Requisitos

Capítulo de requisitos según guía de implementación	Requisito	Cumplimiento	Evidencias	Comentarios
Gestión de riesgos (GR)	GR.1 Establecer un proceso de evaluación de riesgo en base a una metodología que permita guiar a la organización por las buenas prácticas de la evaluación del riesgo a nivel tecnológico y de procesos; permitiendo establecer su apetito riesgo, la tolerancia sobre las desviaciones, calcular la probabilidad de ocurrencias y el impacto potencial sobre la materialización de las vulnerabilidades.			
Gestión de riesgos (GR)	GR.2 Contribuir al cumplimiento de los objetivos de seguridad de la información, prevenir o reducir los efectos no deseados y lograr la mejora continua.			
Gestión de riesgos (GR)	GR.3 Establecer un cronograma y plan de acción para mitigar los riesgos a corto y mediano plazo que se consideren inaceptables según la tolerancia al riesgo definida por la organización. Adicionalmente verificar que, una vez subsanados los riesgos con la aplicación de controles adicionales o compensatorios, los mismos se reducen a un nivel aceptable de exposición en relación a los efectos no deseados.			
Planificación (PL)	PL.1 Establecer objetivos anuales con relación a la Seguridad de la Información.			
Planificación (PL)	PL.2 La organización debe garantizar la mejora de la estrategia, políticas, procedimientos y controles que se hayan adoptado para adecuarse a los cambios organizacionales y/o de contexto que haya tenido o pueda afrontar el negocio.			
Política de seguridad de la información (PS)	PS.1 Proporcionar lineamientos de gestión en línea acorde a los objetivos de la organización, contemplando la normativa aplicable. Disponer de medidas para garantizar la confianza y seguridad de los sistemas y de la información en poder de la organización, así como proteger los activos de información y minimizar el impacto en los servicios causados por amenazas o incidentes de seguridad. Demostrar el compromiso de la Dirección con la seguridad de la información.			
Organización (OR)	OR.1 Lograr liderazgo y guía en la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.			
Organización (OR)	OR.2 Contar con un equipo de personas con capacidad de decisión sobre los objetivos de la organización, que vele por la seguridad de la información, marque los lineamientos estratégicos en la materia y defina los objetivos anuales.			
Organización (OR)	OR.3 Contribuir con las buenas prácticas de gestión y control del SGSI dentro de la organización definiendo un procedimiento documentado de contacto con autoridades (internas y externas), ante un incidente de seguridad de la información y, particularmente, ante un incidente de seguridad informática.			
Organización (OR)	OR.4 Lograr que los temas relativos a seguridad de la información estén incluidos en todos los proyectos desde su inicio, independientemente del tipo de proyecto tratado.			
Organización (OR)	OR.5 Garantizar la seguridad de la información de la organización en caso de utilizarse dispositivos móviles (al menos celulares, portables, tabletas) para uso laboral. Proteger la información de la organización, almacenada o accesible desde dispositivos móviles y evitar que éstos sean causa de distribución de software malicioso dentro de la organización o sean el origen de accesos no autorizados.			
Gestión de activos (GA)	OR.6 Garantizar la seguridad de la información cuando se accede de forma remota a los sistemas de información de la organización tanto por personal interno como externo.			
Gestión humana (GH)	GH.1 Lograr que el personal comprenda sus responsabilidades de seguridad de la información y que apliquen la seguridad de la información de acuerdo a las políticas y los procedimientos establecidos.			
Gestión humana (GH)	GH.2 Lograr conciencia de las responsabilidades y buenas prácticas vinculadas a la seguridad de la información de acuerdo a las políticas de seguridad de la información de la organización.			
Gestión de activos (GA)	GA.1 Garantizar la gestión de los activos asociados a la información y los sistemas e instalaciones para su procesamiento.			

