Directrices para la identificación de medidas de seguridad a partir de cumplimiento a controles

Enero 2025

DIRECTORIO

Av. Insurgentes Sur 3211, Col. Insurgentes Cuicuilco, C.P. 04530, Alcaldía Coyoacán, Ciudad de México.

Edición 2025.

Tabla de contenido

Sobre este documento

El presente documento retoma elementos de la propuesta por el Instituto para la gestión de riesgos, considerando el riesgo como elemento de trabajo en las dimensiones de confidencialidad, integridad y disponibilidad de los soportes en los que se almacenan los datos personales.

Esta actividad retoma el apartado de gestión de riesgos a partir de una base común para el personal con y sin experiencia, técnicos y no técnicos, que utilizan el proceso de gestión de riesgos en sus sistemas de tratamiento de datos personales y se encuentran realizando su documento de seguridad. Se busca que, al abordar el cumplimiento de un objetivo de seguridad, identifiquen cómo es posible definir una o diversas medidas de seguridad enfocadas en garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Es importante destacar que, debido a la diversidad de la composición de los sistemas de tratamiento, no es posible tener un listado genérico de medidas de seguridad. Por ello, es necesario identificar directrices que enlisten los objetivos de seguridad que pueden ser abordados con medidas de seguridad especificas por cada sujeto obligado, en función del contexto en el que se realicen los tratamientos de datos personales.

Este documento presenta ejemplos y no debe ser considerado como un formato o una guía especifica que proporcione soluciones a las medidas de seguridad físicas, tecnológicas y administrativas que deben ser implementadas por los sujetos obligados para cumplir con lo dispuesto en el marco normativo en materia de protección de datos personales para el sector público.

Medidas de seguridad

Este es el paso final de la evaluación de riesgos, ya que parte del cálculo del riesgo inherente. A partir de este valor se realiza una re-interpretación del riesgo mediante un analisis que identifica el contexto en el que la organización enfrente dicho riesgo, describiendo elementos que ayudarán a reasignar valores de impacto y/o a asignar valores de probabilidad de ocurrrencia a partir de registros, haciendo una nueva valoración del valor del riesgo pero ahora incluyendo y analizando la efectividad de las medidas de seguridad que se tienen implementadas.

Para llevar a cabo una valoración de manera efectiva, es necesario contar con una base de comparación que describa los objetivos de seguridad que deben satisfacerse con al menos una medida de seguridad, para así establecer un punto de análisis respecto a la eficiencia de la o las medidas de seguridad que se tienen implementadas al momento de realizar la valoración.

Control de seguridad y medida de seguridad son conceptos diferentes, la diferencia radica en su enfoque y aplicación dentro de un sistema de gestión de riesgos.

- Control de seguridad: Es un término más amplio que se refiere a cualquier acción, mecanismo, procedimiento o política implementada para minimizar o eliminar riesgos de seguridad. Puede incluir medidas preventivas, correctivas y de detección.

- Medida de seguridad: Se refiere específicamente a una acción concreta o tecnología utilizada dentro del marco de un control de seguridad. Es decir, una medida de seguridad es un componente específico dentro de un control de seguridad.

Es así que podemos decir que la medida de seguridad es el como se cumple con el objetivo de seguridad, es decir, la tarea, actividad o acción encaminada a cumplir con el objetivo del control, por ejemplo, control de seguridad puede ser la autenticación para cuidar la confidencialidad de la información y la medida de seguridad podría ser el uso de autenticación multifactor (MFA), como una combinación de contraseña y código enviado al teléfono móvil.

En este sentido, se desarrolló un tabla que enlista y clasifica diversos controles de seguridad, la cual es opcional en su uso ya que puede ser usada como referencia para esta actividad, en caso de contar con alguna base comparativa que se desee aplicar en este paso. Sin

embargo, las organizaciones deben asegurarse de que no pasaron por alto la implementación de medidas que permitan atender riesgos que posiblemente no hayan identificaron durante el análisis de riesgos.

