025914

350.101
Ch52fpm
2010
Doc.f
c.2

ANEXOS

BIBLIOTECA
"JAIME ANDRÉS CRISPI LAGO"
DIRECCIÓN DE PRESUPUESTOS
MINISTERIO DE HACIENDA

TEATINOS 120 PRIMER PISO SANTIAGO - CENTRO

34214

GOBIERNO DE CHILE

DESCRIPCIÓN DE CAMPOS

Red de Expertos
Subsecretaría del Interior - División
Dirección de Presupuestos - División

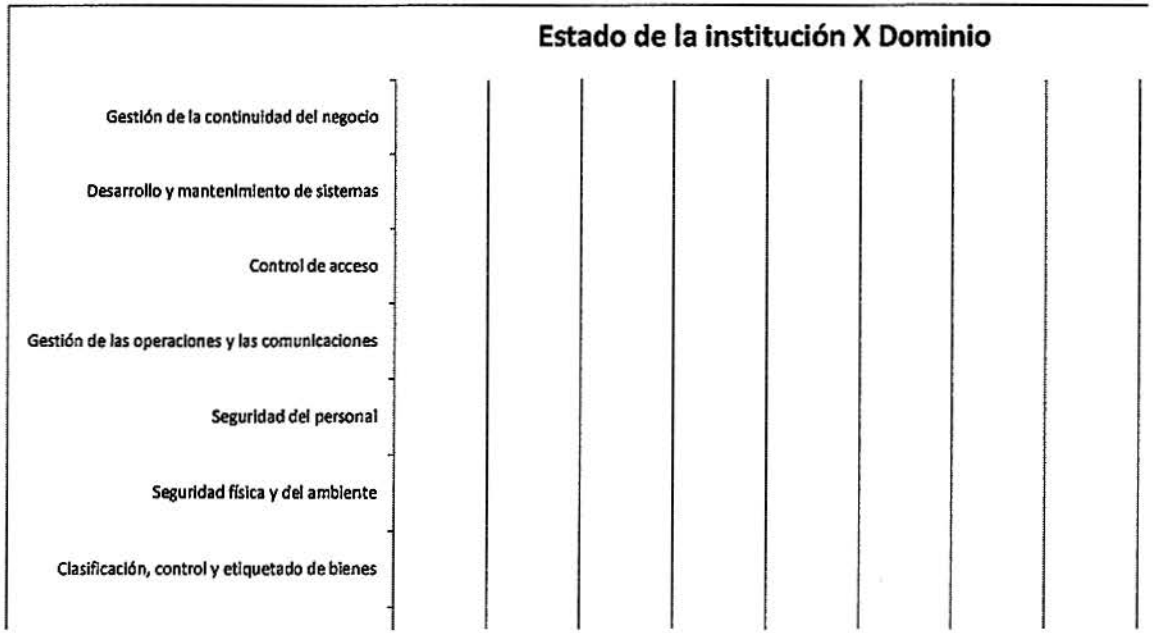
DOMINIO	PARRAFO	ARTICULO	SUB CATEGORIA	DEFINICION	COMPLETITUD	DESCRIPCION DEL ESTADO ACTUAL	DESCRIPCION DE LA BRECHA	ESTRATEGIA PRELIMINAR	OBJETIVOS ESPECIFICOS (CORTO PLAZO)	DOCUMENTO REFERIDO	RESPONSABLE ASIGNADO	SISTEMA / PROYECTO	RELACION CON GOBIERNO ELECTRONICO
1	-		-	2	3	4	5	6	7	8	9	10	11

1. Campo en el cual se concentra (agrupa) en dominios, la información a evaluar para el actual PMG de seguridad de la información.
2. Texto extraido del Decreto supremo N° 83, el cual correspode , dentro del dominio, a lo que el encargado de seguridad de la información deberá evaluar dentro de la institución.
3. Espacio habilitado para la evaluación (ver tabla Criterios) de la institución en relación a cada uno de los artículos del DS-83
4. Descripción de cómo se encuentra actualmente la institución en relación a lo descrito en el artículo analizado
5. Descripción de lo que estaría faltando el a institución para poder cumplir con lo solicitado en el artículo analizado
6. Que debería realizar la institución para poder cumplir con lo solicitado en el artículo analizado
7. Descripción de las tareas especificas que la institución deberá realizar para poder cumplir con lo solicitado en el artículo analizado
8. Documentos que servirá de evidencia y respaldo para cada uno de los elementos evaluados
9. Designación de el o los responsables para realizar el análisis de los artículos
10. Descripción de algún sistema o proyecto (preliminar) que permita disminuir/mitigar la brecha
11. Describir si la solución existe o se debe implementar dentro de pmg gobierno electrónico.