Gestión de activos (GA)	GA.2 Proteger y garantizar la confidencialidad, integridad y disponibilidad de la información durante todo el ciclo de vida de los activos.			
Gestión de activos (GA)	GA.3 Garantizar que el personal, proveedores e interesados de la organización conozcan las reglas y tomen los recaudos necesarios para proteger los activos de la información de la organización.			
Gestión de activos (GA)	GA.4 Evitar la divulgación, modificación y borrado de la información contenida en medios extraíbles, como forma de proteger la información de la organización.			
Gestión de activos (GA)	GA.5 Garantizar la adecuada destrucción de la información y los medios de almacenamiento que la contienen, para proteger su confidencialidad.			
Control de acceso (CA)	CA.1 Gestionar y autorizar el acceso lógico a los activos de información (usuarios y usuarios privilegiados, aplicaciones, redes y servicios de red).			
Control de acceso (CA)	CA.2 Revisar y controlar periódicamente los derechos de acceso lógico a los activos de información (incluyendo los permisos de los usuarios privilegiados).			
Control de acceso (CA)	CA.3 Proteger la confidencialidad, autenticidad e integridad de la información digital.			
Control de acceso (CA)	CA.4 Lograr el cumplimiento con los lineamientos establecidos por la UCE y Agesic para el uso de firma electrónica avanzada.			
Seguridad física y del ambiente (SF)	SF.1 Minimizar el riesgo de acceso no autorizado a los centros de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos) y proteger las instalaciones y equipos contra robos, daños o mal uso.			
Seguridad física y del ambiente (SF)	SF.2 Garantizar la continuidad de las operaciones y reducir los efectos causados por desastres humanos o naturales a través de la implementación de controles ambientales en los centros de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos).			
Seguridad física y del ambiente (SF)	SF.3 Lograr una adecuada administración de los componentes críticos alojados en sitios o centros de datos.			
Seguridad de las operaciones (SO)	SO.1 Prevenir y mitigar el riesgo de explotación de vulnerabilidades técnicas en los sistemas.			
Seguridad de las operaciones (SO)	SO.2 Asegurar que los cambios no comprometan la seguridad. Lograr un adecuado control y seguimiento de los pedidos de cambio de los sistemas y configuraciones de componentes de la infraestructura, asegurar que los cambios están justificados y autorizados, que se llevan a cabo sin perjuicio de la calidad del servicio y se encuentran registrados, clasificados, documentados y probados de manera adecuada.			
Seguridad de las operaciones (SO)	SO.3 Asegurar que la capacidad de servicios de TI y la infraestructura de TI, sean capaces de cumplir con los objetivos acordados de capacidad y desempeño de manera puntual y efectiva en términos económicos.			
Seguridad de las operaciones (SO)	SO.4 Reducir los riesgos de accesos no autorizados o realización de cambios no autorizados en producción, evitar modificaciones no deseadas de archivos o sistemas, evitar fallas de los sistemas.			
Seguridad de las operaciones (SO)	SO.5 Asegurar que la información y los sistemas informáticos que la procesan se encuentren protegidos contra software malicioso (por ejemplo: virus, gusanos, troyanos, spyware, adware intrusivo, crimeware, entre otros).			
Seguridad de las operaciones (SO)	SO.6 Preservar la información de la organización o en poder de ésta y poder restaurarla en tiempo y forma en caso de necesidad.			
Seguridad de las operaciones (SO)	SO.7 Conocer los eventos relevantes que se suceden en una aplicación o sistema, por ejemplo inicios de sesión, fallas en los sistemas, eventos de seguridad, etc. Asegurar la protección de los registros de eventos contra modificaciones y/o accesos no autorizados y asegurar los registros de auditoría.			
Seguridad de las operaciones (SO)	SO.8 Garantizar la integridad y seguridad de los sistemas.			
Seguridad de las comunicaciones (SC)	SC.1 Estandarizar la identificación de los portales Web institucionales de la Administración Central.			
Seguridad de las comunicaciones (SC)	SC.2 Optimizar recursos y facilitar el acceso a la información a los ciudadanos.			
Seguridad de las comunicaciones (SC)	SC.3 Unificar la forma de referenciar los dominios/subdominios.			
Seguridad de las comunicaciones (SC)	SC.4 Establecer un criterio único para nombrar a los dominios/subdominios.			
Seguridad de las comunicaciones (SC)	SC.5 Asegurar que la información de contacto de los responsables de los dominios y subdominio se encuentre actualizada y comunicada.			
Seguridad de las comunicaciones (SC)	SC.6 Proteger la información de la organización.			
Seguridad de las comunicaciones (SC)	SC.7 Proteger los correos electrónicos.			

