TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN – MINTIC	**INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD HOJA PORTADA**	vive digital para la gente

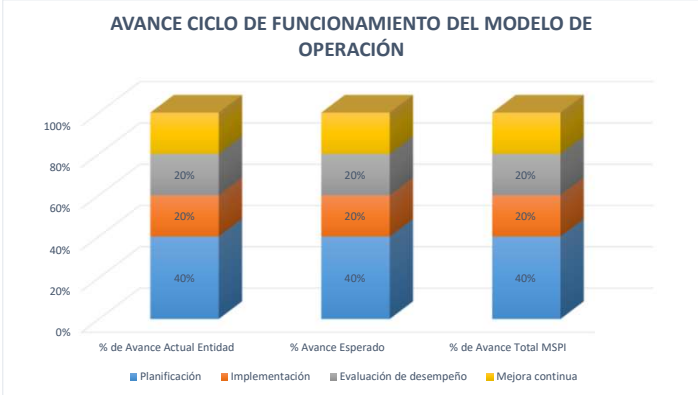
ENTIDAD EVALUADA	**Corporación para el Desarrollo Sostenible del Urabá - CORPOURABA**
FECHAS DE EVALUACIÓN	31/03/2023
CONTACTO	JAIRO AGUDELO - jagudelo@corpouraba.gov.co
ELABORADO POR	JAIRO AGUDELO - jagudelo@corpouraba.gov.co

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	90	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	90	90	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	90	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	81	80	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	85	85	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	90	80	**OPTIMIZADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	85	85	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	82	80	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	84	80	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	83	80	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	100	80	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	80	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	90	80	**OPTIMIZADO**
A.18	CUMPLIMIENTO	82,5	80	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**88**	**83**	**OPTIMIZADO**

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA			
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**	**% de Avance Total MSPI**
2022	Planificación	40%	40%	40%
2022	Implementación	20%	20%	20%
2022	Evaluación de desempeño	20%	20%	20%
2022	Mejora continua	20%	20%	20%
TOTAL				**100%**



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

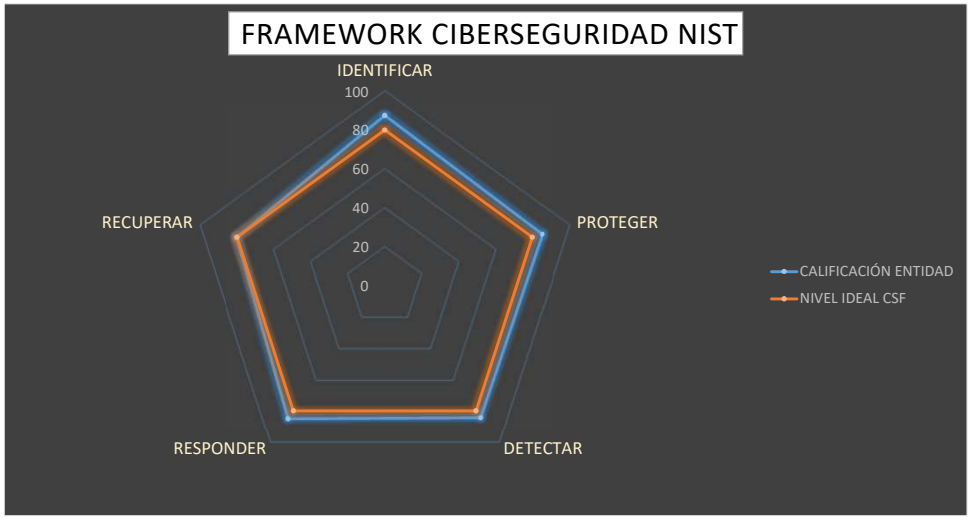
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	SUFICIENTE
Administrado	SUFICIENTE
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	88	80
PROTEGER	85	80
DETECTAR	84	80
RESPONDER	84	80
RECUPERAR	80	80



TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

MINTIC

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

Corporación para el Desarrollo Sostenible del Urabá - CORPOURABA

vive digital para la gente

0
20
40
60
80
100

ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
R1	n/a	1) Si Se identifican en forma general los activos de información de la Entidad, estan en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, estan en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, estan en 80.	Administrativas	AD.4.1.1	80	40	MAYOR	60	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	AD.4.2.1	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R3	n/a	1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, estan en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, estan aprobados y documentados, por la alta Dirección, estan en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Direcciòn, , estan en 60.	Administrativas	AD.3.2.2	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R4	n/a	Existe la necesidad de implementar el Modelo de Seguridad y Privacidad de la Información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten en la Entidad.	PHVA	P.1	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
			Administrativas	AD.1.1	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
			PHVA	P.4	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R5	Responsable de SI	1. Si se tratan temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, coloque 20 2.Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad, coloque 40	Madurez	R5	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R6	n/a	1. Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, estan en 20. 2. Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , estan en 40. 3. Si se divulgan las políticas de seguridad y privacidad de la información, estan en 60.	Administrativas	AD.1.1	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R7	n/a	Establecer y documentar el alcance, límites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y Privacidad de la Información.	PHVA	P.1	100	60	MAYOR	60	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R8	n/a	Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad.	Tecnicas	T.7.1.4	80	20	MAYOR	40	MAYOR	60	MAYOR	60	MAYOR	80	CUMPLE
E DE MADUREZ INICIAL					920	260	CUMPLE	440	CUMPLE	600	CUMPLE	780	MENOR	980	MENOR
R9	Responsable de SI	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.	Madurez	R9	60	N/A	N/A	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R10	n/a	Aprobación de la alta dirección, documentada y firmada, para la Implementación del Modelo de Seguridad y Privacidad de la Información.	Madurez	R9	100	N/A	N/A	60	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R11	n/a	Identificar los riesgos asociados con la información, físicos, lógicos, identificando sus vulnerabilidades y amenazas.	PHVA	P.6	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R12	n/a	1) Si se elaboran informes de TODOS los incidentes de seguridad y privacidad de la información, TODOS estan documentados e incluidos en el plan de mejoramiento continuo.Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro, estan en 40. 2) Si los controles y medidas identificados para disminuir los incidentes fueron implementados, estan en 60.	Tecnicas	T.7.1.2	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R13	n/a	1. Si se cuentan con procedimientos que indican a los funcionarios como manejar la información y los activos de información en forma segura. Se tienen documentados los controles físicos y lógicos que se han definido en la Entidad, con los cuales se busca preservar la seguridad y privacidad de la información, aprobado por la alta Dirección, estan en 40. 2. Si se han divulgado e implementado los controles físicos y lógicos que wse han definido en la entidad, con los cuales se busca preservar la seguridad y privacidad de la información, estan en 60.	Administrativas	AD.4.1	90	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	MENOR
R14	n/a	Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentantan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección, estan en 40. Si se reconoce la importancia de ampliar los planes de continuidade del negocio a otros procesos, pero aun no se pueden incluir ni trabajar con ellos, estan en 60.	Administrativas	AD.5.1.1	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R15	n/a	Los roles de seguridad y privacidad de la información están bien definidos y se lleva un registro de las actividades de cada uno.	Administrativas	AD.2.1	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R16	n/a	Dispositivos para movilidad y teletrabajo	Administrativas	AD.2.2	80	N/A	N/A	40	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
R17	n/a	Protección contra código malicioso	Tecnicas	T.4.2	80	N/A	N/A	40	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
R18	n/a	Copias de seguridad	Tecnicas	T.4.3	80	N/A	N/A	40	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
R19	n/a	Gestión de la vulnerabilidad técnica	Tecnicas	T.4.6	80	N/A	N/A	40	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
E MADUREZ GESTIONADO					970	0		460	CUMPLE	660	CUMPLE	880	MENOR	1100	MENOR
R20	n/a	Seguridad ligada a los recursos humanos, antes de la contratación	Administrativas	AD.3.1	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R21	n/a	Seguridad ligada a los recursos humanos, durante la contratación	Administrativas	AD.3.2	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R22	n/a	Seguridad ligada a los recursos humanos, al cese o cambio de puesto de trabajo	Administrativas	AD.3.3	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R23	n/a	Requisitos de negocio para el control de accesos.	Tecnicas	T.1.1	90	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	MENOR