GOBIERNO DE CHILE

RESUMEN PMG

DOMINIO	COMPLETITUD
Políticas de seguridad	0
Seguridad organizacional	0
Clasificación, control y etiquetado de bienes	0
Seguridad física y del ambiente	0
Seguridad del personal	0
Gestión de las operaciones y las comunicaciones	0
Control de acceso	0
Desarrollo y mantenimiento de sistemas	0
Gestión de la continuidad del negocio	0
ESTADO DE LA INSTITUCIÓN (DIAGNÓSTICO)	0



GOBIERNO DE CHILE

RESUMEN PMG

	Seguridad organizacional								

GOBIERNO DE
CHILE

CRITERIOS DE EVALUACIÓN

Sut
Dire

VALOR	TIPO	DESCRIPCIÓN
0	No cumple	La Institución no cuenta con procedimientos, sistemas, controles u otro que le permita cumplir con el DS-83.
1	Cumple Parcial	La institución cuenta con algunos o varios procedimientos, sistemas, controles u otros que le permita cumplir con el DS-83.
2	Cumple	La institución cuenta con todos los controles, procedimientos, sistemas u otros requeridos por el DS-83

CHILE

MATRIZ DE DIAGNÓSTICO

Red de Expertos
Subsecretaría del Interior - División Informática
Dirección de Presupuestos - División Tecnologías de Información

No cumple	0
Cumple Parcial	1
Cumple	2

Inmediato
Mediano Plazo
Largo Plazo

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	2	11	-	Deberá establecerse una política que fije las directrices generales que orienten la materia de seguridad dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional. La política de seguridad deberá incluir, como mínimo, lo siguiente:										
	2	11	a	Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia.										
	2	11	b	La difusión de sus contenidos al interior de la organización.										
	2	11	c	Su reevaluación en forma periódica, a lo menos cada 3 años. Las políticas de seguridad deberán documentarse y explicitar la periodicidad con que su cumplimiento será revisado.										
[illegible]	3	12	-	En cada organismo regido por esta norma deberá existir un encargado de seguridad, que actuará como asesor del Jefe de Servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos. Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá tener, a lo menos, las siguientes funciones:										
	3	12	a	Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación.										
	3	12	b	Coordinar la respuesta a incidentes computacionales.										
	3	12	c	Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.										

MATRIZ DE DIAGNÓSTICO

Red de Expertos
Subsecretaría del Interior - División Informática
Dirección de Presupuestos - División Tecnologías de Información

[illegible]

[illegible]	
No cumple	0
Cumple Parcial	1
Cumple	2

[illegible]
Inmediato
Mediano Plazo
Largo Plazo

[illegible]	[illegible]	[illegible]	[illegible]	DEFINICIÓN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	4	13	-	Los documentos electrónicos y sistemas informáticos deberán clasificarse y etiquetarse para indicar la necesidad, prioridad y grado de protección. [illegible]										
	4	14	-	Todo documento electrónico deberá ser asignado, [illegible]										
	4	15	-	Para cada clasificación, el encargado de seguridad deberá proponer los procedimientos [illegible]										
	4	15	a	Copiado										
	4	15	b	Almacenamiento										
	4	15	c	Transmisión por correo electrónico y sistemas [illegible]										
	4	15	d	Destrucción										
	4	16	-	[illegible]										
[illegible]	5	17	-	Los equipos deberán protegerse físicamente de las amenazas de riesgos del ambiente externo, pérdida o daño, [illegible]										
	5	17	-	[illegible]										
	5	17	a	[illegible]										
	5	17	b	[illegible]										
	5	17	c	[illegible]										
	5	18	-	[illegible]										
	5	18	a	[illegible]										
	5	18	b	[illegible]										