Seguridad de las comunicaciones (SC)	SC.8 Proteger la seguridad de los correos electrónicos, preservando la propiedad de la confidencialidad en los mensajes transmitidos desde y hacia el servidor de correos electrónicos, tanto para aquellas transferencias realizadas entre servidores de correo como las realizadas entre clientes de correo y servidores.			
Seguridad de las comunicaciones (SC)	SC.9 Lograr que todo correo electrónico intercambiado entre servidores gub.uy se realice únicamente utilizando protocolos seguros, que no estén considerados obsoletos o vulnerables, los cuales hacen uso de cifrado robusto de datos.			
Seguridad de las comunicaciones (SC)	SC.10 Lograr que todo correo intercambiado con servidores externos al ámbito gubernamental sea transmitido tratando de conservar la confidencialidad de los datos.			
Seguridad de las comunicaciones (SC)	SC.11 Asegurar que siempre que un cliente de correo se conecte a un servidor para realizar la descarga o envío de correo electrónico lo pueda hacer únicamente a través de protocolos seguros.			
Seguridad de las comunicaciones (SC)	SC.12 Proteger la confidencialidad de este tramo de la comunicación, entre el navegador del cliente y el servicio Web y para esto se requiere el uso de SSL y la implementación de certificados digitales válidos y emitidos por una Autoridad Certificadora de confianza.			
Seguridad de las comunicaciones (SC)	SC.13 Asegurar la protección de la información en las redes.			
Seguridad de las comunicaciones (SC)	SC.14 Mantener la seguridad de la información que se intercambia o transfiere dentro de la organización y con cualquier entidad externa a la misma. Establecer el marco en el cual se intercambiará información desde y con la organización.			
Seguridad de las comunicaciones (SC)	SC.15 Aumentar los niveles de seguridad de las aplicaciones y/o portales expuestos a Internet.			
Adquisición, desarrollo y mantenimiento de los sistemas (AD)	AD.1 Garantizar que la seguridad de la información forma parte de los sistemas de información en todo el ciclo de vida de los proyectos y en las adquisiciones.			
Relación con proveedores (RP)	RP.1 Contar con acuerdos de niveles de servicios que permitan nivelar las expectativas y responder con la calidad establecida y en los tiempos establecidos.			
Relación con proveedores (RP)	RP.2 Establecer y asegurar el cumplimiento de los términos y condiciones de seguridad de la información de los contratos y acuerdos de nivel de servicio con los proveedores. Garantizar que los incidentes y problemas de seguridad de la información se manejan de forma adecuada. Asegurar que se gestiona adecuadamente la seguridad de la información frente a cambios en los servicios de los proveedores.			
Gestión de incidentes (GI)	GI.1 Prevenir y mitigar el impacto de los incidentes de seguridad de la información.			
Gestión de incidentes (GI)	GI.2 Lograr identificar el impacto y alcance de un evento y determinar si es un incidente.			
Gestión de incidentes (GI)	GI.3 Asegurar que los incidentes de seguridad de la información se reportan a las personas adecuadas y en forma consistente de acuerdo a la política de gestión de incidentes. Determinar si es un incidente de seguridad informática a reportar al CERTuy o equipo de respuestas externo.			
Gestión de incidentes (GI)	GI.4 Lograr que todos los incidentes sean registrados oportunamente para evaluarlos, estudiarlos, contar con estadísticas y tomar las acciones necesarias en forma rápida y efectiva siguiendo los procedimientos establecidos			
Gestión de incidentes (GI)	GI.5 Lograr acciones de respuestas coordinadas, rápidas y efectivas ante los incidentes de seguridad de la información. Asegurar que puede reanudar el nivel de seguridad normal para posteriormente dar comienzo a la recuperación.			
Gestión de incidentes (GI)	GI.6 Lograr que la organización identifique y capitalice las lecciones aprendidas luego de ocurrido un incidentes retroalimentando la gestión de riesgos y los controles implementados.			
Continuidad de las operaciones (CO)	CO.1 Garantizar el normal funcionamiento de los centros de datos y operaciones.			
Continuidad de las operaciones (CO)	CO.2 Asegurar que la infraestructura de redes del centro de datos no tenga puntos únicos de falla, es decir, que la operativa del centro de datos pueda continuar aun ante la caída de un activo de red.			
Continuidad de las operaciones (CO)	CO.3 La organización debe brindar los recursos necesarios a las áreas encargadas de gestionar la continuidad para lograr hacer frente y/o estar preparada para situaciones adversas o crisis que puedan afectar la continuidad de las operaciones.			
Continuidad de las operaciones (CO)	CO.4 Preparar a la organización ante eventos anormales, disruptivos o desastres que puedan afectar sus operaciones, en principio, relacionadas a trámites en línea.			
Continuidad de las operaciones (CO)	CO.5 Definir métricas básicas para planificar la continuidad de las operaciones.			
Continuidad de las operaciones (CO)	CO.6 Difundir y comunicar la situación de crisis o incidentes que afectan a la ciberseguridad de la organización, a través de interlocutores formalmente autorizados.			

