ACUERDO MINISTERIAL NÚMERO 322-2026
GUATEMALA, 25 DE JUNIO DE 2026
LA MINISTRA DE TRABAJO Y PREVISIÓN SOCIAL

CONSIDERANDO

Que de conformidad con la Constitución Política de la República de Guatemala, corresponde a los Ministros de Estado, ejercer jurisdicción sobre todas las dependencias de su Ministerio; y dirigir, tramitar, resolver e inspeccionar todos los negocios relacionados con su Ministerio; por su parte, la Ley del Organismo Ejecutivo, Decreto Número 114-97 del Congreso de la República de Guatemala establece que son atribuciones generales de los Ministros, además de las que asigna la Constitución Política de la República y otras leyes, cumplir y hacer que se cumpla el ordenamiento jurídico en los diversos asuntos de su competencia; dirigir y coordinar la labor de las dependencias y entidades bajo su competencia, así como la administración de los recursos financieros, humanos y físicos bajo su responsabilidad, velando por la eficiencia y la eficacia en el empleo de los mismos; y dictar los acuerdos, resoluciones, circulares y otras disposiciones relacionadas con el despacho de los asuntos de su ramo, conforme la ley.

CONSIDERANDO

Que de conformidad con el Manual de Organización y Funciones de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, aprobado mediante Acuerdo Ministerial Número 508-2023 de fecha uno de diciembre de dos mil veintitrés, la Dirección de Sistemas de Información entre sus funciones están la de planificar, organizar, dirigir y controlar el uso y desarrollo de los recurso tecnológicos e informáticos de las distintas dependencias del Ministerio, a nivel nacional; elaborar, implementar y vigilar el cumplimiento que en materia de informática, telecomunicaciones y desarrollos tecnológicos especiales deban observar las dependencias del Ministerio, para lograr el óptimo aprovechamiento y correcta utilización de los recursos tecnológicos de la institución; entre otras.

CONSIDERANDO

Que la creciente dependencia de las tecnologías de la información en la gestión pública exige que las instituciones adopten medidas sólidas y sistemáticas para resguardar sus activos, asegurar la continuidad operativa y proteger la información bajo su custodia, por lo que se reconoce la importancia de establecer un marco integral de seguridad que abarque aspectos físicos, lógicos y operativos, con el propósito de salvaguardar la confidencialidad, integridad y disponibilidad de la información institucional frente a amenazas internas y externas

CONSIDERANDO

Que para el efecto, el Manual de Políticas de la Dirección de Sistemas de Información, establece las bases para una gestión efectiva de la seguridad de la información, promoviendo buenas prácticas en el uso de los recurso tecnológicos, el control de accesos, la protección de datos y la respuesta ante incidentes, el cual busca fortalecer la cultura de seguridad entre los usuarios, proveedores y terceros, fomentando la responsabilidad compartida en la protección de los activos institucionales, por lo que incluye las políticas; de acceso físico a las instalaciones; de seguridad física y ambiental del centro de datos; de clasificación y manejo de la información; de relación con proveedores y terceros; de copias de seguridad de los sistemas; de seguridad de las comunicaciones; de navegación en internet; de gestión de incidentes de seguridad de la información; de gestión de cambios en tecnología de la información; de registro y monitoreo de eventos; de privacidad y protección de datos personales; y en materia de usuarios, contiene las políticas; de control de acceso; de copias de seguridad de software de usuario final; de uso aceptable de activos; de escritorios y pantalla limpios; de restricciones a las instalaciones y uso del software; de protección contra software malicioso; de dispositivos móviles; de teletrabajo y acceso remoto; de uso y regulación de dispositivos de almacenamiento masivo; y de software seguro.

POR TANTO

Con base en lo considerando, leyes citadas y lo que para el efecto preceptúan los artículos 194, literales a) y f) de la Constitución Política de la Republica de Guatemala; 27 literales a), f) y m) de la Ley del Organismo Ejecutivo, Decreto Número 114-97 del Congreso de la República de Guatemala; Artículo 15 numeral 4 del Reglamento Orgánico Interno del Ministerio de Trabajo y Previsión Social Acuerdo Gubernativo Número 215-2012; y de conformidad con el Manual de Organización y Funciones de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, aprobado mediante Acuerdo Ministerial Número 508-2023 de fecha uno de diciembre de dos mil veintitrés.

ACUERDA

Articulo 1. APROBACIÓN. Aprobar en todo su contenido el **Manual de Políticas de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, Versión-01-2026**, el cual consta de setenta (70) hojas, impresas únicamente en su lado anverso y que forman parte del presente acuerdo.

Articulo 2. RESPONSABILIDAD. La Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, será responsable de revisar periódicamente el Manual de Políticas de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, Versión-01-2026, conforme a las necesidades en el servicio o cambios que surjan en las normas legales o aspectos administrativos, que mejoren la eficiencia de los procesos; así como sugerir realizar las modificaciones y actualizaciones correspondientes.

Articulo 3. DEROGATORIA. Se deroga cualquier otra disposición legal previa que se refiera a lo dispuesto en el Manual de Políticas de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, Versión-01-2026.

Articulo 4. VIGENCIA. El presente Acuerdo Ministerial surte sus efectos de manera inmediata.

Articulo 5. NOTIFÍQUESE al Vicedespacho Administrativo Financiero, a la Dirección de Sistemas de la Información y la Unidad de Planificación y Cooperación del Ministerio de Trabajo y Previsión Social, para lo que corresponda.

Mirlam Catarina Roquel
Ministra de Trabajo y Previsión Social
Ministerio de Trabajo y Previsión Social

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL REPUBLICA DE GUATEMALA, C.A.