Esta tabla parte del anáalisis y re interpretación de los siguientes documentos:

- Anexo D. "Ejemplos de Controles de Seguridad" de la *Guía para implementar un Sistema de Gestión de Seguridad de Datos Pesonales*[1].
- Anexo A. "Controles de la seguridad de la información de referencia del estandar UNE-ISO/IEC 27001:2023"[2].
- Estándar *ISO/IEC 27002:2022(en) Information security, cybersecurity and privacy protection — Information security controls27002*.[3]

[1] Disponible en: https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf, consultado el 10 de diciembre de 2024
[2] Disponible en: https://tienda.aenor.com/norma-une-iso-iec-27001-2023-n0071320, consultado el 10 de diciembre de 2024
[3] Disponible en: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en, consultado el 10 de diciembre de 2024

Anexo de ejemplos

Esta tabla ejemplifica cómo se relaciona el objetivo de seguridad con medidas de seguridad orientadas a cumplir con dicho objetivo. Estos son solo ejemplos y no representan una lista exhaustiva de medidas de seguridad, ni deben ser consideradas como medidas de seguridad completas para el cumplimiento del deber de seguridad en el apartado de análisis de brecha.Son simplemente ejemplos para servir como referencia en el desarrollo del análisis de brecha propio.

Abreviaturas utilizadas:

- MSA – Medida de seguridad administrativa
- MSF – Medida de seguridad fisica
- MST – Medida de seguridad tecnológica

Núm.	Nombre	Descripción / Justificación	Ejemplo de Medidas de seguridad	Evidencia
Políticas de seguridad de la información				
	Directrices establecidas por la dirección para la seguridad de la información	Objetivo: Brindar orientación y apoyo por parte de quienes se encargan de la gestión de la seguridad, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección,	MSA: Política general de seguridad de la información aprobada por Comité de Transparencia.	

		publicada y comunicada a los empleados y partes externas pertinentes.	MSA: Socialización de la política a los perfiles definidos en funciones y obligaciones. MSA: Programa general de capacitación conforme al apartado de funciones y obligaciones	
2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	MSA: Calendario de monitoreo y revisión a las medidas de seguridad administrativas. MSA: Calendario de monitoreo y revisión de los resultados de la política de seguridad de datos personales. MSA: Actualización del documento de seguridad MSA: Plan de trabajo actualizado conforme a las necesidades identificadas en las fases compuestas por la gestión de riesgos.	
Organización de la seguridad de la información				

	Organización interna	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
3	Roles y responsabilidades para la seguridad de información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	MSA: Apartado del documento de seguridad de funciones y obligaciones.	
4	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	MSA: Entrega de información respecto al rol que desempeñara cada actor en el tratamiento de datos personales. MST: Definición de usuarios y contraseñas con restricciones de permisos. MST: Administración de actividades en función de roles definidos.	
5	Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.	MSA: Obtención de directorio de áreas de atención, investigación, verificación y acompañamiento en la materia de seguridad de datos personales.	

			MST: Implementación de solución tecnológica de comunicaciones entre áreas y órganos de toma de decisiones. MST: Definición de correo único para comunicaciones de vulneraciones al exterior de la institución.	
6	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	MSA: Celebración de convenios de adhesión a CERT. MSA: Generación de un equipo de respuesta a incidentes.	
7	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.	MSA: Política de privacidad desde el diseño de una solución tecnológica.	
	Dispositivos móviles y teletrabajo	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
8	Política para dispositivos móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	MSA: Política de uso de dispositivos móviles. MST: Configuración de dispositivos móviles de trabajo.	

			MST: Administración de conexión de dispositivos móviles a la red. MSF: Revisión y registro de dispositivos externos en una bitácora.	
9	Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	MSA: Política de tratamiento de datos personales en teletrabajo. MST: Configuración de VPN MST: Configuración de escritorio remoto MST: Configuración de firewall. MST: Validación de cambios desde puntos de conexión remotos. MST: Configuración de accesos remotos. MSF: Entrega y configuración de dispositivos electrónicos.	

