Tipos de Control					
	Categoría	Control	Descripción	Aplicabilidad	Justificación Es fundamental para definir un marco de seguridad alineado con los objetivos
	5.1	Políticas de seguridad de la información	Establecer políticas que definan cómo proteger la información.	APLICA	organizacionales.
5 Controler Occopiosionale	5.2	Roles y responsabilidades de seguridad de la información	Definir roles claros para gestionar la seguridad.	APLICA	Permite la asignación de responsabilidades específicas para una mejor gestión de riesgos.
	5.3	Separación de funciones	Evitar conflictos de interés mediante roles separados.	APLICA	Reduce el riesgo de fraude o acceso no autorizado al establecer funciones diferenciadas.
	5.4	Responsabilidades de gestión	Asegurar que los gestores asuman la seguridad.	APLICA	Los líderes deben garantizar el cumplimiento de las políticas de seguridad.
	5.5 5.6	Contacto con las autoridades Contacto con grupos de interés especial	Formalizar acuerdos con autoridades relevantes. Formalizar acuerdos de seguridad con terceros.	APLICA APLICA	Facilita la comunicación y cumplimiento con organismos reguladores. Ayuda a compartir información y meiores prácticas en ciberseguridad.
	5.7	Inteligencia de amenazas	Monitoreary responder a amenazas emergentes.	APLICA	Permite anticiparse a riesgos y mejorar la postura de seguridad.
	5.8	Seguridad de la información en la gestión de proyectos	Incorporar seguridad en la gestión de proyectos.	APLICA	Garantiza que los proyectos contemplen medidas de seguridad desde su inicio.
	5.9	Inventario de información y otros activos asociados	Identificar y proteger activos clave.	APLICA	Un inventario actualizado permite una mejor gestión y protección de activos críticos.
	5.10	Uso aceptable de la información y otros activos asociados	Definir reglas de uso permitido de activos.	APLICA	Evita mal uso de recursos y establece pautas claras para los usuarios.
	5.11	Devolución de activos	Garantizar la recuperación de activos al finalizar relaciones laborales.	APLICA	Reduce el riesgo de fuga de información o uso indebido de recursos tras la desvinculación de empleados.
	5.12	Clasificación de la información	Clasificar la información según su sensibilidad.	APLICA	Permite establecer controles adecuados según el nivel de criticidad de la información.
	5.13	Etiquetado de información	Etiquetar datos para indicar su clasificación.	APLICA APLICA	Facilita el manejo seguro de la información conforme a su clasificación.
	5.14	Transferencia de información Control de acceso	Proteger la información durante su transferencia. Restringir el acceso a la información según roles.	APLICA	Asegura la confidencialidad e integridad de la información transmitida. Minimiza riesgos al garantizar que solo usuarios autorizados accedan a la información.
	5.16	Gestión de identidad	Asegurar la gestión adecuada de identidades.	APLICA	Mejora la seguridad al controlar el acceso de los usuarios a los sistemas.
	5.17	Información de autenticación	Proteger las credenciales de autenticación.	APLICA	Reduce el riesgo de acceso no autorizado mediante credenciales seguras.
	5.18	Derechos de acceso	Asegurar que los accesos estén basados en necesidad.	APLICA	Limita la exposición de información solo a quienes lo requieran para sus funciones.
	5.19	Seguridad de la información en las relaciones con los proveedores	Gestionar riesgos en la colaboración con proveedores.	APLICA	Evita posibles brechas de seguridad derivadas de terceros.
5. Controles Organizacionales	5.20	Abordar la seguridad de la información en los acuerdos con	Protogra la información a la large de la cadana de coministra	APLICA	
	5.20	los proveedores	Proteger la información a lo largo de la cadena de suministro.	APLICA	Asegura que los proveedores cumplan con estándares de seguridad adecuados.
	5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Asegurar cambios seguros en los servicios de TI.	APLICA	Reduce riesgos asociados a terceros en la infraestructura tecnológica.
	5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	Supervisar y auditar cambios en los servicios contratados.	APLICA	Permite evaluar el impacto de los cambios en la seguridad de la información.
	5.23	Seguridad de la información para el uso de servicios en la nube	Proteger información almacenada o procesada en la nube.	APLICA	Reduce el riesgo de exposición o pérdida de datos en entornos cloud.
	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Prepararse para gestionar incidentes de seguridad.	APLICA	Garantiza una respuesta rápida y efectiva ante incidentes de seguridad.
	5.25	Evaluación y decisión sobre eventos de seguridad de la información	Evaluar eventos para decidir acciones apropiadas.	APLICA	Facilita la toma de decisiones basada en riesgos y amenazas identificadas.
	5.26	Respuesta a incidentes de seguridad de la información	Responder adecuadamente a incidentes de seguridad.	APLICA	Minimiza el impacto de incidentes mediante un plan de respuesta estructurado.
	5.27	Aprender de los incidentes de seguridad de la información	Usar lecciones aprendidas para prevenir futuros incidentes.	APLICA	Permite mejorar continuamente la postura de seguridad de la organización.
	5.28	Recolección de evidencia Seguridad de la información durante la interrupción	Garantizar la integridad de las evidencias recolectadas.	APLICA APLICA	Facilita investigaciones forenses y cumplimiento legal. Protege equipos contra accesos no autorizados o pérdidas.
	5.29	Seguridad de la información durante la interrupción Preparación de las TIC para la continuidad del negocio	Mantener la seguridad durante interrupciones operativas. Garantizar que los sistemas TIC soporten la continuidad del negocio.	APLICA	
					Asegura la protección de activos en ubicaciones externas.
	5.31	Requisitos legales, estatutarios, regulatorios y contractuales Declaraciones de propiedad intelectual	Cumplir con todas las leyes y regulaciones aplicables. Proteger la propiedad intelectual de la organización.	APLICA APLICA	Minimiza riesgos en la contratación de personal. Controla el acceso a información clasificada y crítica.
6. Controles de Personas	5.33	Protección de registros	Asegurar la protección de registros clave.	APLICA	Evita fugas de información tras la desvinculación de empleados.
	5.34	Privacidad y protección de la información identificable de las personas (PII)	Garantizar la protección de datos personales.	APLICA	Evita manipulaciones no autorizadas en el código fuente.
	5.35	Revisión independiente de la seguridad de la información Cumplimiento de políticas, normas y estándares de seguridad de la	Realizar auditorías independientes de seguridad.	APLICA	Evita interrupciones en la continuidad del negocio.
	5.36	información	Verificar que se cumplan las políticas establecidas.	APLICA	Elimina la recuperación de datos en equipos descartados.
	5.37 6.1	Procedimientos operativos documentados Chequeo	Documentar procedimientos para la gestión de seguridad. Verificar antecedentes antes de contratar.	APLICA APLICA	Evita fugas de información tras la desvinculación de empleados. Minimiza riesgos en la contratación de personal.
	6.2	Términos y condiciones de empleo	Establecer responsabilidades relacionadas con la seguridad en los contratos.	APLICA	Asegura la seguridad física de oficinas y salas de reunión.
	6.3	Concienciación, educación y capacitación en seguridad de la	Educar a los empleados sobre prácticas seguras.	APLICA	
	6.4	información Proceso disciplinario	Definir acciones ante incumplimientos de seguridad.	APLICA	Controla y protege el acceso a infraestructuras sensibles. Garantiza la disponibilidad de la información crítica.
	6.5	Responsabilidades después de la terminación o cambio de empleo	Proteger la información tras cambios laborales.	APLICA	Garantiza que los sistemas de almacenamiento sean confiables.
	6.6 6.7	Acuerdos de confidencialidad o de no divulgación	Formalizar acuerdos para proteger información confidencial.	APLICA	Limita accesos privilegiados para evitar abusos de autoridad.
	6.8	Trabajo remoto Informes de eventos de seguridad de la información	Garantizar la seguridad en entornos de trabajo remoto. Asegurar que los empleados reporten eventos de seguridad.	APLICA APLICA	Evita fugas de información tras la desvinculación de empleados. Refuerza los mecanismos de autenticación de usuarios.
7. Controles Físicos	7.1 7.2	Perimetro de seguridad física Entrada física	Establecer barreras físicas para proteger instalaciones. Controlar el acceso a instalaciones críticas.	APLICA APLICA	Protege equipos contra accesos no autorizados o pérdidas. Controla y protege el acceso a infraestructuras sensibles.
	7.3 7.4	Asegurar oficinas, salas e instalaciones Monitoreo de seguridad física	Proteger las áreas que contienen activos importantes. Implementar vigilancia para detectar amenazas físicas.	APLICA APLICA	Evita interrupciones en los sistemas de apoyo operativo. Permite detectar amenazas físicas en tiempo real.
	7.5	Protección contra amenazas físicas y ambientales	Reducir riesgos por eventos físicos y ambientales.	APLICA	Asegura que el mantenimiento de equipos no comprometa la seguridad.