[redacted]

No cumple	0
Cumple Parcial	1
Cumple	2

Inmediata
Mediano Plazo
Largo Plazo

NUMERO			DEFINICION										
5	20	-	*El Jefe de Servicio deberá impartir instrucciones para la seguridad de los documentos electrónicos y los sistemas informáticos, respecto de los siguientes materias*	[redacted]									
6	20	a	Uso de sistemas informáticos, los deberes en prohibición de instalación de software no autorizado, documentos y archivos electrónicos en el correo interno										
6	20	b	Uso de la red interna, uso de internet, uso del correo electrónico, acceso a personas externas, mensajes encriptados, sanciones de incumplir y fecha/duración/retraso y otros.										
6	20	c	Clasificación, tratamiento, manejo, almacenamiento y almacenamiento de documentos electrónicos										
6	20	d	Procedimientos para historial/ bitácoras de actividad										
6	21	-	Los responsables/roles de seguridad aplicables al personal deberán ser explicitados en la etapa de selección o visibilidad adjuntando en los mismos o mecanismos de mantenimiento a en las correspondientes normativas										
7	22	-	*Se todos los organismos sujetos a la presente norma, deberán capacitarse y difundirse los siguientes procedimientos e información*	[redacted]									
7	22	c	Los contactos de nuevo son difundidos mediante o mecánicamente trasladados de personas informáticas										
7	22	b	Los supervisores palabras y la confidencia por los fracasos de software y la protección del uso de software no autorizado										
7	23	a	Los buenos prácticas para protegerse de los riesgos asociados a la utilización de profesor y software a través de los datos de telecomunicaciones, o por otros medios, indicando qué medidas de seguridad se deberán adoptar										
7	23	-	*Para los efectos de indicar el riesgo de ciberataque a que son sujetos de los sistemas, deberán adherirse políticas de segregación de funciones. Asimismo, deberán documentarse los procedimientos de operación de sistemas informáticos e incorporarse mecanismos periódicos de auditoría de la integridad de los registros de clave criptográfica en dispositivos electrónicos.*	[redacted]										
7	24	-	*En los lugares regidos por la presente norma, deberán realizarse copias de respaldo de la información y los aplicativos críticos para la salida de la institución en forma periódica, así posteriormente con los siguientes medios*	[redacted]									
7	24	a	La periodicidad con que se realizarán las respaldo de los computadores personales de la institución que estén asignados a usuarios, deberá explicarse y no podrá ser menor a 1 respaldo anual.										
7	24	b	La periodicidad con que se realizarán las copias de los sistemas informáticos y los equipos no contemplados en el punto anterior, utilizados en el procesamiento o almacenamiento de documentos electrónicos, deberá establecerse y no podrá ser menor a 1 respaldo semanal.										
7	24	c	Deberá garantizarse la disponibilidad de información adecuada de respaldo, para asegurar que estos sean expedidos antes después de un desastre o la falla de un dispositivo. Los configuradores de respaldo para los sistemas institucionales deberán ser probados con regularidad, o lo menos cada 2 años, para asegurar que ellos cumplirán los requisitos establecidos en los planes de continuidad mediamente.										
7	24	d	Deberá almacenarse en una ubicación remota, un nivel mínimo de información de respaldo, junto con registros exactos y completos de las copias de respaldo y los procedimientos documentados de restablecimiento. Esta ubicación deberá estar ampliada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. En términos ordinarios para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo.										
7	24	e	Los respaldos deberán cumplir con un nivel apropiado de protección físico de los medios, considerando para las prácticas aplicadas en el sitio principal. Los controles ofrecidos a los dispositivos del sitio de respaldo deberán extenderse para alcanzar el sitio de respaldo.										