Seguridad de los recursos humanos				
	Antes de asumir el empleo	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
10	Política para dispositivos móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	MSA: Política de uso de dispositivos móviles. MST: Configuración de dispositivos móviles de trabajo. MST: Administración de conexión de dispositivos móviles a la red.	
11	Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	MST: Cifrado de bases de datos. MST: Configuración de puntos de conexión remotos. MST: Configuración y control de accesos externos. MST: Configuración y restricción de sesiones simultaneas.	
12	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo	MSA: Directrices para la contratación de personal.	

		con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.		
13	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	MSA: Celebración de acuerdos de confidencialidad durante la prestación de servicios. MSA: Política de borrado seguro de la información. MSA: Socialización de perfiles y privilegios que tendrán como parte del sistema de tratamiento.	
	Durante la ejecución del empleo	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
14	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	MSA: Celebración de convenios que integren la protección de datos personales como un capítulo específico.	

15	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	MSA: Programa general de capacitación. MSF: Identificación de reglas y lineamientos en espacios en los que se llevan a cabo tratamiento de datos personales.	
16	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	MSA: Política de medidas de apremio por omisión a las medidas de seguridad. MSA: Proceso de vista a órganos internos de control o puesta a disposición de autoridades por exposición de información realizada intencionalmente y con dolo. MSA: Política restricción en el sistema de tratamiento por su mal uso. MSA: Política de capacitación para evitar eventos no intencionales a la seguridad.	

	Terminación o cambio de empleo	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.		
17	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	MSA: Política de contratación de personal	
Gestión de activos				
	Responsabilidad por los activos	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
18	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	MSA: Elaboración de inventario de sistemas de tratamiento de datos personales. MSA: Elaboración de listado de activos más utilizados. MSA: Elaboración de listado de vulnerabilidades más conocidas del listado de los activos identificados.	

			MSA: Elaboración de listado de amenazas más conocidas.	
19	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.	MSA: Elaboración de inventario de sistemas de tratamiento de datos personales. MSA: Elaboración de apartado de funciones y obligaciones del personal que trata datos personales.	
20	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	MSA: Elaboración de política de uso de dispositivos que serán utilizados para el tratamiento de datos personales. MSA: Registro en bitácoras de uso de dispositivos. MSF: Configuración de software y/o sistemas en función de la definición de funciones y obligaciones.	
21	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se	MSA: Política de contratación de personal.	

		encuentren a su cargo, al terminar su empleo, contrato o acuerdo.		
22	Clasificación de la información	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.	MSA: Manual para el desarrollo de la gestión de riesgos.	
23	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	MSA: Manual para el desarrollo de la gestión de riesgos.	
24	Etiquetado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	MSA: Manual para el desarrollo de la gestión de riesgos.	
25	Manejo de activos	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	MSA: Elaboración de política para el manejo de activos.	
26	Gestión de medios removibles	Control: Se deberían implementar procedimientos para la gestión de	MSA: Elaboración de políticas para el uso de dispositivos de	

		medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	almacenamiento de información que sea extraíble de su gestor de información (USB, Disco duro, tarjetas SD, CD, DVD, Blue-ray, unidades de almacenamiento extraíbles, etc)	
27	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	MSA: Elaboración de política de borrado seguro de la información. MSA: Elaboración de política de reasignación de equipos de cómputo. MSA: Elaboración de política de reasignación de dispositivos móviles.	
28	Transferencia de medios físicos	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	MSA: Elaboración de política de borrado seguro de la información.	
Controles de acceso				
	Requisitos del negocio para control de acceso	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		

29	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	MSF: Configuración de usuarios y contraseñas.	
30	Política sobre el uso de los servicios de red	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.		
	Gestión de acceso de usuarios	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
31	Registro y cancelación del registro de usuarios	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	MSA: Gestión de cambios a los servicios de terceros MSF: Eliminación de los derechos de acceso	
32	Suministro de acceso de usuarios	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	MSA: Política de asignación de usuarios y contraseñas acordes a funciones y obligaciones.	

33	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	MSF: Configuración de usuarios.	
34	Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	MSF: Configuración de autenticación de usuarios. MSF: Proceso de doble autenticación. MSF: Proceso de validación de identidad.	
35	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	MSF: Configuración de autenticación de usuarios.	
36	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	MSF: Eliminación de los derechos de acceso	
37	Responsabilidades de los usuarios	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda	MSF: Elaboración de bitácoras de uso de activos físicos.	

		de su información de autenticación.	MSF: Elaboración de bitácoras de uso de activos digitales.	
38	Uso de la información de autenticación secreta	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	MSA: Política de autenticación de usuarios	
39	Control de acceso a sistemas y aplicaciones	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.	MSF: Configuración de sesiones múltiples. MSF: Configuración de sesiones remotas. MSF: Configuración de cierre de sesiones múltiples.	
40	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	MSF: Configuración de privilegios a usuarios.	
41	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	MSF: Configuración de privilegios a usuarios.	