	7.6 7.7	Trabajar en áreas seguras Escritorio despejado y pantalla despejada	Asegurar que áreas críticas estén protegidas.	APLICA	
	7.8		Prevenir exposición accidental de información.	APLICA	Asegura que la información esté protegida en todo momento. Evita fugas de información tras la desvinculación de empleados.
	7.9	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones	Proteger equipos contra daños o acceso no autorizado.		Evita fugas de información tras la desvinculación de empleados. Protege la infraestructura contra sabotajes o fallos físicos.
	7.10	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento	Proteger equipos contra daños o acceso no autorizado. Asegurar los activos en ubicaciones externas.	APLICA APLICA APLICA	Evita fugas de información tras la desvinculación de empleados. Protege la infraestructura contra sabotajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Mantiene configuraciones seguras en los sistemas de la empresa.
		Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones	Proteger equipos contra daños o acceso no autorizado.	APLICA APLICA APLICA	Evita fugas de información tras la desvinculación de empleados. Protege la infraestructura contra sabotajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada.
	7.10 7.11 7.12 7.13	Emplazamiento y protección de equipos Seguiridad de los activos fuera de las instalaciones Medios de almacenamiento Ubilidades de apoyo Seguiridad del declableado Mantenimiento de equipos	Proteger equipos contra daños o acceso no autorizado. Asegurar los activos en ubicaciones externas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad.	APLICA APLICA APLICA APLICA APLICA APLICA APLICA APLICA	Exita Tugas de información tras la desvinculación de empleados. Potolege la infraestructura contra sabotajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Mantiene configuraciones seguras en los sistemas de la empresa. Protege ecuipos contra accesso no autorizados o pérfeidas.
	7.10 7.11 7.12 7.13 7.14	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento Utilidades de apoyo Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos	Proteger equipos contra daños o acceso no autorizado. Asegurar los activos en ubicaciones externas. Asegurar que los sistemas de soporte sean confiables. Proteger el cabieso contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que los datos sean eliminados de equipos desechados.	APLICA	Exita tugas de información tras la deveniculación de empleados. Protege la infraericultura contra sabrejas o fallos físicos. Facilita la continuidad de processos mediante documentación adecuada. Mamben confliguraciones seguas en los sistemas de la empresa. Protege equipos contra accesso no autorizados o perdidas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de disos sensibles. Exita exposiciones accidentales de datos sensibles.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Utilidades de appoyo Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado	Proteger equipos contra daños o acceso no autorizado. Asegurar los activos en ubicaciones externas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad.	APLICA	Exita Jugas de Información tras la develinculación de empleados. Protege la infracturular contra sabrejas o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Mantiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos no autorizados o perididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de disos sensibles. Evita exposiciones accidentales de datos sensibles. Protege equipos contra accesos no autorizados o péridida. Protege equipos contra accesos no autorizados o pérididas.
	7.10 7.11 7.12 7.13 7.14	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento Utilidades de apopo Seguridad del cableado Adartenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso de privilegiado	Proteger equipos contra daños a acceso na autorizado. Asegurar los activos en ubicaciones externas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento ne comprometa la seguridad. Carantizar que los datos sean eliminatos de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios cievados. Controlar quida preda exceder a quel información.	APLICA	Exita Tugas de Información tras la desvinculación de empleados. Protege la infraestructura contra subotajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Mantiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos no autorizados o perfidos. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accesos no autorizados o pérdidas. Protege equipos contra accesos no autorizados o pérdidas. Protege equipos contra accesos no autorizados so pérdidas.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento Utilidades de apoyo Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso a la información Acceso al código fuente Actenticación segura o	Proteger equipos contra daños a acceso na autorizado. Asegurar cas activos en ubicaciones externas. Asegurar que los sistemas de soporte sana conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento na compomenta la seguridad. Garantizar que lo datos sean eliminados de equipos desenhados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quicha pueda ecoder a que información. Proteger al acceso al código tuente de sistemas. Implementar mecanismos fuetes de autentacción.	APLICA	Exita Tugas de Información tras la devoliculación de empleados. Protege la infraestrutura contra sabotajes o fallos físicos. Facilità la continuidad de processos mediante documentación adecuada. Mantiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesso na advortados o pérdidas. Facilità la continuidad de processos mediante documentación adecuada. Exita exposiciones accidentales de dosos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accessos na autorizados o pérdidas. Protege equipos contra accessos no autorizados o pérdidas. Protege dispositivos de usuario contra amenazas cibernéticas. Permete la identificación de vulterabilidades mediante autoritas. Exita mangulaciones no autorizados en el código fuente. Protege información sensible mediante acuerdos de confidencialidad.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento Utilidades de apoyo Seguridad del cabileado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto finat de usuario Derechos de acceso de privilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura o reutilización de operación de Acceso al Codigo fuente Autenticación segura o Gestión de capacidad Protección contra malware	Proteger equipos contra daños a acceso na autorizado. Asegurar cue los activos en ublicaciones externas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que lo dados sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con pritegios elevados. Comitoral quide pueda ecoder a que información. Proteger al acceso al código breinte de sistemas. Implementar mecanismos fuetes de autenticación. Proteger contraseñas y otros datos de autenticación. Proteger contraseñas y otros datos de autenticación.	APLICA	Exita tugas de información tras la devoliculación de empleados. Protegla la infraeturbura contra sabularjos o fallos físicos. Facilità la continuidad de procesos mediante documentación adecuada. Mantiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos na autorizados peridida. Facilità la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de discos semisibles. Exita exposiciones accidentales de datos semisibles. Protege equipos contra accesos na autorizados o pérididas. Protege equipos contra accesos na autorizados o pérididas. Permite la identificación de vutnerabilidades mediante auditorias. Exita manipulaciones no autorizados en el código fuente. Protege información sensibles mediante acuerdos de confidencialidad. Protege información sensibles mediante acuerdos de confidencialidad. Protege información sensibles mediante acuerdos de confidencialidad.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Utilidades de apoyo Seguridad de le de cableado Martenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura o Gestión de cogura	Proteger equipos contra daños o acceso no autorizado. Asegurar los activos en ubicaciones externas. Asegurar que los sistemas de soporte sean conflables. Proteger el cabileado contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que el mantenimiento no comprometa la seguridad. Garantizar que el mantenimiento no comprometa la seguridad. Carantizar que el os datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quién puede acceder a que información. Proteger el accesos al código fuente de sistemas. Implementar mecanismos fuertes de autenticación. Proteger contraselarsy stores datos de suenticación.	APLICA	Exita Jugas de Información tera la desvinculación de empleados. Protege la Infraericultura contra salvejas o fallos fisicos. Facilita la continuidad de processos mediante documentación adocuado. Hantinea configuiaciones segúras en los sistemas de la empresa. Protege equipos contra accessos no autorizados opéridas. Exita la continuidad de processos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Evita exposiciones accidentales de datos sensibles. Protege equipos contra accessos no autorizados o pérididas. Protege equipos contra accessos no autorizados o pérididas. Permite la identificación de vulnerabilidades mediante auditorias. Evita manipulaciones no autorizados en el código fuente. Protege información se nosibile mediante auditorias. Protege información sensibile mediante acuerdos de confidencialidad. Protege información sensibile mediante acuerdos de confidencialidad.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.9 8.10	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento Utilidades de apopo Seguridad de la papo Seguridad de la cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura Gestión de capacidad Protección contra malvare Gestión de de universabilidades técnicas Gestión de la configuración Eliminación de litormación	Proteger equipose contra daños o access on autorizado. Asegurar que los sistemas de soporte sean conflables. Proteger et cabiles de contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que el mantenimiento no comprometa la seguridad. Garantizar que el mantenimiento no comprometa la seguridad. Proteger los datos sean el liminados de equipos desenhados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quiel puede acceder a que información. Proteger el acceso al código luente de sistemas. Implementar macenimos buteris de autenticación. Peroteger contraerias y otros datos de autenticación. Usar soluciones para prevenir y detectar maluvare. dentricar y compre vulnerabilidades ticnicas. Asegurar que los sistemas estima configurados correctamente. Asegurar que los sistemas sestemas formas segura.	APLICA	Exit sugas de información na las devinculación de empleados. Protege la infractulura contra salvajes o fallos fisicos. Facilita la continuidad de procesos mediante documentación adecuada. Mantiene configuiaciones segúras en los sistemas de la empresa. Protege equipos contra accesos no autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accesos no autorizados o pérididas. Protege equipos contra accesos no autorizados o pérididas. Protege finado en la usua contra amenzara cibernéficas. Permite la identificación de vulvirazibilidades mediante autoriorias. Exita manipulaciones no autorizados en el código fuente. Protege información sensible mediante acuerdos de confidencialidad. Protege información sensible mediante acuerdos de confidencialidad. Define responsabilidades circas en termas de seguridad. Define responsabilidades circas en termas de seguridad. Controla y protege el acceso a infraertururas sensibles. Exita interrupciones en las continuada del negocio.