Cumplimiento normativo (CN)	CN.1 Asegurar el cumplimiento normativo relacionado con la seguridad de la información y con los requisitos de seguridad.			
Cumplimiento normativo (CN)	CN.2 Asegurar la conveniencia, adecuación y eficacia continua de la gestión de la seguridad de la información en la organización de acuerdo al presente marco.			
Cumplimiento normativo (CN)	CN.3 Conocer y mitigar las vulnerabilidades existentes en los sistemas de información de la organización de acuerdo a los requisitos de seguridad de la información establecidos en la política.			
Cumplimiento normativo (CN)	CN.4 Mantener el número óptimo de licencias para soportar de forma adecuada los requerimientos de las operaciones y documentar su uso.			

Modelo de madurez

Función	Categoría	Subcategoría	Madurez	Comentarios
Identificar	Gestión de Activos (ID.GA)	ID.GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.		
Identificar	Gestión de Activos (ID.GA)	ID.GA-2. Las plataformas de software y aplicaciones se encuentran inventariadas.		
Identificar	Gestión de Activos (ID.GA)	ID.GA-3. Se utilizan medidas de seguridad y procedimientos de gestión para proteger y controlar el flujo de información interna y externa.		
Identificar	Gestión de Activos (ID.GA)	ID.GA-4. El equipamiento y los sistemas de información utilizados fuera de las instalaciones se encuentran identificados y se aplican medidas para mantener la seguridad de la información.		
Identificar	Gestión de Activos (ID.GA)	ID.GA-5. Los activos (por ejemplo: hardware, dispositivos, datos y software) se encuentran clasificados en función del tipo de información que contienen o procesan y en el valor que poseen para el negocio.		
Identificar	Gestión de Activos (ID.GA)	ID.GA-6. Los roles y responsabilidades de seguridad de la información y ciberseguridad se encuentran asignados.		
Identificar	Ambiente de Negocio (ID.AN)	ID.AN-1. Se identifica y comunica el rol de la organización en la cadena de suministro.		
Identificar	Ambiente de Negocio (ID.AN)	ID.AN-2. El lugar que ocupa la organización en la infraestructura crítica y en su sector de industria se encuentra identificado y comunicado.		
Identificar	Ambiente de Negocio (ID.AN)	ID.AN-3. Se establecen y se comunican las prioridades para la misión de la organización, sus objetivos y actividades.		