7	24	f	Deberán mantenerse claves de encripción de los respaldos de la información, así como mantener mecanismo de restauración de respaldo que estén correctamente operativos y										
7	24	g	Deberán utilizarse medios y procedimientos claros de almacenamiento que garanticen una vida útil adecuada de los datos definidos en el plan respectivo.										
7	25	-	*Las instituciones regidas por la presente norma deberán impartir instrucciones respecto al uso seguro del correo electrónico. Estas instrucciones deberán incluir al menos*	[redacted]									
7	25	d	Una advertencia sobre la vulnerabilidad del correo electrónico y mecanismos a asumirse en subsanarlos;										
7	25	b	Una advertencia sobre los peligros asociados a la apertura de archivos adjuntos sin a la veracidad de procesos que se realice un correo electrónico;										
7	25	c	La responsabilidad de no alterar características de correos el correo electrónico;										
7	25	d	Una advertencia sobre la suplantación de elementos personales de correos el correo electrónico en el correo, especialmente donde el cual se expida el correo electrónico;										
7	25	e	Instrucciones sobre la situación de sospechosos respecto de acceso al correo electrónico;										
7	25	f	Una responsabilidad sobre la autenticidad de que los usuarios tienen cuenta de correo electrónico deberán ser claves de su uso personal										
7	25	g	Un instructivo de materia en usar el correo electrónico;										
7	25	h	Una advertencia sobre la necesidad de encriptar el envío documentos, archivos y cualquiera material firma electrónica; e										
7	25	i	Una prohibición de los responsabilidades que corresponderán a los usuarios en caso de comprometer a la institución, por ejemplo, con el envío de correos electrónicos difamatorios, uso para hostigamiento sexual, behavior no autorizado, etc.										
7	26	-	*Los encargados deberán a la seguridad interna, así la medida de sus posibilidades, deberán*	[redacted]									
7	26	a	Instalar un antivirus que analice frente a la posibilidad de ataques vía correo electrónico, software malicioso;										
7	26	b	Proveer mecanismos que mediante el uso de técnicas de cifrado, permitan proteger la confidencialidad e integridad de los documentos electrónicos;										
7	26	c	Evitar el uso de cuentas de correo personal;										
7	26	d	Desarrollar mecanismos adicionales para la verificación de emisión y que no se realice suplantación;										
7	26	e	Verificar que todos los equipos informáticos y medios digitales que sean usados en el almacenamiento y/o procesamiento de documentos electrónicos, de sus predios, sean adecuadamente previo a ser dados de baja.										
8	27	-	*El campo de identificador formal de subsiguiente constituye un componente básico para el uso de firma electrónica.* *Los identificadores son un componente de validación de la identidad del usuario para acceder a un sistema informático.* *Un identificador temporal es aquel que se asigna a un usuario la primera vez que accede a un sistema, y que debe ser modificado por este en su primer acceso.* *Los sistemas informáticos deberán configurarse de manera que los nuevos no sean reconocidos a temprano; así los administradores en los nuevos ordenadores.*	[redacted]										
8	28	-	La asignación de los identificadores se deberá realizar mediante un proceso formal de gestión, en que el jefe directo del usuario peticionario sea el responsable de la respectiva solicitud. *Para los efectos del referido control, en cada institución se impartirán instrucciones sobre la forma de asignación de identificadores que se aplicará. Dichas instrucciones deberán incluir a lo menos lo siguiente:*	[redacted]									
8	28	a	La obligación de mantener en forma confidencial de los identificadores que se asignen;										
8	28	b	La prohibición de no mantener los identificadores en papel;										
8	28	c	La prohibición de almacenar identificadores en un computador de manera desprotegida;										