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.11	Emplazamiento y protección de equipos Seguridad de las activos fuera de las instalaciones Medios de almacenamiento Utilidades de apopo Seguridad de la papo Seguridad de la cableado Mantenimiento de equipos Eliminación seguria o reutifización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura Gestión de capacidad Protección contra malvare Gestión de de la configuración Eliminación de información	Proteger equipos contra daños a acceso na autorizado. Asegurar cos citos en ubicaciones esternas. Asegurar que los sistemas de soporte sean conflables. Proteger el cabiles da contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Asegurar que el mantenimiento no comprometa la seguridad. Garmitizar que el mantenimiento no comprometa la seguridad. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quiel puede acceder a que información. Proteger el acceso al código buente de sistemas implementar meanismos fuertes de autenticación. Proteger contraeñas y otros datos de autenticación. Proteger contraeñas y otros datos de autenticación. Lasra soluciones para prevenir y detectar maivare. Identificar y corregir vulnerabilidades técnicas. Asegurar que los distemas están configurados correctamente, Asegurar que los distemas están configurados correctamente, Reguar que los distemas están de alumacenamiento. Implementar medios para prevenir y lárecta, se información.	APLICA	Exit sugas de información tera la deveniculación de empleados. Protege la infractular acortra salvajes o fallos fisicos. Facilita la continuidad de procesos mediante documentación adecuada. Mantiena configuiaciones segúras en los sistemas de la empresa. Protege equipos contra accesos no autorizados o pérididas. Exital su continuidad de proceso mediante documentación adecuada. Exital su continuidad de proceso mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accesos no autorizados o pérididas. Protege equipos contra accesos no autorizados o perididas. Pemeta la identificación de vulnerabilidades mediante autoriarias. Exita manipulaciones no autorizados en el código fuente. Protege información sensible mediante acuendos de confidencialidad. Define responsabilidades claras en temas de seguridad. Controla y protege el acceso a infraestruturas sensibles. Exita interrupciones en la continuidad del negocio. Previene incidentes de seguridad do incumplimiento de normas. Asegura que el mantenimiento de equipos no comprometa la seguridad.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildiades de apoyo Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso de riprivilegiado Restricción de acceso a la información Acceso al código fuerte Autenticación segura Gestión de canacidad Protección contra malvara Gestión de canacidad Gestión de canendidades tercicas Gestión de sus de canendidades tercicas Gestión de sus gestión de la configuración Ermas caramiento de datos revocción de la gas de ators Copia de seguridad de la información	Proteger equipos contra daños o acceso no autorizado. Asgurar que los sistemas de soporte sean conflables. Proteger el cableado contra amipulaciones. Asgurar que los sistemas de soporte sean conflables. Proteger el cableado contra amipulaciones. Asgurar que le mantenimiento no comprometa la seguridad. Garantizar que los datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por unuanios finales. Limitar accesos com privilegios elevados. Controlar quién puede acceder a que información. Proteger la carcea do cidigo fueme de sistemas. Implementar mecanismos fuertes de autenticación. Porteger contraciado y otros datos de unidenticación. Usar soluciones para prevenir y detectar malware. Hentificar y comegi vunicabilidades térciciaes. Asegurar que los sistemas estim configurados correctamente. Asegurar que los sistemas estim configurados correctamente. Proteger los datos sean eliminados de forma segura. Proteger los datos sean eliminados de forma segura. Proteger los datos suantes su alumaconamiento. Implementar medidas para prevenir y alumaconamiento. Implementar medidas para prevenir programa de información. Garantizar las ecoperación de latos en caso de péridida.	APLICA	Exita Tugas de Información tras la develinculación de empleados. Protege la infraecturura contra saburajos o fallos físicos. Sacilita la continuidad de processos mediante documentación adecuada. Mamben confliguraciones seguras en los sidemais de la empresa. Protege equipos contra accesso na outorizados perdidas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accesso no autorizados o pérdidas. Protege equipos contra accesso no autorizados o pérdidas. Permite la identificación de vulnerabilidades mediante autitorias. Exita manipulaciones no autorizados en cicódigo fuente. Protege información sensible mediante acuentos de confidencialidad. Protege información sensible mediante acuentos de confidencialidad. Define responsabilidades clara en temas de seguridad. Controla y protege el acceso a lifiaestructuras sensibles. Exita interrucciones en la confidencialidad. Previene incidentes de seguridad por incumplimiento de nomas. Asegura que el materimiento de equipos no comprometa la seguridad.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildidades de apoyo Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Oispositivos de punto final de usuario Derechos de accesso de privilegiado Restricción de accesso a la información Accesso al códiglo tuente Actenticación segura Gestión de capacidad Protección contra malware Gestión de evulnerabilidades técnicas Gestión de vulnerabilidades técnicas Gestión de la configuración Eliminación de información Protección contri de dato Protección de lugia de datos Redundancia de las instalaciones de procesamiento de información Redundancia de las instalaciones de procesamiento de información	Proteger equipos contra daños o acceso no autorizado. Asegurar que los cárbos en utilizaciones externas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amapulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que ols datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controtar quinh puede acceder a que derindimación. Proteger el acceso al código buente de sistemas. Implementar mecanismos betres de auterificación. Proteger contraserlas y otros datos de auterificación. Proteger contraserlas y otros datos de auterificación. Sar soluciones para prevenir y detectar malware. Identificar y corregir vulnerabilidades tecinicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos durantes su almo-amariento. Implementar medidas para prevenir y detecta.	APLICA	Exita hugas de información tras la deveniculación de empleados. Protege la infraericultura contra sabrejas o fallos físicos. Facilita la continuidad de processos mediante documentación adecuada. Anatiene confligiraciones seguras en los sistemas de la empresa. Protege equipos contra accesso no autorizados o perfedidas. Facilita la continuidad de processos mediante documentación adecuada. Evita exposiciones accidentales de datos sensibles. Evita exposiciones accidentales de datos sensibles. Protege equipos contra accessos no autorizados o perfedidas. Protege equipos contra accessos no autorizados o perfedidas. Perente la identificación de vulnerabilidades mediante autificación. Evita exposiciones no autorizados en el código fuente. Protege información sensible mediante acuerdos de confidencialidad. Protege información sensible mediante acuerdos de confidencialidad. Define responsabilidades claras en temas de seguridad. Controla y protege el accesos a infaevruturas sensibles. Evita interrupciones en la continuidad del negocio. Previene incidentes de seguridad do incumplimiento de nomas. Asegura que el matemiento de equipos no comprometa la separidad. Facilita la identificación y esquesta ante incidentes de seguridad. Centralización y elementalización en la contra de que sea en explotadas. Previene indecciones por mativare y ataques de virus.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.14 8.15 8.16 8.15 8.16 8.11 8.12 8.13	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildidades de apoyo Seguridad del cableado Mantenimiento de equipos Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto fina de usuario Derechos de accesso de privilegiado Restricción de accesso a la información Accessa al código fueries Autenticación segura Gestión de capacidad Protección contra malvarar Gestión de la configuración Eliminación de información Eliminación de información Eliminación de información Eliminación de información Frotección de la ga de datos Protección de la ga de datos Redundancia de las instalaciones de procesamiento de información Redundancia de las instalaciones de procesamiento de información Inicio sesión	Proteger equipos contra daños a acceso na autorizado. Asegurar los activos en ubicaciones sistemas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amajoulaciones. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amajoulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que los datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos com privilegios elevados. Controlar quide paede acceder a que información. Proteger a dacesos al código benefo de sistemas. Implementar mecanismos benes de acuericación. Proteger contraserias y otros datos de autenificación. Proteger contraserias y otros datos de autenificación. Ales soluciones para prevenir y detectorica. Asegurar que los datos sean eliminados de forma segura. Proteger los datos durantes su alimicanamiento. Implementar mecidas para prevenir pagas de información. Garantizar la recupicación de datos es aces de peridido. Implementar medidas para prevenir huga de información. Garantizar la recupicación de datos es aces de peridido. Implementar recurdancia para mayor disponibilidad. Registrar eventos relevantes en los sistemas. Montorezar sistemas para detectar anomalias.	APLICA AP	Exita Jugas de Información tras la deviniculación de empleados. Protege la infraericular contra sabrejas o fallos físicos. Facilita la continuidad de processos mediante documentación adecuada. Nantiene confliguraciones seguras en los sistemas de la empresa. Protege equipos contra accessos no autorizados o perfedidas. Facilita la continuidad de processos mediante documentación adecuada. Evita exposiciones accidentales del distos sembiles. Evita exposiciones accidentales del datos sembiles. Evita exposiciones accidentales del datos sembiles. Protege equipos contra accessos no autorizados o pérididas. Protege equipos contra accessos no autorizados o pérididas. Perente la identificación de vulnerabilidades mediante auditorias. Evita manipulaciones no autorizados en el código fuente. Protege información sensible mediante acuerdos de confidencialidad. Define responsabilidades clara sen temas de seguridad. Controla y protege el accesos a infraestruturas sensibles. Evita interrupciones en la continuidad del negoto. Prevelene incidentes de seguridad por incumplimiento de nomas. Asegura que el mantenimiento de ecuipos no comprometa la seguridad. Facilita la identificación y espuesta amé nicidentes de seguridad. Finellita la identificación y espuesta amé nicidentes de seguridad. Previene incidentes de seguridad por incumplimiento de nomas. Asegura que el mantenimiento de ecuipos no comprometa la seguridad. Previene incidentes de seguridad por incumplimiento de nomas. Asegura que el mantenimiento de ecuipos no comprometa la seguridad. Finellita la identificación y respuesta amé nicidentes de seguridad. Finellita la identificación y espuesta amé nicidentes de seguridad.