Identificar	Ambiente de Negocio (ID.AN)	ID.AN-4. Se definen las dependencias y funciones críticas para la entrega de los servicios críticos.		
Identificar	Ambiente de Negocio (ID.AN)	ID.AN-5. Se establecen requisitos de resiliencia para soportar la entrega de servicios críticos.		
Identificar	Gobernanza (ID.GO)	ID.GO-1. La política de seguridad de la información se encuentra establecida.		
Identificar	Gobernanza (ID.GO)	ID.GO-2. Los roles y las responsabilidades de la seguridad de la información están coordinados y alineados con roles internos y socios externos.		
Identificar	Gobernanza (ID.GO)	ID.GO-3. Los requisitos legales y regulatorios sobre la ciberseguridad, incluyendo las obligaciones de privacidad, son comprendidos y se gestionan.		
Identificar	Gobernanza (ID.GO)	ID.GO-4. Construcción de procesos de gobernanza y administración de riesgos dirigidos a atender los problemas de ciberseguridad.		
Identificar	Evaluación de Riesgos (ID.ER)	ID.ER-1. Se identifican y documentan las vulnerabilidades de los activos.		
Identificar	Evaluación de Riesgos (ID.ER)	ID.ER-2. Recepción de información sobre amenazas y vulnerabilidades por parte de grupos y fuentes especializadas.		
Identificar	Evaluación de Riesgos (ID.ER)	ID.ER-3. Identificación y documentación de las amenazas internas y externas.		
Identificar	Evaluación de Riesgos (ID.ER)	ID.ER-4. Identificación del impacto potencial en el negocio y la probabilidad de ocurrencia.		
Identificar	Evaluación de Riesgos (ID.ER)	ID.ER-5. Las amenazas, vulnerabilidades, probabilidad de ocurrencia e impactos, se utilizan para determinar el riesgo.		

Identificar	Evaluación de Riesgos (ID.ER)	ID.ER-6. Identificación y priorización de las respuestas a los riesgos.		
Identificar	ID.GR. Estrategia para la gestión de riesgos	ID.GR-1. Los procesos de gestión de riesgos se encuentran establecidos, gestionados y aprobados por todos los interesados de la organización.		
Identificar	ID.GR. Estrategia para la gestión de riesgos	ID.GR-2. Se determina y se expresa de forma clara la tolerancia al riesgo a nivel de toda la organización.		
Identificar	ID.GR. Estrategia para la gestión de riesgos	ID.GR-3. La tolerancia al riesgo de la organización es determinada por su rol y pertenencia a la infraestructura crítica y por la evaluación de riesgos específicos del sector al que pertenece.		
Identificar	Gestión de riesgos en la cadena de suministros (ID.CS)	ID.CS-1. Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.		
Identificar	Gestión de riesgos en la cadena de suministros (ID.CS)	ID.CS-2. Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.		
Identificar	Gestión de riesgos en la cadena de suministros (ID.CS)	ID.CS-3. Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.		
Identificar	Gestión de riesgos en la cadena de suministros (ID.CS)	ID.CS-4. Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.		
Identificar	Gestión de riesgos en la cadena de suministros (ID.CS)	ID.CS-5. Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.		

Proteger	Control de Acceso (PR.CA)	PR.CA-1. Las identidades y credenciales para usuarios y dispositivos autorizados son gestionadas.		
Proteger	Control de Acceso (PR.CA)	PR.CA-2. Se gestiona y protege el acceso físico a los activos.		
Proteger	Control de Acceso (PR.CA)	PR.CA-3. Gestión de acceso remoto.		
Proteger	Control de Acceso (PR.CA)	PR.CA-4. Gestión de permisos de acceso, incorporando los principios de menor privilegio y segregación de funciones.		
Proteger	Control de Acceso (PR.CA)	PR.CA-5. Protección de la integridad de la red incorporando segregación cuando es apropiado.		
Proteger	Control de Acceso (PR.CA)	PR.CA-6. Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.		
Proteger	Control de Acceso (PR.CA)	PR.CA-7. Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).		
Proteger	Concientización y Formación (PR.CF)	PR.CF-1. Todos los usuarios se encuentran entrenados e informados.		
Proteger	Concientización y Formación (PR.CF)	PR.CF-2. Los usuarios privilegiados comprenden sus roles y responsabilidades.		
Proteger	Concientización y Formación (PR.CF)	PR.CF-3. Interesados externos (proveedores, clientes, socios) comprenden sus roles y responsabilidades.		