R24	n/a	Responsabilidades del usuario frente al control de accesos	Tecnicas	T.1.2.6	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R25	n/a	Seguridad física y ambiental en áreas seguras	Tecnicas	T.1.3.1	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R26	n/a	Seguridad física y ambiental de los equipos	Tecnicas	T.3.2	82	N/A	N/A	N/A	N/A	60	MAYOR	***80***	***MAYOR***	100	MENOR
R27	n/a	Responsabilidades y procedimientos de operación	Tecnicas	T.4.1	85	N/A	N/A	N/A	N/A	60	MAYOR	***80***	***MAYOR***	100	MENOR
R28	n/a	Seguridad en la operativa, control del software en explotación	Tecnicas	T.4.5	80	N/A	N/A	N/A	N/A	60	MAYOR	***80***	***CUMPLE***	100	MENOR
R29	n/a	Gestión de la seguridad en las redes.	Tecnicas	T.5.1	87	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	MENOR
R30	n/a	Intercambio de información con partes externas	Tecnicas	T.5.2	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R31	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, requisitos de seguridad de los sistemas de información.	Tecnicas	T.6.1	90	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	MENOR
R32	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, seguridad en los procesos de desarrollo y soporte.	Tecnicas	T.6.2	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R33	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, datos de prueba.	Tecnicas	T.6.3	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R34	n/a	Gestión de incidentes en la seguridad de la información, notificación de los eventos de seguridad de la información.	Tecnicas	T.7.1.2	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R35	n/a	Gestión de incidentes en la seguridad de la información, notificación de puntos débiles de la seguridad.	Tecnicas	T.7.1.3	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R36	n/a	Gestión de incidentes en la seguridad de la información, recopilación de evidencias.	Tecnicas	T.7.1.7	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R37	n/a	Implantación de la continuidad de la seguridad de la información.	Administrativas	AD.5.1.2	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R38	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con suministradores.	Administrativas	AD.7.1	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R39	Responsable de compras y adquisiciones	Gestión de la prestación del servicio por suministradores.	Administrativas	AD.7.2	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R40	n/a	Se implementa el plan de tratamiento de riesgos y las medidas necesarias para mitigar la materialización de las amenazas.	PHVA	P.8	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
DE MADUREZ DEFINIDO					990	0		0		660	CUMPLE	880	CUMPLE	1100	MENOR
R41	n/a	Se utilizan indicadores de cumplimiento para establecer si las políticas de seguridad y privacidad de la información y las clausulas establecidas por la organización en los contratos de trabajo, son acatadas correctamente. Se deben generar informes del desempeño de la operación del MSPI, con la medición de los indicadores de gestión definidos.	PHVA	I.5	100	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
			PHVA	E.1	100	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MAYOR
			PHVA	E.2	100	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MAYOR
			PHVA	E.3	100	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MAYOR
			PHVA	M.1	100	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MAYOR
R42	n/a	Se realizan pruebas de manera sistemática a los controles, para determinar si están funcionando de manera adecuada. Se deben generar informes del desempeño de la operación del MSPI, con la revisión y verificación continua de los controles implementados. Tambien se generan informes de auditorías de acuerdo a lo establecido en el plan de auditorías de la entidad. Se realizan pruebas de efectividad en la Entidad, para detectar vulnerabilidades (físicas, lógicas y humanas) y accesos no autorizados a activos de información críticos.	Administrativas	AD.6.2	80	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MAYOR
R43	n/a	1) Se realizan pruebas y ventanas de mantenimiento (simulacro), para determinar la efectividad de los planes de respuesta de incidentes, es 60. 2) Si La Entidad aprende continuamente sobre los incidentes de seguridad presentados, es 80.	Tecnicas	T.7.1.6	80	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE
R44	n/a	Se realizan pruebas a las aplicaciones o software desarrollado "in house" para determinar que umplen con los requisitos de seguridad y privacidad de la información	Tecnicas	T.6.2.8	80	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE
R45	n/a	Registro de actividades en seguridad (bitácora operativa).	Tecnicas	T.4.4.1	100	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R46	n/a	1) Elaboración de planes de mejora es 60 2) Se implementan las acciones correctivas y planes de mejora es 80	PHVA	M.2	100	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R47	n/a	1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes es 80	Tecnicas	T.7.1.5	80	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE
R48	n/a	Gestión de acceso de usuario.	Tecnicas	T.1.2	87	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R49	n/a	Control de acceso a sistemas y aplicaciones	Tecnicas	T.1.4	84	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R50	n/a	Controles Criptográficos	Tecnicas	T.2.1	90	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R51	n/a	Consideraciones de las auditorías de los sistemas de información.	Tecnicas	T.4.4	90	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R52	n/a	Seguridad en la operativa, registro de actividad y supervisión.	Tecnicas	T.4.7	80	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE
R53	n/a	Cumplimiento de los requisitos legales y contractuales.	Administrativas	AD.6.1	85	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
E GESTIONADO CUANTITATIVAMENTE					956	0		0		0		660	CUMPLE	880	CUMPLE
R55	n/a	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Administrativas	AD.5.1.3	100	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR
LIMITE DE MADUREZ OPTIMIZADO					1852									1660	CUMPLE