	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.11 8.12 8.13 8.14 8.15	Emplazamiento y protección de equipos Seguridad de los activos fuera de la instalaciones Medios de almacenamiento Wildiades de apoyo Seguridad del cabieado Nattenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura Gestión de capacidad Protección contra malware Gestión de capacidad Gestión de la configuración Eliminación de vinterabilidades técnicas Gestión de la configuración Eliminación de información Eliminación de información Eliminación de información Copia de seguridad de la información Redundancia de las instalaciones de procesamiento de información Inicio sesión	Proteger equipos contra daños a acceso na autorizado. Asegurar los activos en ubicaciones externas. Asegurar que los sistemas de soporte san conflables. Proteger el cableado contra manipidaciones. Asegurar que los sistemas de soporte san conflables. Proteger el cableado contra manipidaciones. Asegurar que el mantenimiento ne comprometa la seguridad. Garantizar que lo datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar guide puede acceder a quel información. Proteger el acceso al código fuente de sistemas. Implementar mecanismos fuente de autenticación. Usar soluciones para prevenir y detectar malware. Identificar y corregir vulnerabilidades técnicas. Asegurar que los datos sean eliminados de forma segura. Proteger con la dotos sean eliminados de forma segura. Proteger con datos sean eliminados de forma segura. Proteger datos datos datos sean eliminados de forma segura. Proteger los datos dunante su almacenamiento. Implementar medidas para prevent rigas de información. Garantizar la recuperación de datos en caso de petidida. Implementar emedidas para prevent rigas de información. Garantizar la recuperación de datos en caso de petidida. Implementar emedidas para prevent rigos de información. Garantizar la recuperación de datos en caso de petidida.	APLICA	Exit sugas de información na sia desvinculación de empleados. Protege la infractular acortra salvajes o fallos físicos. Facilita la continuidad de proceso mediante documentación adecuada. Martiene configuraciones seguiras en los sistemas de la empresa. Protege equipos contra accesos no autorizados o pérididas. Facilita la continuidad de proceso mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accesos no autorizados o pérididas. Protege edispositores de usuario contra amenazas cibernéficas. Protege objectivas de usuario contra amenazas cibernéficas. Protege información sensible mediante autoriados o pérididas. Protege información sensible mediante acuerdos de confidencialidad. Protege información sensible mediante acuerdos de confidencialidad. Define responsabilidades citars en ternas de seguridad. Controla y protege el acceso a infraestruturas sensibles. Evita interrupciones en la continuidad del negocio. Previene incidentes de seguridad do incumplimiento de normas. Asegura que el mantenimiento de equipos no componeta la seguridad. Controla y protege se desceso a infraestruturas sensibles. Evita interrupciones en la continuidad del negocio. Previene incidentes des deguridads do micrumplimiento de normas. Asegura que el mantenimiento de equipos no componeta la seguridad. Identifica y confige vulnerabilidades antes de que sean explotadas.
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.16 8.16 8.16 8.16 8.16 8.16 8.16	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento Utilidades de apoyo Seguridad del cabileado Nesterio de equipos Seguridad del cabileado Nantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de pivilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura o reutilización de capacidad Protección contra malware Gestión de capacidad Protección contra malware Gestión de vulnerabilidades técnicas Gestión de los configuración Eliminación de información Eliminación de información Protección contra de da toto Copia de seguridad de la información Inicio sesión Actividades de segurimiento Sincronación de retejo	Proteger equipos contra daños a acceso na autorizado. Asegurar cos activos en ubicaciones externas. Asegurar los cistemas de sopore sen contables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento ne comprometa la seguridad. Carantzar que los datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quiel puede acceder a quel información. Proteger el acceso al código fuente de sistemas. Imitar accesos con privilegios elevados. Controlar quiel puede acceder a quel información. Proteger el acceso al código fuente de sistemas. Implementar mecianismos fuetes de auterticación. Proteger contraseñas y otros datos de auterticación. Proteger contraseñas y otros datos de auterticación. Senguar que los datos sean eliminados de forma segura. Proteger contraseñas protes de infirmación. Garantizar la recuperación de datos en caso de péridida. Implementar medidas para prevenir fugas de información. Garantizar la recuperación de datos en caso de péridida. Implementar reedidas para prevenir fugas de información. Garantizar la recuperación de datos en caso de péridida. Implementar reedidas para prevenir fugas de información. Garantizar la recuperación de datos en caso de péridida. Implementar reedidas para prevenir fugas de información. Garantizar se recuperación de datos en caso de péridida. Implementar reedidas para prevenir fugas de información. Garantizar se recuperación de datos en caso de péridida. Minglementar reedidas para prevenir fugas de información. Garantizar se recuperación de datos en caso de péridida. Minglementar reedidas para prevenir fugas de información. Garantizar se recuperación de datos en caso de péridida. Monitores resistemas para detectar anomalias.	APPLICA	Exit sugas de información na las devinculación de empleados. Protege la infractular acortra salvajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguiras en los sistemas de la empresa. Protege equipos contra accesos no autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Potege eguipos contra accesos no autorizados o pérididas. Potege dispositivos de usuario corrora amenazar ciberneticas. Potege dispositivos de usuario corrora amenazar ciberneticas. Potege información accidentales en datos sensibles. Protege información en entibe mediante acude o de confidencialidad. Protege información sensible mediante acude o de confidencialidad. Define responsabilidades citar en ternas de seguridad. Controla y protege el acceso a infraestruturas sensibles. Evia interrupciones en la continuidad del regocio. Controla y rotege el acceso a infraestruturas sensibles. Evia interrupciones en la continuidad del regocio. Sensibilidades citars en ternas de seguridad o normanis. Asegura que el mantenimiento de equipos no comprometa la sepuridad. Controla y rotege se desego a infraestruturas sensibles. Evia interrupciones en la continuidad del regocio. Jerevice infecciones por malware y ataques de virus. Previene infecciones por malware y ataques de virus. Protege eguipos contra accesso no autorizados o peridida. Garantiza que los sistemas de almacenamiento sean conflables. Facilita la identifica de susuario contra amenazas cibernéticas. Facilita la continuidad de procesos mediante documentación adecuada.
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.16 8.16 8.17 8.18 8.19 8.10 8.11 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.19 8.20	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de almacenamiento Utilidades de apoyo Seguridad del cabileado Nantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto finat de usuario Derechos de acceso de privelguidad Restricción de acceso a la información Acceso al código fuente Autenticación segura o reutilización de reutilización de capacidad Protección contra malvare Gestión de capacidad Protección contra malvare Gestión de vulnerabilidades técnicas Gestión de la configuración Eliminación de información Eliminación de información Redundancia del sa instalaciones de procesamiento de información Redundancia de las instalaciones de procesamiento de información Inicio sesión Redundancia de las instalaciones de procesamiento de información Inicio sesión Redundancia de las instalaciones de procesamiento de información Inicio sesión Redundancia de las instalaciones de procesamiento de información Inicio sesión Redundancia de las instalaciones de procesamiento de información Inicio sesión Restriction de reusión de religio de sistemas operativos Seguridad de la red	Proteger equiposc contra daños a acceso na autorizado. Asegurar que los activos en ubicaciones externas. Asegurar que los sistemas de soporte sana conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento na compometa la seguridad. Garantizar que lo datos sean eliminado de equipos desenhados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quida pueda ecoder a qui información. Proteger el acceso al código tuente de sistemas. Implementar mecanismos fuetes de autenticación. Proteger outraseñas y otros datos de autenticación. Proteger contraseñas y otros datos de autenticación. Bara soluciones para prevenir y detectar malware. Identificar y corregir vulnerabilidades técnicas. Asegurar que los datos sean eliminados de forma segura. Proteger contraseñas portes dariantes us almocamamiento. Implementar medidas para prevenir y dates de información. Sarantizar la recuperación de datos en caso de pérdida. Implementar endundancia para mayor disponibilidad. Registrar eventos relevantes en los sistemas. Montroura sistemas para detectur anomalías. Asegurar que los cistes de los sistemas estes inicronizados. Controlar el uso de herramientas con privilegios elevados. Proteger los datos eles de los sistemas sets nicronizados. Controlar el uso de herramientas con privilegios elevados.	APPLICA APPLIC	Exit sugas de información na sia desvinculación de empleados. Protege la infractular acortra salvajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguiras en los sistemas de la empresa. Protege equipos contra accesos na autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Potege dispositivos de usuario contra amenazas ciberneticas. Potege dispositivos de usuario contra amenazas ciberneticas. Potege dispositivos de usuario contra amenazas ciberneticas. Potege información sensible mediante acuerdos de confidencialidad. Protege información sensible mediante acuerdos de confidencialidad. Define responsabilidades citara en ternas de seguridad. Controla y protege el acceso a infraestructuras sensibles. Exita interrupciones en la continuidad del regocio. Previene incidentes de seguridad do rimorpionio incumplimiento de normas. Asegura que el mantenimiento de equipos no comprometa la separidad. Controla y protege se desegua el mantenimiento de equipos no comprometa la separidad. Controla y protege so espuridad por incumplimiento de normas. Asegura que el mantenimiento de equipos no comprometa la separidad. Joen de la continuidad de proceso mediante documentación adecuadas. Previene infecciones por malware y atraques de virus. Proviene infecciones por malware y atraques de virus. Previene infecciones por malware y atraques de virus. Previene infecciones por malware y atraques de virus. Previene infecciones por malware y atraques de virus.