Proteger	Concientización y Formación (PR.CF)	PR.CF-4. La gerencia ejecutiva comprende sus roles y responsabilidades.		
Proteger	Concientización y Formación (PR.CF)	PR.CF-5. El personal de seguridad física y de seguridad de la información comprende sus roles y responsabilidades.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-1. Los datos en reposo (inactivos) se encuentran protegidos.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-2. Los datos en tránsito se encuentran protegidos.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-3. Los activos se gestionan formalmente a lo largo de la eliminación, las transferencias y disposición.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-4. Se mantiene una adecuada capacidad para asegurar la disponibilidad.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-5. Se implementan medidas de protección contra fuga de datos.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-6. Se realizan chequeos de integridad para verificar software, firmware e integridad de la información.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-7. Los entornos de desarrollo y pruebas están separados del entorno de producción.		
Proteger	Seguridad de los datos (PR.SD)	PR.SD-8. Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-1. Existe una línea base de la configuración de los sistemas de información que es mantenida.		

Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-2. Se implementa el ciclo de vida de desarrollo para gestionar los sistemas.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-3. Existen procesos de gestión del cambio en las configuraciones.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-4. Se realizan y mantienen respaldos de la información y se testean periódicamente.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-5. Las políticas y reglamentos relacionados con el medio ambiente físico operativo se cumplen.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-6. Los datos son eliminados de acuerdo a las políticas de seguridad.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-7. Existe mejora continua de los procesos de protección.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-8. La eficacia de las tecnologías de protección se comparten con las partes apropiadas.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-9. Existen y se gestionan planes de respuesta a incidentes (respuesta a incidentes y continuidad del negocio) y planes de recuperación (recuperación de incidentes y recuperación de desastres).		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-10. Los planes de respuesta y recuperación se testean regularmente.		
Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-11. La ciberseguridad se encuentra incluida en las prácticas de RRHH.		

Proteger	Procesos y procedimientos para la protección de la información (PR.PI)	PR.PI-12. Existe un plan de gestión de vulnerabilidades.		
Proteger	PR.MA. Mantenimiento	PR.MA-1. El mantenimiento y las reparaciones de los activos de la organización se lleva a cabo y es registrado en forma oportuna con herramientas aprobadas y controladas.		
Proteger	PR.MA. Mantenimiento	PR.MA-2. El mantenimiento a distancia de los activos de la organización se aprueba, registra y lleva a cabo de forma tal que se impide el acceso no autorizado.		
Proteger	Tecnología de protección (PR.TP)	PR.TP-1. Los registros de auditoría (logs) se documentan, implementan y se revisan de conformidad con la política.		
Proteger	Tecnología de protección (PR.TP)	PR.TP-2. Los medios extraíbles se encuentran protegidos y su uso se encuentra restringido de acuerdo con las políticas.		
Proteger	Tecnología de protección (PR.TP)	PR.TP-3. El acceso a los sistemas y activos se controla incorporando el principio de menor privilegio.		
Proteger	Tecnología de protección (PR.TP)	PR.TP-4. Las redes y comunicaciones se encuentran protegidas.		
Proteger	Tecnología de protección (PR.TP)	PR.TP-5. Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o “hot swap”) para lograr los requisitos de resiliencia en situaciones normales y adversas.		
Detectar	Anomalías y eventos (DE.AE)	DE.AE-1. Se establece y gestiona una línea base de operaciones de red y flujos de datos esperados para usuarios y sistemas.		
Detectar	Anomalías y eventos (DE.AE)	DE.AE-2. Los eventos detectados son analizados para entender los objetivos y métodos de ataque.		
Detectar	Anomalías y eventos (DE.AE)	DE.AE-3. Los datos de los eventos se agrupan y correlacionan desde múltiples fuentes y sensores.		