8	28	d	El deber de no mantener los identificadores de usuarios inhabilitados;										
8	28	e	El cambio de la total el identificador en ausencia durante de días de cada actividad, sin excepción, almacenada en una clave;										
8	28	f	La inhabilitación de ocultar los identificadores cuando hayan indicios de un posible compromiso del identificador o del sistema;										
8	28	g	La caracterización de cómo identificadores que tengan una longitud mínima de ocho caracteres; sean fáciles de recordar; combinen letras, mayúsculas, dígitos, y caracteres de puntuación; no estén basados en algún dato o de fácil deducción o parte de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, estado de identidad, fecha de nacimiento; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos; y no sean palabras de diccionario o nombres comunes;	[redacted]										
8	28	h	La inhabilitación de ocultar los identificadores a intervalos regulares. Las contraseñas de sesiones privilegiadas se deberán cambiar más frecuentemente que las identificadores normales;	[redacted]									
8	28	i	Normas para evitar el registro de identificadores vistos; e										
8	28	j	La prohibición de guardar el identificador temporal al crear la primera sesión.										
8	29	-	Se deberá asignar a los usuarios identificadores temporales de una manera segura. Específicamente, se deberá evitar el uso de terceras partes o mensajes de correo electrónico sin protección (texto en claro) para comunicar el identificador. *Los usuarios deberán dar un acuse recibo de recepción del identificador.*	[redacted]									
8	30	-	*En caso que los usuarios necesiten acceder a múltiples servicios o plataformas y sea necesario que mantengan múltiples identificadores, deberán ser notificados de que sólo deben ser distintos, si pudieran, se implantará y facilitará el uso de certificados de firma electrónica.*	[redacted]									
8	31	-	*Para reducir el riesgo de accesos no autorizados a documentos electrónicos y sistemas informáticos, se deberá promover buenas prácticas, como las de puesto limpio.* *En particular, se brandeberá a los usuarios a asegurar los sistemas de manera que no sea suplantados y los abusos a o atacantes.*	[redacted]									
		a	Cerrar las sesiones activas en el computador cuando se finalice la labor, a menos que estas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con protector de pantalla con una contraseña protegida;										
		b	Cerrar las sesiones de los equipos clientes principales cuando la sesión finalice, a que se efectúe reconectando, aunque el terminal o la sesión; y										
		c	Asegurar los terminales o equipos fuera de uso no autorizado, mediante una contraseña de bloqueo o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se usa.										
9	32	-	*Se deberá controlar el acceso y los cambios de red internos y externos mediante el uso de identificadores o certificados digitales.* *Por tal efecto, los Artículos de la Administración del Estado deberán y la ley más normativa deberán abstenerse a los atacantes o atacantes:*	[redacted]									
9	32	a	Restringir la instalación de equipamiento personal que difiera el control de acceso a documentos electrónicos y sistemas informáticos, de manera acorde a las políticas de seguridad de la institución; y										
9	32	b	Mantener un registro del equipamiento que permita la conexión, distribución e implantación media de información, y de los terceros con derechos de acceso a ellos.										
9	33	-	*Las instituciones regidas por la ley serán norma implantarán mecanismos para controlar el uso de redes y servicios de red que, al menos, consideren lo siguiente:*	[redacted]									
9	33	a	Las redes y servicios de red a los que el acceso está permitido;										
9	33	b	Los procedimientos de autorización para determinar quién tiene permiso acceder a los distintos redes y servicios de red; e										
9	33	c	Los controles de gestión y procedimientos para proteger el acceso a los conexiones de la red y servicios de red.										