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.19 8.19 8.10 8.11 8.11 8.12 8.14 8.15 8.16 8.17 8.18 8.18 8.18 8.18 8.18 8.18 8.18	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Utilidades de apoyo Seguridad del cabileado Nantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso de privilegiado Restricción de acceso a la información Acceso al código luente Autenticación sesgura Gestión de capacidad Protección contra malware Gestión de capacidad Protección contra malware Gestión de configuración Eliminación de información Eliminación de información Redundancia del las instalaciones de procesamiento de información Redundancia de las instalaciones de procesamiento de información Redundancia de las instalaciones de procesamiento de información Inicio sessión Actividades de seguimiento Sincronización de retiol Uso de programas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la red Seguridad de las servicios de red Seguridad de la red Seguridad de las servicios de red	Proteger equipos contra daños a acceso na autorizado. Asegurar que los activos en ubicaciones externas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que lo datos sean eliminados de equipos desenhados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quiden pueda ecoder a que información. Proteger al acceso al código treme de sistemas. Implementar mecanismos fuentes de autenticación. Proteger al acceso al código treme de sistemas. Implementar mecanismos fuentes de autenticación. Proteger contraseñas y otros datos de autenticación. Bars soluciones para prevenir y detectar maiware. Identificar y cornegir vulnerabilidades técnicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos durantes su almocanismo. Implementar mecidas para prevenir y detactos de peridida. Implementar recurdunáncia para mayor disponibilidad. Registrar eventos relevantes en los sistemas. Monitorear sistemas para detectar anomalias. Acequar que los relevantes en los sistemas. Monitorear sistemas para detectar anomalias. Acequar que los relevantes en los sistemas. Monitorear sistemas para detectar anomalias. Acequar que los relevantes en los sistemas. Monitorear sistemas para detectar anomalias. Acequar que los relevas de los sistemas as este nos influentes. Supervisar redes para fuentes en privelegos elevados. Proteger los datos portevos de relevantes en los sistemas. Supervisar redes para detectar problemas. Supervisar redes para detectar problemas. Supervisar redes para detector de incidentes.	APPLICA APPLIC	Exit sugas de información na sia desvinculación de empleados. Protege la infractular acortra salvajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguiras en los sistemas de la empresa. Protege equipos contra accesos na autorizados o pérdidas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege dispositiones accidentales de datos sensibles. Protege dispositiones de usuario contra amenzara ciberneticas. Exita exposiciones na cacidentales de datos sensibles. Protege dispositiones de usuario contra amenzara ciberneticas. Exita exposiciones na cacidentales de datos sensibles. Protege información sensible mediante acuerdos de confidencialidad. Define responsabilidades cibans en termas de seguridad. Controla y protege el acceso a infraestructuras sensibles. Exita entrupciones en la continuidad del negocio. Previene incidente de securidad por incumplimiento de normas. Asegura que el mantenimiento de equipos no comprometa la seguridad. Controla y protege de securidad por incumplimiento de normas. Asegura que el mantenimiento de equipos no comprometa la seguridad. Certa interrupciones en la continuidad del negocio. Previene indecciones por malwar y ataques de virus. Previene infecciones por malwar y ataques de virus. Previene infecciones por malwar y ataques de virus. Extra menipulaciones no autorizados en el código fouente. Previene infecciones por malwar y ataques de virus. Extra menipulaciones no autorizados en el código fouente. Previene infecciones por malwar y ataques de virus. Extra menipulaciones no autorizados en el código fouente.
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.10 8.10 8.11 8.12 8.11 8.12 8.13 8.14	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildidades de apoyo Seguridad del cableado Mantenimiento de equipos Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Describos de accesso de privilegiado Restricción de accesso a la información Accessa al código fuerier Autenticación segura Gestión de accesso a la información Accessa describos de entre describos de seguina de la configuración Eliminación de información Eliminación de información Eliminación de información Redundancia del las instalaciones de procesamiento de información Inicio sesión Redundancia de las instalaciones de procesamiento de información Inicio sesión Actividades de seguimiento Sincontazción de reloi Uso de programas de utilicia di privilegiados Instalación de software en sistemas operativos Seguridad de la red Seguridad de la red Seguridad de servicios de red	Proteger equipos contra daños o acceso no autorizado. Asegurar que los estiemas de soporte sean conflables. Proteger el cableado contra manipulaciones. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra manipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que los datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con privilegios elevados. Controlar quide puede acceder a que información. Proteger a daceso al código benito de sistemas. Implementar mecanismos benetes de audenticación. Proteger contraserlas y otros datos de autenticación. Proteger contraserlas y otros datos de autenticación. Senagurar que los sistemas sestem configurados correctamente. Asegurar que los datos sean eliminados de forma segura. Proteger los datos sucentes sestemas estemas estemas estemas configurados correctamente. Asegurar que los datos sean eliminados de forma segura. Proteger los datos sucentes sestemas estema configurados correctamente. Asegurar que los datos sean eliminados de forma segura. Proteger los datos para prevenir fugas de información. Garantizar la recupicación de datos es nas de peridido. Implementar medidas para prevenir fugas de información. Registrar eventos relevantes en los sistemas. Asegurar que los relevantes en los sistemas. Proteger los sistemas operativos de riesgos a la instalación de software. Implementar medidas para protegor dedes.	APLICA	Exita Jugas de Información tra sia desvinculación de empleados. Protege la infracturular contra salvajes o fallos fisicos. Facilita la continuidad de procesos mediante documentación adocuado. Mantiene configuiaciones segizar se inos sistemas de la empresa. Protege equipos contra accesos no autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Evita exposiciones accidentales ed datos sensibles. Evita exposiciones accidentales de datos sensibles. Evita exposiciones accidentales de datos sensibles. Protege equipos contra accesos no autorizados o pérididas. Protege equipos contra accesos no autorizados o pérididas. Protege equipos contra accesos no autorizados o pérididas. Permite la identificación de vulnerabilidades mediante auditorias. Evita manipulaciones no autorizados en el códigio fuente. Protege información sensible mediante acuerdos de confidencialidad. Permite la identificación de vulnerabilidades mediante auditorias. Evita interrupciones en las continuidad del negocio. Previene incidentes de acceso a infraestruturas sensibles. Evita interrupciones en las continuidad del negocio. Previene incidentes de seguridad no incumplimiento de normas. Asegura que el mantenimiento de equipos no comprometa la seguridad. Garintiza que les discosos promitantes de que sean explotadas. Previene incidentes de seguridad no incumplimiento de normas. Asegura que el mantenimiento de soupos no comprometa la seguridad. Garintiza que les sistemas de almacenamiento sean conflables. Previene incidentes de contra accessos no autorizados o pérididas. Carnatiza que les assemas de miscone en el códigio fuente.
