MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACION

PROCESO: Gestion de Informatica

OBJETIVO: Garantizar la disponibilidad de servicios tecnológicos con innovación y ciencia, que permitan atender los requerimientos de la Alcaldía Municipal de Palmira para cumplirle a la comunidad, teniendo en cuenta las políticas de gobierno digital, lineamientos y estándares tecnológicos, que aseguren el correcto funcionamiento y sostenibilidad de las soluciones.

TIPO DE ACTIVO	VULNERABILIDAD O DEBILIDAD	AMENAZA	RIESGO	CONSECUENCIA	PROBABILIDAD		EVALUACIÓN DEL RIESGO	DESCRIPCIÓN EVALUACIÓN DEL RIESGO	OPCIONES DE MANEJO DEL RIESGO	CONTROLES	EVALUACION DEL CONTROL	RESULTADO DE LA EVALUACION DEL CONTROL	RIESGO RESIDUAL	ACCIONES
					Probabilidad	Impacto							Nueva Zona del riesgo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en la herramienta de gestion	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.14.2.8 Pruebas de seguridad de sistemas	2,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Se debe establecer politica donde se debe realizar pruebas de vulnerabilidades al sistema de informacion. esto se debe realizar al menos una vez al año. - Se debe generar un plan para cerrar las brechas identificadas. - Se debe cerrar las brechas identificadas en los tiempos estipulados en el plan
Informacion	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en la herramienta de gestion	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - Establecer politicas de control de acceso - Asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - Validar que el backup se haya generado en la periodicidad establecida
Organizaciòn	No se realiza seguimiento y monitoreo al contrato con mi Hosting SAS	Incumplimiento por parte del proveedor	Indisponibilidad o perdida de informacion por falta de seguimiento al contrato con proveedor y obligaciones contractuales tecnicas	el no monitoreo de la relacion con AWS puede ocasionar que se descuiden alcances y obligaciones que puede afectar la disponibilidad de la informacion	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Realizar monitoreo periodico del contrato con el proveedor - Hacer gestion para velar por el cumplimiento de las condiciones del contrato con el proveedor
Software	Asignación errada de los derechos de acceso	Abuso de los derechos	Perdida o alteracion de informacion por mal asignacion de derechos al usuario	Un usuario puede alterar o eliminar informaicon por mala asignacion de privilegios para el acceso al sistema	4	10	40	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.9.2 Gestión de acceso de usuarios	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	Establecer un procedimiento de acceso a informacion y asignacion de permisos - Establecer politicas de control de acceso - Asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.9.2.2 Suministro de acceso de usuarios	1,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	
										A.9.2.3 Gestión de derechos de acceso privilegiado	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	

Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en la plataforma	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	4	10	40	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.14.2.8 Pruebas de seguridad de sistemas	2,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Se debe realizar pruebas de vulnerabilidades al sistema de informacion. esto se debe realizar al menos una vez al año. - Se debe generar un plan para cerrar las brechas idnetificadas. - Se debe cerrar las brechas identificadas en los tiempos estipulados en el plan
										A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - Establecer politicas de control de acceso - Asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - Validar que el backup se haya generado en la periodicidad establecida.
Organizaciòn	No se realiza seguimiento y monitoreo al contrato con proveedor	Incumplimiento por parte del proveedor	Indisponibilidad o perdida de informacion por falta de seguimiento al contratos con el proveedor	el no monitoreo de la relacion con el proveedor puede ocasionar que se descuiden alcances y obligaciones que puede afectar la disponibilidad de la informacion	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Realizar monitoreo periodico del contrato con el proveedor - Hacer gestion para velar por el cumplimiento de las condiciones del contrato con el proveedor
Organizaciòn	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en la herramienta KLSHARE	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.14.2.8 Pruebas de seguridad de sistemas	2,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Se debe realizar pruebas de vulnerabilidades al sistema de informacion. esto se debe realizar al menos una vez al año. - Se debe generar un plan para cerrar las brechas idnetificadas. - Se debe cerrar las brechas identificadas en los tiempos estipulados en el plan
										A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - Establecer politicas de control de acceso - Asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Desginar un responsable - Programar monitoreo de los controles
Software	Asignación errada de los derechos de acceso	Abuso de los derechos	Perdida o alteracion de informacion por mal asignacion de derechos al usuario	Un usuario puede alterar o eliminar informaicon por mala asignacion de privilegios para el acceso al sistema	4	10	40	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.9.2 Gestión de acceso de usuarios	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - Establecer politicas de control de acceso - Asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.9.2.2 Suministro de acceso de usuarios	1,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	
										A.9.2.3 Gestión de derechos de acceso privilegiado	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	
Informacion	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en la herramienta	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	Establecer una politica de copias de respaldo para el sistema definiendo periodisidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.

Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en el aplicativo	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.14.2.8 Pruebas de seguridad de sistemas	2,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Se debe realizar pruebas de vulnerabilidades al sistema de informacion. esto se debe realizar al menos una vez al año. - se debe generar un plan para cerrar las brechas idnetificadas. - Se debe cerrar las brechas identificadas en los tiempos estipulados en el plan
Informacion	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en el aplicativo	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	Establecer una politica de copias de respaldo para el sistema definiendo periodisidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en el aplicativo de consulta	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Organizaciòn	No se realiza seguimiento y monitoreo al contrato con proveedor	Incumplimiento por parte del proveedor	Indisponibilidad o perdida de informacion por falta de seguimiento al contratos con el proveedor de herramienta google	el no monitoreo de la relacion con el proveedor puede ocasionar que se descuiden alcances y obligaciones que puede afectar la disponibilidad de la informacion	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- realizar monitoreo periodico del contrato con el proveedor - hacer gestion para velar por el cumplimiento de las condiciones del contrato con el proveedor
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Accesos no autorizados a informacion confidencial	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.14.2.8 Pruebas de seguridad de sistemas	2,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Se debe realizar pruebas de vulnerabilidades al sistema de informacion. esto se debe realizar al menos una vez al año. - se debe generar un plan para cerrar las brechas idnetificadas. - Se debe cerrar las brechas identificadas en los tiempos estipulados en el plan
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en el portal	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Accesos no autorizados a informacion confidencial	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.14.2.8 Pruebas de seguridad de sistemas	2,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Se debe realizar pruebas de vulnerabilidades al sistema de informacion. esto se debe realizar al menos una vez al año. - se debe generar un plan para cerrar las brechas idnetificadas. - Se debe cerrar las brechas identificadas en los tiempos estipulados en el plan
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en la intranet	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.

Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Accesos no autorizados a informacion confidencial	Un atacante puede explotar vulnerabilidades del software y alterar o secuestrar la informacion de la aplicación y solicitar rescate o escalar dentro de la red para acceder a otros servicios	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.14.2.8 Pruebas de seguridad de sistemas	2,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Se debe realizar pruebas de vulnerabilidades al sistema de informacion. esto se debe realizar al menos una vez al año. - se debe generar un plan para cerrar las brechas idnetificadas. - Se debe cerrar las brechas identificadas en los tiempos estipulados en el plan
Software	Asignación errada de los derechos de acceso	Abuso de los derechos	Perdida o alteracion de informacion por mal asignacion de derechos al usuario	Un usuario puede alterar o eliminar informaicon por mala asignacion de privilegios para el acceso al sistema	4	10	40	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.9.2 Gestión de acceso de usuarios	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.9.2.2 Suministro de acceso de usuarios	1,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	
										A.9.2.3 Gestión de derechos de acceso privilegiado	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Accesos no autorizados a informacion confidencial	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Alteracion y Accesos no autorizados a informacion confidencial	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados

Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Alteracion y Accesos no autorizados a informacion confidencial	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Alteracion y Accesos no autorizados a informacion confidencial	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	

Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Alteracion y Accesos no autorizados a informacion confidencial	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada en en el servidor de almacenamiento	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de configuracion por explotacion de vulnerabilidades	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
	Almacenamiento sin	Hurtos medios o	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20		Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	