MATRIZ DE DIAGNÓSTICO

ÍNDICE

[illegible]

[illegible]	
No cumple	0
Cumple Parcial	1
Cumple	2

[illegible]
Inmediato
Mediano Plazo
Largo Plazo

[illegible]	[illegible]	[illegible]	[illegible]	DEFINICIÓN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	9	34	-	Aquellos organismos que requieran preservar que la seguridad esté incorporada en los sistemas en la etapa de diseño, se entenderán como organismos complejos y para tal efecto, deberán adoptar los indicadores contenidos en la sección correspondiente del Título V de esta norma, sobre el Nivel Avanzado de Seguridad para el Documento Electrónico.										
[illegible]	10	36	-	El encargado de seguridad deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la institución. Este plan deberá, como mínimo, disponer la efectiva gestión de los recursos públicos, la eficiente coordinación con las autoridades apropiadas, como policía, bomberos, autoridad directiva, etc., y mecanismos eficaces para comunicar a quienes sean los responsables de los documentos electrónicos y sistemas informáticos afectados.										

GOBIERNO DE
CHILE

NOMBRE PROYECTO	Dominio PMG SSI	Proyecto PMG Gobierno Electrónico relacionado

DECRIPCIÓN

CARTERA DE PROYECTOS / ACTIVIDADES

EVIDENCIA DE CUMPLIMIENTO	OBJETIVO ESPECIFICO

RESPONSABLE	FECHA ESTIMADA INICIO	FECHA ESTIMADA TERMINO	PRIORIDAD	PRESUPUESTO	PERSONAL INVOLUCRADO

Red de Expertos
el Interior - División Informática
uestos - División Tecnologías de

REQUIERE ASESORIA EXTERNA	COMENTARIOS

Dominio	DS 83	DS 77	DS 81	DS 93	DS 100	DS 158	I.P. 5	I.P. 6	I.P. 8	Ley 17336	Ley 19223	Ley 19628	Ley 19799	Ley 19927	Ley 19880	Ley 2021
Dominio 1 Política de seguridad de la información	Art. 11 Art. 37		Art. 15 Art. 29	Art. 2			II. 1. b)									Art. 11 Art. 33 Art. Déci
Dominio 2 Organización de la seguridad de la información	Art. 12 Art. 10 Art. 37	Art. 3		Art. 2 Art. 5	Art. 6		II. 1. b) II. 2. g) II. 4 II. 6. i)	3. 4. b. 4. d. 4. e.	II. 4. II. 6.		Art. 4	Art. 7 Art. 11	Art. 9 Art. 10 Art. 11 Art. 12 Art. 17 Art. 18 Art. 21 Art. 23	Art. 1 N°18 Art. 2 N°2		Art. 3 Art. 11 Art. 16 Art. 20 Art. 26 Art. 31 Art. 32 Art. 33 Art. 34 Art. 35 Art. 1 tra Art. Déci
Dominio 3 Gestión de activos	Art. 13 Art. 14 Art. 15 Art. 16 Art. 37	Art. 7 Art. 9	Art. 9 Art. 10 Art. 13 Art. 14 Art. 16 Art. 17 Art. 18 Art. 19 Art. 20 Art. 21 Art. 22 Art. 23 Art. 24 Art. 26 Art. 27		Art. 4										Art. 7 Art. 18	Art. 2 Art. 2
Dominio 4 Seguridad de recursos humanos	Art. 20 Art. 21 Art. 37			Art. 1 Art. 2 Art. 9			II. 2. f) II. 6. b) II. 6. h)	4. a. 4. d.			Art. 4	Art. 7	Art. 11 Art. 12 Art. 16 Art. 17 Art. 18 Art. 20 Art. 23	Art. 2 N°2 Art. 7 b)		Art. 3 Art. Déc

Dominio 5 Seguridad física y ambiental	Art. 17 Art. 18 Art. 19 Art. 26 Art. 37			Art. 4 Art. 5									Art. 17			
Dominio 6 Gestión de las comunicaciones y operaciones	Art. 7 Art. 10 Art. 15 Art. 22 Art. 23 Art. 25 Art. 26 Art. 24 Art. 37	Art. 3 Art. 4 Art. 5 Art. 6 Art. 7 Art. 8 Art. 9 Art. 12	Art. 1 Art. 2 Art. 3 Art. 7 Art. 15	Art. 1 Art. 2 Art. 5 Art. 6 Art. 7 Art. 9	Art. 1 Art. 2 Art. 3 Art. 4 Art. 9 Art. 11 Art. 12 Art. 13		II. 2. f) II. 2. g) II. 5. d) II. 6. c)	4. b. iii. 4. c. ii. 4. c. iii. 4. c. iv.	II. 5.	Art. 47		Art. 4 Art. 5 Art. 12 Art. 17 Art. 18 Art. 19 Art. 22	Art. 8 Art. 12 Art. 18 Art. 19 Art. 20 Art. 23 Art. 24	Art. 1 N°18 Art. 2 N°2 Art. 3 a)	Art. 5 Art. 14 Art. 19 Art. 30 Art. 39 Art. 46 Art. 48 Art. 58 Art. 59 Art. 65	Art. 4 Art. 5 Art. 6 Art. 7 Art. 1(Art. 1 Art. 1 Art. 3 Art. Cua Art. Oct
Dominio 7 Control de acceso	Art. 9 Art. 18 Art. 27 Art. 28 Art. 29 Art. 37 Art. 30 Art. 31 Art. 32 Art. 33	Art. 11					II. 5. e) II. 6. d)	4. b. ii. 4. c. i. 4. c. ii. 4. c. iii.			Art. 1 Art. 2 Art. 3		Art. 1 Art. 14 Art. 15 Art. 16			
Dominio 8 Adquisición, desarrollo y mantenimiento de los sistemas de información	Art. 26 Art. 37		Art. 7 Art. 15 Art. 20	Art. 2 Art. 8	Art. 2 Art. 5		II. 6. f) II. 6. g)				Art. 1 Art. 2 Art. 3 Art. 4		Art. 17			Art. 1
Dominio 9 Gestión de un incidente de seguridad	Art. 12	Art. 8	Art. 13									Art. 5 Art. 16 Art. 23	Art. 5 Art. 9 Art. 13 Art. 19	Art. 1 N°18 Art. 2 N°2 Art. 2 N°3 Art. 3 b)	Art. 35	Art. 2 Art. 2 Art. 2 Art. 2 Art. 4 Art. 4 Art. 4 Art. 4 Art. Sép