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.8 8.9 8.1 8.1 8.1 8.1 8.1 8.1 8.1 8.1 8.1 8.1	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildidades de apoyo Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción do acceso a la información Acceso al código fuente Autenticación segura Gestión de caceso a la información Acceso al código fuente Autenticación segura Gestión de canadidad Protección do acceso a la información Cestión de canadidad Protección contra malvara Gestión de canadidad Protección contra malvara Gestión de susparidad de la información Eliminación de información Eliminación de información Redundancia de las instalaciones de procesamiento de información incicio sessión Actividades de seguimiento Siniconiación de software en sistemas operativos Seguridad de la relo Los de prociamas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la relo Los de prociamas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la relo Los de recipionaria Listitudo de los servicios de red Segregación de redes Filtrado web Uso de criptionaria	Proteger equipos contra daños a acceso na autorizado. Asegurar los daños en ublicaciones sietemas. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amajoulaciones. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amajoulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que los datos sean elliminados de equipos desechados. Proteger los dispositivos stillizados por usuarios finales. Limitar acceso con privilegios elevados. Controlar quién puede acceder a que información. Proteger or privilegios elevados. Controlar quién puede acceder a que información. Proteger el carceso de celegio fuene de sistemas. Implementar mecanismos fuertes de autenticación. Puedeger consessiva y prote sichos de autenticación. Puedeger consessiva y prote sichos de autenticación. Albar elobiciones para prevenir y detectar muliura. Indementar mecanismos fuertes de autenticación. Proteger consessiva y prote sichos de autenticación. Asegurar que los asistemas sesión configurados correctamente. Asegurar que los asistemas sesión configurados correctamente. Asegurar que los datos sean eliminados de fermación. Implementar medidas para prevenir fuga de información. Garantizar la recupicación de dias se e caso de peridida. Implementar redundancia para mayor disponibilidad. Registrar eventos relevantes en los sistemas. Asegurar que los relos a de los sistemas sestén sicronizados. Comorbiar el uso fermamentas con pueltypos de levados. Proteger los sistemas operativos de riesgos a la instalación de software. Implementar medidas para proteger dess. Separa redes para lumitar el impacto de originación. Usar critogorafía para proteger datos. Los controlares de los de costas se a testas de desarrollo.	APPLICA APPLIC	Exit a Jugas de Información tera la deviniculación de empleados. Protege la Infraericultura contra salvejas o fallos físicos. Facilita la continuidad de processos mediante documentación adocuado. Hantinea configuraciones segúras en los sistemas de la empresa. Protege equipos contra accessos no autorizados o pelrididas. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Evita exposiciones accidentales de datos sensibles. Protege equipos contra accessos no autorizados o perididas. Protege equipos contra accessos no autorizados o perididas. Protege información de usuario contra amenuza a chemeticas. Permite la identificación de vulnerabilidades mediante autotorias. Exita manipulaciones no autorizados en el código fuente. Protege información sensible mediante acurados de confidencialidad. Define responsabilidades claras en temas de seguridad. Controla y protege el acceso a infraestruturas sensibles. Exita interrupciones en las continuidad del negocio. Previene inicidentes de seguridad por incumplimiento en omnas. Asegura que el mantenimiento de equipos no comprometa la seguridad. Facilita la identificación y respuesta amb incindentes de seguridad. Carantira su continuidad del negocio. Previene inicidentes de seguridad por incumplimiento en omnas. Asegura que el mantenimiento de equipos no comprometa la seguridad. Identifica y corrige vulnerabilidades antes de que sean explotadas. Previene infecciones por malvarer y ataques de virus. Previene indentes en autorizados a perididas. Aperia que la siria estrutura contra amenazas ciberneficas. Sectila la contrinuidad de procesos mediante documentación adecuada. Previene indentes de seguridad por incumplimiento de nomas. Asegura que la inferioridad por procesos mediantes documen
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.18 8.19 8.20 8.21 8.20 8.21 8.22 8.23	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildidades de apoyo Seguridad del cabileado Nantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derectivos de acceso de priveligados Restricción de acceso de priveligados Restricción de acceso de priveligados Restricción de acceso de la información Acceso al código luente Autenticación segura Gestión de capacidad Protección contra malware Gestión de capacidad Protección contra malware Gestión de vulnerabilidades técnicas Gestión de los ordiguación Eliminación de información Eliminación de información Redundancia de las instalaciones de procesamiento de información Redundancia de las instalaciones de procesamiento de información Inicio sesión Actividades de segurimiento Sincronización de reloi Uso de programas de utilidad privilegiados Instalación de so segurimiento Seguridad de la red Seguridad de la red Seguridad de la red Seguridad de la red Seguridad de la redes Filtrado web Uso de criptografía	Proteger equipos contra daños a acceso na autorizado. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amipulaciones. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amipulaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que los datos sean eliminados de equipos desechados. Proteger los dispositivos stillizados por usuarios finales. Limitar acceso con privilegios elevados. Controlar quién puede acceder a que información. Proteger for descos de cidigo fueme de sistemas. Implamentar mecanismos fuerias de autenticación. Proteger for acceso de cidigo fueme de sistemas. Implamentar mecanismos fuerias de autenticación. Proteger convenida y ordes datos desirtencias de la destinación de la composição de la compo	APPLICA APPLIC	Exit sugas de información ras la desvinculación de empleados. Protege la infracturar contra salvajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos na autorizados o pérdidas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege dispositiones accidentales de datos sensibles. Protege dispositiones accidentales de datos sensibles. Protege dispositiones de usuario contra amenaza cibernéticas. Portege dispositiones de usuario contra amenaza cibernéticas. Portege dispositiones de usuario contra amenaza cibernéticas. Portege información acentificam en en designa finados. Portege información acentificam en en cuertos de confidencialidad. Portege información acentificam en entre acentros de confidencialidad. Portege información acentificam en entre acentros de confidencialidad. Portege información acentificam en entre acentros de confidencialidad. Portege información acentificam en termas de seguridad. Controla y protege el acceso a infraentructuras senables. Exita mentración es en la continuidad del negocio. Previene indeteciones en la continuidad del negocio. Previene infecciones por malvar y ataques de virus. Protege que el mantenimiento de equipos no comprometa la seguridad. Controla y protege por malvar y ataques de virus. Previene infecciones por malvar y ataques de virus. Previene infecciones por malvar y ataques de virus. Extra menipulaciones no autorizados en el código fuente. Previene infecciones por malvar y ataques de virus. Cumple con las regulaciones y normalvas agiicables. Extra menipulaciones no autorizados en el código fuente. Previene infecciones por malvar y ataques de virus. Cumple con las regulaciones y conneciones de los fosos. Restringe et acceso a áreas
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.18 8.19 8.20 8.21 8.20 8.21 8.22 8.23 8.24 8.25 8.24 8.25	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Medios de alma cenamiento Seguridad del cableado Seguridad del cableado Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derectivos de accesos de printegiado Restricción de accesos de la información Acceso al código luente Adrenticación tesegura Gestión de capacidad Protección contra malware Gestión de vulnerabilidades técnicas Gestión de los onfiguración Eliminación de información Eliminación de información Redundancia de las instrataciones de procesamiento de información inicio sesión Redundancia de las instalaciones de procesamiento de información inicio sesión Actividades de seguimiento Sincronización de reloi Uso de programas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la red Seguridad de las deservicios de redi Viso de programas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la red Seguridad de las deservicios de redi Viso de criptografía Ciclo de vida de desarrolto seguro Requistos de seguridad de la aplicación	Proteger equiposc contra daños a access on autorizado. Asegurar que los cistiemas de soporte sean conflables. Proteger el cableado contra ampidaciones. Asegurar que los distemas de soporte sean conflables. Proteger el cableado contra ampidaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que los datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con prinlegios elevados. Comotiar quide puede acceder a que información. Proteger la cceso al código breinto de sistemas. Implementar mecanismos betes de autenticación. Proteger al acceso al código breinto de sistemas. Replaces de compresente de sistemas estenas de la compresente de sistemas estenas configurados correctamente. Asegurar que los datos sean eliminados de forma segura. Proteger los datos da autenticación. Liber soluciones para prevenir y detectar malware. Identificar y corregir vulnerabilidades técnicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos da variare su almacenamiento. Implementar medidas para prevenir fugas de información. Garantizar la recuperación de datos en aco de pérdido. Implementar eventos relevantes en los sistemas. Montiores sistemas para detectar amonalis. Asegurar que los relevantes en los sistemas. Montiores sistemas para detectar amonalis. Asegurar que los relevantes en los sistemas. Montiores relevantes en los sistemas estén onfigurados. Controlar el los de hertamientas con privilegios elevados. Proteger