42	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	MSA: Política de generación y uso de contraseñas en sistemas informáticos. MSF: Configuración de control de contraseñas.	
43	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	MSF: Configuración de instalación de software. MSF: Configuración de registro de hardware.	
44	Control de acceso a códigos fuente de programas	Control: Se debería restringir el acceso a los códigos fuente de los programas.	MSA: Política de desarrollo de soluciones tecnológicas. MSF: Reglas de reprocesamiento de programación de software.	
Criptografía				
	Controles criptográficos	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
45	Política sobre el uso de controles criptográficos	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	MSA: Política sobre el uso de controles criptográficos. MST: Uso de contraseñas.	

			MST: Uso de criptografía en reposo. MST: Uso de criptografía en tránsito.	
46	Gestión de llaves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	MSA: Política de uso, protección y tiempo de vida de llaves criptográficas. MSA: Capacitación de uso de software.	
Seguridad física y del entorno				
	Áreas seguras	Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
47	Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	MSF: Personal de seguridad. MSF: Integración de seguridad perimetral. MSF: Control de accesos. MSF: Registro de visitantes. MSF: Identificación de usuarios para el acceso a instalaciones.	

48	Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	MSF: Control de accesos.	
49	Seguridad de oficinas, recintos e instalaciones	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	MSF: Cámaras de seguridad MSF: Resguardo seguro en espacios. MSF: Control de accesos.	
50	Protección contra amenazas externas y ambientales	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	MSA: Contratación de póliza contra daños. MSA: Programa de respuesta a incidentes.	
51	Trabajo en áreas seguras	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	MSA: Programa de respuesta a incidentes.	
52	Áreas de despacho y carga	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de	MSF: Control de accesos.	

		información para evitar el acceso no autorizado.		
	Equipos	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
53	Ubicación y protección de los equipos	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	MSA: Política de escritorio limpio. MSA: política de dispositivos desatendidos.	
54	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	MSF: Suministro de energía externo mediante UPS. MSF: Respaldo de conexión a suministro eléctrico.	
55	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	MSF: Cableado seguro de instalaciones eléctricas. MSF: Cableado seguro de instalaciones de red.	
56	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	MSA: Programa de actualización de equipos en materia de software. MSA: Programa de actualización de equipos en su hardware.	

			MSA: Política de destrucción y re-uso de componentes.	
57	Retiro de activos	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	MSF: Bitácora de uso de activos.	
58	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	MSA: Política de uso de equipos de cómputo y dispositivos móviles.	
59	Disposición segura o reutilización de equipos	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	MSA: Política de destrucción y re-uso de componentes.	
60	Equipos de usuario desatendidos	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	MSA: Política de activos desatendidos.	

61	Política de escritorio limpio y pantalla limpia	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	MSA: política de escritorio limpio. MST: Política de configuración de bloqueo automatizado.	
Seguridad de las operaciones				
	Procedimientos operacionales y responsabilidades	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
62	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	MSA: Funciones y obligaciones del personal que trata datos personales.	
63	Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	MSA: Política de gestión de cambios en sistemas informáticos.	
64	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al	MSA: Gestión de asignación de espacios de almacenamiento virtuales.	

		uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	MSA: Gestión de asignación de dispositivos de almacenamiento extraíble.	
65	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	MSA: Política de desarrollo de software seguro.	
	Protección contra códigos maliciosos	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
66	Controles contra códigos maliciosos	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	MST: Controles de red. MST: Controles contra código malicioso. MST: Controles contra software malicioso. MST: Controles de firewall.	
	Copias de respaldo	Objetivo: Proteger contra la perdida de datos.		
67	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba	MST: Configuración de respaldos automáticos.	

		regularmente de acuerdo con una política de copias de respaldo aceptada.	MSF: Ejecución de respaldos físicos.	
	Registro y seguimiento	Objetivo: Registrar eventos y generar evidencia.		
68	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	MSA: Elaboración de bitácora de vulneraciones.	
69	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	MSA: Elaboración de bitácora de vulneraciones.	
70	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	MSA: Elaboración de bitácora de vulneraciones.	
71	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	MST: Sincronización de relojes.	