Detectar	Anomalías y eventos (DE.AE)	DE.AE-4. Se determina el impacto de los eventos.		
Detectar	Anomalías y eventos (DE.AE)	DE.AE-5. Se establecen los umbrales de alerta de incidentes.		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-1. Se monitorea la red para detectar potenciales eventos de ciberseguridad.		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-2. Se monitorea el ambiente físico para detectar potenciales eventos de ciberseguridad.		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-3. Se monitorea la actividad del personal para detectar potenciales eventos de ciberseguridad.		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-4. Se detecta el código malicioso.		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-5. Se detecta el código móvil no autorizado		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-6. Se controla la actividad de los proveedores de servicios externos para detectar posibles eventos de ciberseguridad.		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-7. Se realiza monitoreo para personas, conexiones, dispositivos y software.		
Detectar	Monitoreo contínuo de la seguridad (DE.MC)	DE.MC-8. Se realizan escaneos de vulnerabilidades.		
Detectar	Procesos de detección (DE.PD)	DE.PD-1. Los roles y las responsabilidades de detección se encuentran definidos para asegurar responsabilidades.		

Detectar	Procesos de detección (DE.PD)	DE.PD-2. Las actividades de detección cumplen con todos los requisitos aplicables.		
Detectar	Procesos de detección (DE.PD)	DE.PD-3. Los procesos de detección son probados.		
Detectar	Procesos de detección (DE.PD)	DE.PD-4. La información de la detección de eventos es comunicada a las partes pertinentes.		
Detectar	Procesos de detección (DE.PD)	DE.PD-5. Los procesos de detección son mejorados continuamente.		
Responder	Planificación de la respuesta (RE.PR)	RE.PR-1. El plan de respuesta se ejecuta durante o luego de un evento.		
Responder	Comunicaciones (RE.CO)	RE.CO-1. El personal conoce sus roles y el orden de operaciones cuando es necesaria una respuesta.		
Responder	Comunicaciones (RE.CO)	RE.CO-2. Los eventos son reportados consistentemente con los criterios establecidos.		
Responder	Comunicaciones (RE.CO)	RE.CO-3. La información se comparte consistentemente con los planes de respuesta.		
Responder	Comunicaciones (RE.CO)	RE.CO-4. La coordinación con las partes interesadas se realiza consistentemente con los planes de respuesta.		
Responder	Comunicaciones (RE.CO)	RE.CO-5. Se realiza intercambio de información voluntaria con partes interesadas externas para alcanzar una conciencia de ciberseguridad más amplia.		
Responder	Análisis (RE.AN)	RE.AN-1. Se investigan las notificaciones de los sistemas de detección.		

Responder	Análisis (RE.AN)	RE.AN-2. El impacto del incidente es comprendido.		
Responder	Análisis (RE.AN)	RE.AN-3. Se realiza análisis forense.		
Responder	Análisis (RE.AN)	RE.AN-4. Los incidentes son categorizados consistentemente con los planes de respuesta.		
Responder	Análisis (RE.AN)	RE-AN-5. Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).		
Responder	Mitigación (RE.MI)	RE.MI-1. Se logra contener los incidentes.		
Responder	Mitigación (RE.MI)	RE.MI-2. Se logra mitigar los incidentes.		
Responder	Mitigación (RE.MI)	RE.MI-3. Las nuevas vulnerabilidades identificadas se mitigan o documentan como riesgos aceptados.		
Responder	Mejoras (RE.ME)	RE.ME-1. Los planes de respuesta incorporan lecciones aprendidas		
Responder	Mejoras (RE.ME)	RE.ME-2. Las estrategias de respuesta se actualizan.		
Recuperar	Planificación de la recuperación (RC.PR)	RC.PR-1. El plan de recuperación se ejecuta durante o luego de un evento.		
Recuperar	Mejoras (RC.ME)	RC.ME-1. Los planes de recuperación incorporan lecciones aprendidas		

Recuperar	Mejoras (RC.ME)	RC.ME-2 Las estrategias de recuperación se actualizan.		
Recuperar	Comunicaciones (RC.CO)	RC.CO-1. Se gestionan las relaciones públicas.		
Recuperar	Comunicaciones (RC.CO)	RC.CO-2. Se repara la reputación luego del evento.		
Recuperar	Comunicaciones (RC.CO)	RC.CO-3. Se comunican las actividades de recuperación a los interesados internos y a los equipos ejecutivos y de gestión.		