																Art. Nov
Dominio 10 Gestión de la continuidad del negocio	Art. 7 Art. 35 Art. 37				Art. 7								Art. 12 Art. 16 Art. 18		Art. 9 Art. 19	
Dominio 11 Cumplimiento	Art. 7 Art. 22	Art. 1 Art. 2 Art. 6 Art. 8 Art. 13	Art. 4 Art. 7 Art. 12	Art. 2 Art. 3 Art. 8	Art. 1 Art. 2 Art. 4 Art. 9		II. 2. e) II. 5. d) II. 5. e) II. 6. b) II. 10	1. 2. 4. a.	II. 2. II. 3. II. 7.	Art. 3 Art. 8 Art. 37 bis Art. 45 Art. 47	Art. 1 Art. 2 Art. 3	Art. 1 Art. 3 Art. 5 Art. 7 Art. 9 Art. 10 Art. 11 Art. 13 Art. 15 Art. 16 Art. 18 Art. 20 Art. 21 Art. 23 Art. 1 trans. Art. 2 trans.	Art. 1 Art. 3 Art. 6 Art. 9 Art. 12 Art. 19 Art. 23	Art. 1 N°18 Art. 1 N°21 Art. 1 N°22 Art. 2 N°2 Art. 2 N°3 Art. 3 b)		Art. 7 Art. 1 Art. 1 Art. 2 Art. 2 Art. 3 Art. Qui Art. Se Art. Sépt Art. Nov Art. Déc

- *: DS 158 Modifica a DS 81 en ámbito de aplicación, en cuanto a que excluye a municipalidades, empresas del Estado y Universidades públicas. Además modifica los plazos, por lo cual, se entiende que la aplicación de los dominios es igual a la del DS 81.

Definiciones a tener en consideración – Etapa I Diagnóstico

Activo
Cualquier cosa que tenga valor para la organización.

Amenaza
Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.

Análisis del riesgo
Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Controles
Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.
NOTA: El control también se utiliza como sinónimo de salvaguarda o contramedida.

Evaluación del riesgo
Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evento de seguridad de la información
Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Gestión del riesgo
Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
NOTA: La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

Incidente de seguridad de la información
Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Lineamiento
Una descripción que aclara qué se debe hacer y cómo, para lograr los objetivos establecidos en las políticas.

Medios de procesamiento de la información
Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Política
Intención y dirección general expresada formalmente por la autoridad máxima en la institución.

Riesgo
Combinación de la probabilidad de un evento y su ocurrencia.

Seguridad de la información
Preservación de confidencialidad, integridad y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.

Terceros Relevantes
Persona u organismo reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

Tratamiento del riesgo
Proceso de selección e implementación de medidas para modificar el riesgo.

Vulnerabilidad
Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Definiciones a tener en consideración – Etapa II Planificación

Indicador
Es una herramienta que captura determinadas características del dominio analizado, involucra variables asociadas a los problemas u oportunidades detectadas en el diagnóstico y, por lo tanto, constituyen una definición operativa de los objetivos del proyecto o actividad para el dominio correspondiente.

Algunos elementos a considerar para esta etapa son:

- Claridad en los objetivos.
- Compromiso realista, en términos del tiempo y presupuesto disponibles.
- División del trabajo, de acuerdo con los objetivos definidos.
- Precisión en el alcance de las decisiones.
- Perfil del recurso humano requerido para el desarrollo de las actividades, la jefatura del proyecto, el control, seguimiento y la ejecución.
- Clima y cultura organizacional que podría presentar resistencia a la implantación de políticas de seguridad.
- Consideración de la carga de trabajo y responsabilidades asociadas de las áreas a intervenir.
- Difusión oportuna de la planificación.