	Control de software operacional	Objetivo: Asegurar la integridad de los sistemas operacionales.		
72	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	MSA: Configuración de instalación de software. MST: Restricción de instalación de software. MST: Configuración de actualizaciones automatizadas.	
	Gestión de la vulnerabilidad técnica	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
73	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	MSA: Elaboración de bitácora de vulneraciones.	
74	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	MSA: Política de instalación de software externo.	

			MST: Autorización para instalación y cambios a nivel de software.	
	Consideraciones sobre auditorias de sistemas de información	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.		
75	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	MSF: Registros de auditoría. MSA: Programa de auditoría. MSA: Programa de monitoreo y revisión.	
Seguridad de las comunicaciones				
	Gestión de la seguridad de las redes	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
76	Controles de redes	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	MST: Gestión de redes. MST: Configuración de redes MST: Configuración de sistemas y aplicativos.	

77	Seguridad de los servicios de red	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	MSA: Política de servicios de red suministrados por un proveedor. MST: Configuración de tablas de ruteo. MST: Asignación de IP para conexión.	
78	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	MST: Separación de redes	
79	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	MSA: Procedimientos de manejo de información: MSA: Acuerdos de intercambio de información.	
80	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	MST: Configuración de correo electrónico. MST: Configuración de criptografía en correo electrónico.	
81	Acuerdos de confidencialidad o de no divulgación	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los	MSA: Celebración de acuerdos de confidencialidad.	

		acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	MSA: Celebración de acuerdos de no divulgación.	
Adquisición, desarrollo y mantenimientos de sistemas				
	Requisitos de seguridad de los sistemas de información	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.		
82	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	MSA: Programa de mejora continua. MSA: Elaboración de plan de trabajo. MSA: Actualización de planes de trabajo.	
83	Seguridad de servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y	MST: Configuración de aplicaciones. MST: Restricción de tipos de redes (público/ privado).	

		divulgación y modificación no autorizadas.		
84	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	MST: Configuración de comunicaciones de datos personales.	
	Seguridad en los procesos de desarrollo y soporte	Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
85	Política de desarrollo seguro	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	MSA: Política de desarrollo de software. MSA: Política de privacidad desde el diseño.	
86	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	MSA: Elaboración de bitácora de vulneraciones.	

87	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	MST: Desarrollo de pruebas de calidad. MST: Desarrollo de pruebas de penetración. MST: Desarrollo de pruebas de seguridad.	
88	Restricciones en los cambios a los paquetes de software	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	MSA: Política de restricción a modificaciones de software.	
89	Principios de construcción de sistemas seguros	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	MSA: Política de diseño y desarrollo de software. MSA: Política de privacidad desde el diseño.	
90	Ambiente de desarrollo seguro	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el	MSA: Política de diseño y desarrollo de software. MSA: Política de privacidad desde el diseño.	

		ciclo de vida de desarrollo de sistemas.		
91	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	MSA: Política de tercerización de desarrollo. MSA: Política de entrega y liberación de soluciones tecnológicas.	
Relación con los proveedores				
	Seguridad de la información en las relaciones con los proveedores	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
92	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.	MSA: Política de seguridad de la información para las relaciones con proveedores	
93	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o	MSA: Política de seguridad de la información para las relaciones con proveedores	

		suministrar componentes de infraestructura de TI para la información de la organización.		
94	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	MSA: Política de seguridad de la información para las relaciones con proveedores	
	Gestión de la prestación de servicios con los proveedores	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
95	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	MSA: Política de seguridad de la información para las relaciones con proveedores	
96	Gestión de cambios en los servicios de proveedores	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la	MSA: Elaboración de bitácora de vulneraciones.	

		información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.		
Gestión de incidentes de seguridad de la información				
	Gestión de incidentes y mejoras en la seguridad de la información	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
97	Responsabilidad y procedimientos	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	MSA: Desarrollo de funciones y obligaciones de personal que trata datos personales.	
98	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	MSA: Bitácora de incidentes. MSF: Directorio de contacto con autoridades.	
99	Reporte de debilidades de seguridad de la información	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen	MSA: Bitácora de incidentes.	

		cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.		
100	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	MSA: Bitácora de incidentes.	
101	Respuesta a incidentes de seguridad de la información	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	MSA: Bitácora de incidentes.	
102	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	MSA: Bitácora de incidentes.	
103	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	MSA: Bitácora de incidentes.	

