

Control NIST	Pregunta	Respuesta (Sí/No/Parcial)	Evidencia Documental
RS.CO-2	¿Se comunican los incidentes de ciberseguridad de manera interna y externa?	Sí/No	Registro de comunicaciones de incidentes
RS.CO-3	¿Se involucran las partes interesadas clave en la respuesta a incidentes?	Sí/No	Plan de respuesta documentado
RS.AN-1	¿Se realiza un análisis forense tras cada incidente de ciberseguridad?	Sí/No	Informes de análisis forense
RS.IM-2	¿Existen procesos documentados para mitigar los efectos de los incidentes de ciberseguridad?	Sí/No	Procedimientos de mitigación
RS.IM-3	¿Se realizan simulacros de incidentes de ciberseguridad?	Sí/No	Registro de simulacros
DE.DP-1	¿Se cuenta con un plan formal de respuesta ante incidentes detectados?	Sí/No	Plan de respuesta documentado
PR.DS-3	¿Se aplican controles adecuados para proteger los datos sensibles?	Sí/No	Informe de clasificación de datos
PR.DS-4	¿Existe un plan de retención y destrucción segura de datos?	Sí/No	Política de retención de datos
PR.IP-2	¿Se aplican actualizaciones y parches de seguridad de manera oportuna?	Sí/No	Logs de actualizaciones de software
PR.IP-3	¿Se cuenta con mecanismos de protección contra malware actualizados?	Sí/No	Configuración de software de protección
PR.MA-1	¿Se realiza mantenimiento regular de los sistemas críticos?	Sí/No	Plan de mantenimiento
PR.PT-1	¿Se han implementado controles físicos de seguridad en las instalaciones críticas?	Sí/No	Políticas de seguridad física

PR.PT-2	¿Se controlan los accesos físicos a los servidores y redes?	Sí/No	Logs de acceso físico

Comentarios del Auditor	Nivel de Cumplimiento (0-100%)
Procedimientos documentados de comunicación	%
Identificación de partes interesadas y sus roles	%
Frecuencia de análisis post-incidente	%
Descripción de los procesos y responsables asignados	%
Frecuencia y resultados de los simulacros realizados	%
Pruebas del plan de respuesta y responsables asignados	%
Políticas de clasificación y protección de datos sensibles	%
Proceso documentado de eliminación segura de datos	%
Frecuencia de aplicación de parches y responsables	%
Frecuencia de actualización y monitoreo de amenazas	%
Descripción del mantenimiento y frecuencia	%
Mecanismos físicos (cámaras, acceso controlado)	%

Monitoreo y control de accesos físicos a infraestructuras críticas	%

Recuperar (RC)

Control NIST	Pregunta	Respuesta (Sí/No/Parcial)	Evidencia Documental
RC.RP-2	¿Se han establecido tiempos de recuperación (RTO/RPO) para cada sistema crítico?	Sí/No	Plan de continuidad
RC.CO-2	¿Se comunica el proceso de recuperación a las partes interesadas clave?	Sí/No	Plan de comunicaciones
RC.IM-2	¿Se revisa y actualiza el plan de recuperación regularmente?	Sí/No	Informes de revisión
RC.IM-3	¿Se prueban regularmente los planes de recuperación?	Sí/No	Informes de pruebas de recuperación
RS.IM-3	¿Se realizan simulacros de incidentes de ciberseguridad?	Sí/No	Registro de simulacros
DE.DP-1	¿Se cuenta con un plan formal de respuesta ante incidentes detectados?	Sí/No	Plan de respuesta documentado
PR.DS-3	¿Se aplican controles adecuados para proteger los datos sensibles?	Sí/No	Informe de clasificación de datos
PR.DS-4	¿Existe un plan de retención y destrucción segura de datos?	Sí/No	Política de retención de datos
PR.IP-2	¿Se aplican actualizaciones y parches de seguridad de manera oportuna?	Sí/No	Logs de actualizaciones de software
PR.IP-3	¿Se cuenta con mecanismos de protección contra malware actualizados?	Sí/No	Configuración de software de protección
PR.MA-1	¿Se realiza mantenimiento regular de los sistemas críticos?	Sí/No	Plan de mantenimiento
PR.PT-1	¿Se han implementado controles físicos de seguridad en las instalaciones críticas?	Sí/No	Políticas de seguridad física

PR.PT-2	¿Se controlan los accesos físicos a los servidores y redes?	Sí/No		Logs de acceso físico

Comentarios del Auditor	Nivel de Cumplimiento (0-100%)
Documentación de tiempos de recuperación y responsables	%
Comunicación planificada para incidentes mayores	%
Frecuencia de revisión y actualización del plan de recuperación	%
Resultados y ajustes tras las pruebas	%
Frecuencia y resultados de los simulacros realizados	%
Pruebas del plan de respuesta y responsables asignados	%
Políticas de clasificación y protección de datos sensibles	%
Proceso documentado de eliminación segura de datos	%
Frecuencia de aplicación de parches y responsables	%
Frecuencia de actualización y monitoreo de amenazas	%
Descripción del mantenimiento y frecuencia	%
Mecanismos físicos (cámaras, acceso controlado)	%

Monitoreo y control de accesos físicos a infraestructuras críticas	%

Gap Analisis – Auditoria

Área	Control NIST	Brecha Detectada	Recomendación del Auditor
Gestión de activos	ID.AM-1	No existe un inventario de activos actualizado	Crear un inventario centralizado
Monitoreo de red	DE.AE-4	No se utiliza sistema IDS/IPS	Implementar IDS/IPS para detección temprana
Recuperación	RC.RP-2	No se han definido los tiempos RTO/RPO	Definir y documentar RTO/RPO para sistemas críticos

Prioridad
Alta
Media
Alta