Línea base
Corresponde a la medición de la situación actual o al valor de los indicadores antes de implementar el proyecto o actividad. Permite tener una idea precisa de la magnitud o cualidades del problema abordado, definir de mejor manera un estado deseable y, al comparar ambos estados, saber de qué manera el proyecto o actividad implementada contribuyó al logro de los objetivos planteados disminuyendo la brecha inicial capturada en la etapa de diagnóstico.

Objetivo
Es la definición de lo que se espera como consecuencia de la realización de determinadas actividades o la implementación acabada de un proyecto. Dicha definición debe mostrar cómo el proyecto o actividad contribuye al mejoramiento de la gestión, y puede ser operacionalizada en función de un conjunto de variables que la representen.

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

INSTITUCION

FECHA DE GESTACION

NOTA DE CONFIDENCIALIDAD

Especificar una nota de confidencialidad estándar de acuerdo a la normativa vigente en la institución

CONTROL DE VERSIONES

Insertar cuadro de control de versionamiento y cambios a la política

I.- DECLARACION INSTITUCIONAL

Especificar la declaración institucional de seguridad de la información de acuerdo a la normativa generada internamente en el servicio.

II.- OBJETIVOS DE LA GESTION DE SEGURIDAD DE LA INFORMACION

- Describir a modo general las acciones a realizar para la clasificación y catastro de activos de información.
- Describir a modo general las acciones necesarias para el análisis de Riesgo de acuerdo a la normativa vigente en la institución.
- Describir a modo general las acciones a realizar para la capacitación del personal.
- Describir la estructura para el marco de políticas, estándares y procedimientos en materia de seguridad de la información a ser desarrollados en la institución.

III.- ALCANCE O AMPLITUD DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

Describir los ámbitos a desarrollar en materia de seguridad de la información, como por ejemplo:

- Política General de Seguridad
- Política Correo Electrónico
- Política Uso de Internet
- Política Clasificación y Manejo de Información
- Etc.

IV.- ROLES Y RESPONSABILIDADES

Especificar los roles y responsabilidades del(os) comité(s) a crear dentro de la institución, y el rol del personal en materias de seguridad.

V.- MARCO GENERAL PARA LAS POLITICAS DE SEGURIDAD DE LA INFORMACION

Definir un marco general para la gestación de las políticas, considerando:

- Objetivos políticas de seguridad
- Formato de las Políticas
- Gestación de una Política
- Aprobación de Políticas
- Difusión de las Políticas
- Revisión de las Políticas

VI.- GLOSARIO DE TERMINOS

Incluir un glosario general de términos utilizados.

Nombre y firma de la autoridad máxima dentro de la institución

Informe de Diagnóstico

Introducción

Resumen ejecutivo

- *Políticas de Seguridad*

Descripción de las políticas de seguridad existentes en la institución, considerando al menos la existencia de:

  - Políticas
  - Estándares
  - Procedimientos internos

- *Seguridad Organizacional*

Descripción del nivel de gestión de seguridad existente en la institución, considerando la existencia de:

  - Un comité de Seguridad de la Información
  - Personal de Seguridad de la información (Gestión y TIC)

- *Clasificación, control y etiquetado de bienes*

Descripción del nivel de clasificación de la información existente en la institución

- *Seguridad Física y del ambiente*

Descripción de los controles existentes respecto a:

  - Seguridad Física
  - Seguridad de equipamiento de usuarios, y seguridad de acceso

- *Seguridad del Personal*

Descripción de las políticas de contratación, despido y creación de cuentas del personal.

- *Gestión de las operaciones y las comunicaciones*

Descripción del nivel de seguridad y controles existentes en las operaciones y las comunicaciones, considerando al menos:

  - Procedimientos técnicos y responsabilidades del personal
  - Administración de contratos con terceros
  - Protección contra virus y código malicioso
  - Estrategias de respaldos y administración de medios
  - Administración de la red
  - Sistemas de monitoreo