los sistemas para detectar amonalis. Asegurar que los relevantes en los sistemas. Supervisar redes para detectar problemas. La conferencia para proteger dece. Supervisar redes para detectar problemas. La conferencia para proteger dece. Supervisar redes para detectar problemas. La conferencia para proteger	APPLICA APPLIC	Exit sugas de información na sia desvinculación de empleados. Protege la infracturar contra salosigo o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos na autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accessos na utorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Protege dispositivos de usuario contra amenaza cibernéticas. Protege dispositivos de usuario contra amenaza cibernéticas. Exita manipulaciones no autorizados en el código fuente. Protege información sensible mediante acuarios de confidencialidad. Define rasponsabilidades calus en riema de seguridad. Controla y protege el acceso a infraestructuras sensibles. Exita materiación es en la continuidad del negocio. Evita materiación es en la continuidad del negocio. Evita materiación es en la continuidad del negocio. Terviene indotención verguestas ante nicolhentes de seguridad. Controla y protege el acceso a infraestructuras sensibles. Exita materiación es en la continuidad del negocio. Terviene infecciones por materiación es es es es es especificad. Controla y protege por es se especificad por les proteges equipos contra accesos no autorizados o peridas. Previene infecciones por materia y ataques de virus. Previene infecciones por materia y ataques de virus. Evita manipulaciones no autorizados en el código for une le protege el acceso a fraes con información caladicades. Previene infecciones por materia y ataques de virus. Cumple con las regulaciones y normativas agilicables. Exta accesos no autorizados en el código for lente. Previene infecciones por materiación de documentación ad
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.12 8.19 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.20 8.20 8.21 8.22 8.22 8.28	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Medios de alma cenamiento Medios de alma cenamiento Seguridad del cableado Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Olspositivos de parto final de usuario Describos de accesos de privilegiado Restricción de acceso a la información Acceso al código luente Adventicación segura Gestión de capacidad Proteción corta malware Gestión de capacidad Proteción de real malware Gestión de vulnerabilidades técnicas Gestión de la configuración Eliminación de información Eliminación de información Proteción de fuga de datos Opopa de seguridad de la información Redundancia de las instalaciones de procesamiento de información Inicio sesión Actividades de seguimiento Sincornización de reloi Uso de criprograzación de reloi Uso de programas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la la red Seguridad de las servicios de red Segregación de redes Filtrados vedio de desarrollo seguro Prucebos de aequiridad de la sipicación Principios de arquitectura e ingenieria de sistemas seguros Codificación segura Pruebas de seguridad de la sipicación Principios de arquitectura ingenieria de sistemas seguros Codificación segura Pruebas de seguridad en desarrollo y aceptación	Proteger equipos contra daños a acceso na autorizado. Asegurar que los cistemas de soporte sean conflables. Proteger el cableado contra ampidaciones. Asegurar que los cistemas de soporte sean conflables. Proteger el cableado contra ampidaciones. Asegurar que el mantenimiento no compromenta la seguridad. Garantizar que los datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con priveligos elevados. Contratar quich puede acceder a que información. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con priveligos elevados. Contratar quich puede acceder a que información. Proteger la caceso al código buento de sistemas. Ingeneratar mecanismos lutente de autenticación. Usar soluciones para prevenir y detectar malware. Identificar y corregir vulnerabilidades tecnicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos da da utenticación. Limplementar medidas para prevenir y detectar malware. Identificar y corregir vulnerabilidades tecnicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos da autenticación de forma segura. Registrar eventos relevantes su información. Garantizar la recuperación de datos en acos de péridida. Implementar medidas para prevenir y detecta. Asegurar que los relovantes su disconsidados. Controlar el suos de heramanientos. Implementar redundancia para mayor disponibilidad. Registrar eventos relevantes en los sistemas. Montificar sistemas para detectar anomalias. Adegurar que los relois de los sistemas estetin sinconicados. Proteger los datos da en amientas con privilegios elevados. Proteger los sistemas para detectar anomalias. Separar redes para lumitar el impacto de incidentes. Carlegoritar las positosas permitidas en la organización. Usar cripiosaria para detectar apoleticas elevandos. Proteger los sistemas segurados controlacions. Incorporar seguridad en todas las etapas del desarrollo. Definitar que interniento	APPLICA APPLIC	Exit sugas de información na sia desvinculación de empleados. Protege la infractular acorta salutajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos na autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accessos na autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Protege dispositiones accidentales de datos sensibles. Protege dispositiones de usuario contra amenazara obernéticas. Protege dispositiones de usuario contra amenazara obernéticas. Exita manipulaciones no autorizados en el códego fuente. Protege información sensibile mediante acuerdos de confidencialidad. Protege información sensibile mediante acuerdos de confidencialidad. Controla y protege el acceso a infraestructuras sensibiles. Exita interrupciones en la confituación de legación. Previene indentes de seguridad por inicumplimiento de normas. Acegora que el mantenimiento de eculpos no comprometa la seguridad. Controla y contige vulnerabilidades antes de que sean exploidadas. Protege equipos contra accessos no autorizados o pendias. Protege equipos contra accessos no autorizados o pendias. Protege equipos contra accessos no autorizados o prendias. Protege equipos contra accessos no autorizados o prendias. Protege equipos contra accessos no autorizados o protegidos. Previene indentes de seguridad o por inicumplimiento de normas. Asegora que el mantenimiento de equipos no comprometa la seguridad. Controla y confige vulnerabilidades en mediante adocumentación adecuada. Previene indentes de seguridad o por inicumplimiento de normas de contra de la continuidad de procesos mediantes documentación adecuada. Previene indentes de segur
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.20 8.21 8.22 8.23 8.24 8.25 8.26 8.27 8.28	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Medios de alma cenamiento Medios de alma cenamiento Seguridad del cableado Nantenimiento de equipos Seguridad del cableado Nantenimiento de equipos Eliminación segura o reutilización de equipos Olspositivos de parto final de usuario Describos de acceso a la Información Acceso al código Ibente Adureticación segura Gestión de acceso a la Información Acceso al código Ibente Adureticación segura Gestión de capacidad Protección contra malware Gestión de capacidad Protección contra malware Gestión de vulnerabilidades técnicas Gestión de la configuración Eliminación de información Eliminación de información Protección de fuga de datos Opoga de seguridad de la información Redundancia de las instalaciones de procesamiento de información Inicio sesión Actividades de seguimiento Sincronización de reloi Uso de criptosparida de la la de Seguinad de la la policación Principios de arquitectura e ingeniería de sistemas seguros Codificación segura Pruebas de seguindad en desarrolto y aceptación Desarrollo subcontratado Desarrollo subcontratado Desarrollo subcontratado Desarrollo subcontratado	Proteger equiposc contra daños a acceso na autorizado. Asegurar que los cártos en ubicaciones externas. Asegurar que los cistemas de soporte sean conflables. Proteger el cableado contra anapudaciones. Asegurar que el mantenimiento no comprometa la seguridad. Garantizar que lo dados sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con priteligos elevados. Controlar quien pueda ecoder a que información. Proteger la coseo al código treme de sistemas. Ilimitar accesos con priteligos elevados. Controlar quien pueda ecoder a que información. Proteger al acceso al código treme de sistemas. Implementar mecanismos fuertes de autenticación. Libar soluciones para prevenir y detectar maiware, tidentificar y corregir vulnerabilidades técnicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos sean eliminados de forma segura. Proteger los datos darantes su almocanismos. Implementar medidas para prevenir y detectar maiware. Implementar redundancia para mayor disporibilidad. Implementar redundancia para mayor disporibilidad. Registrar eventos relevantes en los sistemas. Monitorear sistemas para detectar anomalios. Asegurar que los terios de considera en los sistemas. Monitorear sistemas para detectar anomalios. Asegurar que los reloses de los sistemas estemas. Monitorear sistemas para detectar anomalios. Supervisar redes para detectar anomalios. Supervisar redes para proteger des. Supervisar redes para a detectar problemas. Supervisar redes para a detectar poblemas. Supervisar redes para a detectar poblemas. Supervisar redes para a detectar problemas. Supervisar redes para a detectar poblemas. Supervisar redes para a detectar anomalios. Incorporar seguridade no todas las etapas del desarrollo. Deferir requerimentos de segurida	APPLICA APPLIC	Exit sugas de información na sia desvinculación de empleados. Protege la infractular acortra salvajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos na autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accessos na utorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Protege dispositiones de usuario contra amenazara obernéticas. Protege dispositiones de usuario contra amenazara obernéticas. Exita manipulaciones no autorizadas en el códego fuerte. Protege información sensible mediante acuerdos de confidencialidad. Protege información sensible mediante acuerdos de confidencialidad. Controla y protege el acceso a infraestructuras sensibles. Exita interrupciones en la confirmación de inegicio. Previene indentes de seguridad por incumplimiento de normas. Acegora que el mantenimiento de eculpos no comprometa la seguridad. Controla y contige vulnerabilidades antes de que sea exploidadas. Protege equipos contra accesos no autorizados o peridias. Protege equipos contra accesos no autorizados o peridias. Protege equipos contra accesos no autorizados o peridias. Protege equipos contra accesos no autorizados o predidas. Previene indentes de seguridad por incumplimiento de normas. Asegora que el mantenimiento de eculpos no comprometa la seguridad. Controla y confige vulnerabilidades antes de que sean exploidadas. Previene indentes de seguridad por incumplimiento de normas. Asegora que el mantenimiento de eculpos no comprometa la seguridad. Experimiento de la continuidad de procesos mediantes adocumentación adecuada. Previene indentes de seguridad por i