Aspectos de seguridad de la información de la gestión de continuidad de negocio				
	Continuidad de seguridad de la información	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
104	Planificación de la continuidad de la seguridad de la información	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre	MSA: Mejora continua a partir de la implementación del sistema de gestión.	
105	Implementación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	MSA: Programa de monitoreo y revisión a las medidas de seguridad.	
106	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son	MSA: Programa de monitoreo y revisión a las medidas de seguridad.	

		válidos y eficaces durante situaciones adversas		
Cumplimiento				
	Cumplimiento de requisitos legales y contractuales	Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.		
107	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	MSA: Documento de seguridad elaborado. MSA: Planificación de actualización del documento de seguridad como parte de la mejora continua. MSA: Planificación de actualización del documento de seguridad por incidentes. MSA: Elaboración de planes de trabajo.	
108	Derechos de propiedad intelectual	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales	MSA: Política de registro por derechos de autor. MSA: Política de uso de propiedad intelectual.	

		relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.		
109	Protección de registros	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	MSA: Elaboración del documento de seguridad.	
110	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	MSA: Elaboración del documento de seguridad.	
111	Reglamentación de controles criptográficos	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	MST: Integración de controles criptográficos por defecto a sistemas con datos personales.	
112	Revisiones de seguridad de la información	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo	MSA: Elaboración del documento de seguridad	

		con las políticas y procedimientos organizacionales.		
113	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	MSA: Elaboración del documento de seguridad MSA: Elaboración del sistema de gestión de seguridad de datos personales.	
114	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	MSA: Elaboración del documento de seguridad MSA: Elaboración del sistema de gestión de seguridad de datos personales.	
115	Revisión del cumplimiento técnico	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y	MSA: Elaboración del documento de seguridad	

		normas de seguridad de la información.	MSA: Elaboración del sistema de gestión de seguridad de datos personales.	
	Redundancias	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
116	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	MSF: Controles de acceso	

De esta manera, los interesados en conocer las necesidades de seguridad, al revisar los controles de seguridad relacionados con la implementación de su sistema de tratamiento, contarán con un elemento que le permitirá asociar y describir los controles de seguridad que deben implementar para mantener la seguridad de la información en sus sistemas.

A partir de la interpetación de las medidas de seguridad, podrá comenzar a identificar cómo éstas afectan el valor del riesgo, determinando la eventual degradación del riesgo gracias a las medidas de seguridad implementadas. Así,, en esta etapa conocerá el valor del riesgo residual, es decir, el riesgo calculado despues de analizar cómo las medidas de seguridad impactan el escenario de vulneración evaluado.
Así, además, deberá revisar la Declaración de Aplicabilidad, conocida en inglés como *Statement of Applicability* (SoA), la cual es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

- La declaración de aplicabilidad se debe elaborarse después del tratamiento de riesgos y constituye la actividad posterior a la evaluación de riesgos.
- La declaración de aplicabilidad debe indicar si los objetivos de control y los controles están implementados y en funcionamiento, así como aquellos que hayan sido descartados. Además, debe justificarse por qué algunas medidas han sido excluidas, especificando cuáles son innecesarias y las razones por las cuales no son requeridas por el sujeto obligado).

Dentro de las actividades a seguir, después de la selección de los controles de seguridad, se procede a crear el plan de tratamiento de riesgos, con el fin de definir las actividades necesarias para implementar dichos controles.

ETAPA DE IDENTIFICACIÓN DEL RIESGO			ETAPA DE ANÁLISIS DE RIESGO			ETAPA DE VALORACIÓN DE RIESGO				
Activos	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Inherente	Probabilidad	Impacto	Riesgo Residual	Medidas de seguridad	Mecanismos de monitoreo