Hardware	Almacenamiento sin protección	Hurtos medios o documentos.						Riesgo Medio		A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
Organizaciòn	No se realiza seguimiento y monitoreo al contrato con proveedor	Incumplimiento por parte del proveedor	Indisponibilidad o perdida de informacion por falta de seguimiento al contratos con el proveedor	el no monitoreo de la relacion con el proveedor puede ocasionar que se descuiden alcances y obligaciones que puede afectar la disponibilidad de la informacion	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- realizar monitoreo periodico del contrato con el proveedor - hacer gestion para velar por el cumplimiento de las condiciones del contrato con el proveedor
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de informacion almacenada por acceso no autorizados a la informacion	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware de almacenamiento	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
	Vulnerabilidades	Abuso de los	Perdida o alteracion de informacion almacenada por acceso no autorizados a la informacion	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60		Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados

Software	conocidos en el software	Abuso de los derechos						Riesgo Alto		A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Software	Asignación errada de los derechos de acceso	Abuso de los derechos	Perdida o alteracion de informacion por mal asignacion de derechos al usuario	Un usuario puede alterar o eliminar informaicon por mala asignacion de privilegios para el acceso al sistema	4	10	40	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.9.2 Gestión de acceso de usuarios	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.9.2.2 Suministro de acceso de usuarios	1,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	
										A.9.2.3 Gestión de derechos de acceso privilegiado	1,5	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	
Software	Asignación errada de los derechos de acceso	Abuso de los derechos	Perdida o alteracion de informacion por mal asignacion de derechos al usuario	Un usuario puede alterar o eliminar informaicon por mala asignacion de privilegios para el acceso al sistema	4	10	40	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.9.2 Gestión de acceso de usuarios	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	Establecer un procedimiento de acceso a informacion y asignacion de permisos
										A.9.2.2 Suministro de acceso de usuarios	1,25	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias
										A.9.2.3 Gestión de derechos de acceso privilegiado	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Medio	- Realizar seguimiento a los accesos asignados
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de configuracion por explotacion de vulnerabilidades	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.

Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de configuracion por explotacion de vulnerabilidades	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de configuracion por explotacion de vulnerabilidades	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de configuracion por explotacion de vulnerabilidades	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Establecer un procedimiento de acceso a informacion y asignacion de permisos establecer politicas de control de acceso asignar los permisos implementando el procedimiento y teniendo evidencias
										A.12.6.1 Gestión de las vulnerabilidades técnicas	1,00	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Se debe mantener actualizado los sistemas de informacion como el sistema operativo, y aplicaciones instaladas en el sistema
			Perdida de informacion por hurto del hardware	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20		Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	

Hardware	Almacenamiento sin protección	Hurtos medios o documentos.						Riesgo Medio		A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
Software	Vulnerabilidades conocidos en el software	Abuso de los derechos	Perdida o alteracion de configuracion por explotacion de vulnerabilidades	La explotacion de una vulnerabilidad en el sistema operativo, puede generar la perdida o alteracion de la informacion, ya sea por acceso de un atacante o por ataque de un malware	6	10	60	Riesgo Alto	Reducir el riesgo, evitar, compartir o transferir	A.9.4 Control de acceso a sistemas y aplicaciones	1,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	- Establecer un procedimiento de acceso a informacion y asignacion de permisos - establecer politicas de control de acceso - asignar los permisos implementando el procedimiento y teniendo evidencias - Realizar seguimiento a los accesos asignados
										A.12.3.1 Respaldo de información	2,50	Se mantiene el resultado de la evaluacion antes de controles	Riesgo Alto	Establecer una politica de copias de respaldo para el sistema definiendo periodicidad para el sistema de informacion - validar que el backup se haya generado en la periodicidad establecida.
Hardware	Almacenamiento sin protección	Hurtos medios o documentos.	Perdida de informacion por hurto del hardware	Un atacante puede acceder fisicamente al dispositivo de almacenamiento y hurtar el dispositivo	2	10	20	Riesgo Medio	Reducir el riesgo, evitar, compartir o transferir	A.11.2.1 . Ubicación y protección de los equipos	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	- Mantener el control debidamente supervisado para evitar degradacion
										A.11.1.1. Perímetro de seguridad física	2,75	Se desplaza el nivel de riesgo en un punto, dependiendo si el control afecta el impacto o la probabilidad	Riesgo Bajo	