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.8 8.8 8.9 8.10 8.11 8.12 8.13 8.14 8.15 8.16 8.17 8.18 8.19 8.20 8.21 8.22 8.23 8.24 8.25 8.26 8.27 8.28 8.28 8.28 8.29 8.20 8.20 8.21 8.22 8.23 8.23 8.24 8.25 8.26 8.27 8.28 8.28	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildiades de apoyo Seguridad del cableado Mantenimiento de equipos Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Derechos de acceso de privilegiado Restricción de acceso a la información Acceso al codigo fuente Autenticación segura Gestón de canceso a la información Acceso al codigo fuente Información contra malvara Gestón de canacidad Protección contra malvara Gestón de valentalidiades técnicas Gestón de la configuración Eliminación de información Enmascaramiento de datos Protección de prise de datos Copia de seguridad de la información Redundancia del las instalaciones de procesamiento de información Nicrotazción de retio) Livo de procurama de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la red Seguridad de la se sestimiento Sincotazción de retio; Uso de procurama de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de la se sespiridad de la pipicación Pritirado web Uso de criptografía Pricebos de desarrollo seguro Requisitos de seguridad de la applicación Principios de arquitectura e ingeniería de sistemas seguros Codificación segura Pruebas de seguridad en de sarrolto y aceptación	Proteger equipos contra daños a acceso na autorizado. Asegurar que los cistemas de soporte sean conflables. Proteger el cableado contra ampidaciones. Asegurar que los cistemas de soporte sean conflables. Proteger el cableado contra ampidaciones. Asegurar que el mantenimiento no compromenta la seguridad. Garantizar que los datos sean eliminados de equipos desechados. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con priveligos elevados. Contratar quich puede acceder a que información. Proteger los dispositivos utilizados por usuarios finales. Limitar accesos con priveligos elevados. Contratar quich puede acceder a que información. Proteger la caceso al código buento de sistemas. Ingeneratar mecanismos lutente de autenticación. Usar soluciones para prevenir y detectar malware. Identificar y corregir vulnerabilidades tecnicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos da da utenticación. Limplementar medidas para prevenir y detectar malware. Identificar y corregir vulnerabilidades tecnicas. Asegurar que los datos sean eliminados de forma segura. Proteger los datos da autenticación de forma segura. Registrar eventos relevantes su información. Garantizar la recuperación de datos en acos de péridida. Implementar medidas para prevenir y detecta. Asegurar que los relovantes su disconsidados. Controlar el suos de heramanientos. Implementar redundancia para mayor disponibilidad. Registrar eventos relevantes en los sistemas. Montificar sistemas para detectar anomalias. Adegurar que los relois de los sistemas estetin sinconicados. Proteger los datos da en amientas con privilegios elevados. Proteger los sistemas para detectar anomalias. Separar redes para lumitar el impacto de incidentes. Carlegoritar las positosas permitidas en la organización. Usar cripiosaria para detectar apoleticas elevandos. Proteger los sistemas segurados controlacions. Incorporar seguridad en todas las etapas del desarrollo. Definitar que interniento	APPLICA APPLIC	Exit sugas de información na sia desvinculación de empleados. Protege la infractular acorta salutajes o fallos físicos. Facilita la continuidad de procesos mediante documentación adecuada. Martiene configuraciones seguras en los sistemas de la empresa. Protege equipos contra accesos na autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accessos na autorizados o pérididas. Facilita la continuidad de procesos mediante documentación adecuada. Exita exposiciones accidentales de datos sensibles. Protege dispositiones accidentales de datos sensibles. Protege dispositiones de usuario contra amenazara obernéticas. Protege dispositiones de usuario contra amenazara obernéticas. Exita manipulaciones no autorizados en el códego fuente. Protege información sensibile mediante acuerdos de confidencialidad. Protege información sensibile mediante acuerdos de confidencialidad. Controla y protege el acceso a infraestructuras sensibiles. Exita interrupciones en la confituación de legación. Previene indentes de seguridad por inicumplimiento de normas. Acegora que el mantenimiento de eculpos no comprometa la seguridad. Controla y contige vulnerabilidades antes de que sean exploidadas. Protege equipos contra accessos no autorizados o pendias. Protege equipos contra accessos no autorizados o pendias. Protege equipos contra accessos no autorizados o prendias. Protege equipos contra accessos no autorizados o prendias. Protege equipos contra accessos no autorizados o protegidos. Previene indentes de seguridad o por inicumplimiento de normas. Asegora que el mantenimiento de equipos no comprometa la seguridad. Controla y confige vulnerabilidades en mediante adocumentación adecuada. Previene indentes de seguridad o por inicumplimiento de normas de contra de la continuidad de procesos mediantes documentación adecuada. Previene indentes de segur
8. Controles Tecnológicos	7.10 7.11 7.12 7.13 7.14 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.9 8.9 8.10 8.11 8.12 8.12 8.13 8.14 8.15 8.16 8.17 8.19 8.20 8.21 8.22 8.22 8.24 8.25 8.26 8.27 8.28 8.28 8.29 8.20 8.21 8.22 8.28 8.28 8.29 8.28 8.29 8.28 8.29 8.30	Emplazamiento y protección de equipos Seguridad de los activos fuera de las instalaciones Medios de alma cenamiento Wildiades de apoyo Seguridad del cableado Mantenimiento de equipos Seguridad del cableado Mantenimiento de equipos Eliminación segura o reutilización de equipos Dispositivos de punto final de usuario Despositivos de punto final de usuario Derechos de acceso a la información Acceso al codigo fuente Autenticación segura Gestión de acceso a la información Acceso al codigo fuente Autenticación segura Gestión de vaneadidad Protección contra malvara Gestión de vaneadidad Gestión de valenadidades tecinicas Gestión de configuración Eliminación de información Enmascaramiento de datos Protección de pira de datos Copia de seguridad de la información Incico sesión Actividades de segurimiento Siniconización de relioi Uso de procaramiento de utilidad privilegidados Instalación de software en sistemas operativos Seguridad de la se un estidad privilegidados Instalación de software en sistemas operativos Seguridad de la se un estidad privilegidados Instalación de software en sistemas operativos Seguridad de la se sequiridad de la picicación Pititado web Uso de criptografía Pititado veb Uso de procaramiento una de sistemas seguros Codificación segura Pruebas de seguridad en de sarrolto y aceptación Peparación de los entornos de desarrolto, prueba y producción Peparación de los entornos de desarrolto, prueba y producción	Proteger equipos contra daños o acceso no autorizado. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amipulaciones. Asegurar que los sistemas de soporte sean conflables. Proteger el cableado contra amipulaciones. Asegurar que los ados sean eliminados de equipos deschados. Garantizar que los datos sean eliminados de equipos deschados. Proteger los dispositives utilizados por usuarios finales. Limitar acresos cos privilegios elevados. Controlar quién puede acceder a que información. Proteger los dispositives utilizados por usuarios finales. Controlar quién puede acceder a que información. Proteger at quién puede acceder a que información. Proteger el carcesión calegio fueme de sistemas. Implamentar mecanismos huerias de autenticación. Usar obliciones para prevenir y detectar malvane. Iduaridad y como de la carcelar de la como de la como de la carcelar de la como de la carcelar del carcelar	APPLICA APPLIC	Exit sugas de información na sia deveniculación de empleados. Protege la infractular acontra salesjas o fallos fisicas. Facilita la continuidad de procesos mediante documentación adocuada. Mantiene configuiaciones seguiras en los sistemas de la empresa. Protege equipos contra accesos no autorizados o péridads. Exita exposiciones accidentales de datos sensibles. Protege equipos contra accesos no autorizados o perididas. Protege equipos contra accesos no autorizados o perididas. Pemite la identificación de vulnerabilidades em dediante autoriarias. Exita internación en autorizados en el códigio fuente. Protege información sensibis mediante acuerdos de confidencialidad. Protege información sensibis mediante acuerdos de confidencialidad. Define responsabilidades claras en ternas de seguridad. Controla y protege el acceso a infraestruturas sensibise. Exita interrupciones en la continuidad del negocio. Previene incidentes de seguridad por incumplimiento de normas. Asegura que el mantenimiento de equipos no comprometa la seguridad. Facilita ta infertificación y respuesta ame inciedentes de seguridad. Carantiza que el os sistemas de inacesos en accesos na respectados. Previene infecciones por mativare y atraques de virus. Protege en infecciones por mativare y atraques de virus. Previene incidentes de usuario contra accesso no autorizados o perididas. Garantiza que los sistemas de almacenamiento sean conflables. Exita instrucciones por mativare y atraques de virus. Previene incidentes de usuario contra amenzas cibernificas. Facilita ta infraestructura contra saboriajes o fallos fisicos. Restringe el acceso a áreas con indornación clasificados. Previene incidentes de seguridad o froncomplimiente de normas. Asegura que la infraestructura contra saboriajes o fallos fisicos. Restringe el acceso a áreas con información clasificados. Previen