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL SECRETARIA GENERAL GUATEMALA C.A.

Lic. Erwin Eduardo Velásquez Herrera
Secretario General
Ministerio de Trabajo y Previsión Social

VERSIÓN-01-2026

MANUAL DE POLÍTICAS DE LA DIRECCIÓN DE SISTEMAS DE INFORMACIÓN

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

GOBIERNO DE LA REPÚBLICA GUATEMALA

Ministerio de Trabajo y Previsión Social

UTZ SAMAJ

CUADRO DE VALIDACIÓN

MANUAL DE POLÍTICAS DE LA DIRECCIÓN DE SISTEMAS DE INFORMACIÓN

	Elaboró (Dirección de Sistemas de Información)	Revisó y Aprobó (Dirección de Sistemas de Información)
Nombre	Erick N. Allara Arias	Ing. Edwin Omar de la Cruz García
Cargo	Infraestructura / Técnico Asignado	Director de Sistemas de Información
Firma		Ing. Edwin Omar de la Cruz García Director de Sistemas de Información Ministerio de Trabajo y Previsión Social

Vo.Bo.

Vo.Bo. Licda. Karen Elizabeth Reyes Cruz
Viceministra Administrativa Financiera
Ministerio de Trabajo y Previsión Social

Viceministra Administrativa Financiera

CONTENIDO

INTRODUCCIÓN 11

Objetivos específicos 12

1. Dirección de Sistemas de Información (DISI) 13

1.1 Política de acceso físico a las instalaciones 13

1.1.1 Propósito 13

1.1.2 Alcance 13

1.1.3 Responsabilidades del usuario 13

1.1.4 Revisión y cumplimiento 14

1.2 Política de seguridad física y ambiental del centro de datos 14

1.2.1 Propósito 14

1.2.2 Alcance 14

1.2.3 Control de acceso físico (seguridad perimetral) 15

1.2.4 Controles ambientales (protección del hardware) 15

1.2.5 Responsabilidades de los administradores y operadores 16

1.2.6 Gestión de terceros y mantenimiento externo 16

1.2.7 Revisión y cumplimiento 16

1.3 Política de clasificación y manejo de la información 17

1.3.1 Propósito 17

1.3.2 Alcance 17

1.3.3 Niveles de clasificación 17

1.3.4 Etiquetado y manejo 18

1.3.5 Responsabilidades del usuario 18

1.3.6 Disposición final (destrucción segura) 18

1.3.7 Revisión y cumplimiento 18

1.4 Política de relación con proveedores y terceros 19

1.4.1 Propósito 19
1.4.2 Alcance 19
1.4.3 Selección y evaluación del proveedor 19
1.4.4 Responsabilidades y controles durante el servicio 19
1.4.5 Ciclo de vida del proveedor (gestión de cambios) 20
1.4.6 Revisión y cumplimiento 20
1.5 Política de copias de seguridad de los sistemas 20
1.5.1 Propósito 20
1.5.2 Alcance 21
1.5.3 Contenido 21
1.5.4 Revisión y cumplimiento 21
1.6 Política de seguridad de las comunicaciones 21
1.6.1 Propósito 21
1.6.2 Alcance 21
1.6.3 Uso del correo electrónico institucional 21
1.6.4 Sistemas de colaboración institucional 22
1.6.5 Responsabilidades del usuario 22
1.6.6 Consideraciones legales y de privacidad 23
1.6.7 Revisión y cumplimiento 23
1.7 Política de navegación en internet 23
1.7.1 Propósito 23
1.7.2 Alcance 23
1.7.3 Categorización y filtrado de contenidos 24
1.7.3.1 Sitios permitidos 24
1.7.3.2 Sitios restringidos (bajo demanda) 24
1.7.3.3 Sitios prohibidos 24

1.7.4 Normas de navegación segura 24
1.7.5 Responsabilidades del usuario 25
1.7.6 Revisión y cumplimiento 25
1.8 Política de gestión de incidentes de seguridad de la información 25
1.8.1 Propósito 25
1.8.2 Alcance 25
1.8.3 Definiciones 26
1.8.4 Clasificación de incidentes 26
1.8.5 Ciclo de gestión del incidente 27
1.8.6 Equipo de respuesta a incidentes 27
1.8.7 Comunicación y notificación 27
1.8.8 Responsabilidades del usuario 28
1.8.9 Revisión y cumplimiento 28
1.9 Política de gestión de cambios en tecnología de la información 28
1.9.1 Propósito 28
1.9.2 Alcance 28
1.9.3 Tipos de cambio 29
1.9.4 Ciclo de gestión del cambio 29
1.9.5 Cambios emergentes 30
1.9.6 Segregación de ambientes 30
1.9.7 Responsabilidades 30
1.9.8 Revisión y cumplimiento 30
1.10 Política de registro y monitoreo de eventos (logs y auditoría) 31
1.10.1 Propósito 31
1.10.2 Alcance 31
1.10.3 Eventos mínimos a registrar 31

1.10.4 Contenido mínimo de los registros 31
1.10.5 Sincronización temporal 32
1.10.6 Almacenamiento, protección y retención 32
1.10.7 Monitoreo y análisis 32
1.10.8 Acceso a los registros 32
1.10.9 Privacidad y proporcionalidad 33
1.10.10 Revisión y cumplimiento 33
1.11 Política de privacidad y protección de datos personales 33
1.11.1 Propósito 33
1.11.2 Alcance 34
1.11.3 Principios rectores 34
1.11.4 Derechos de los titulares 34
1.11.5 Tratamiento por terceros y encargados 35
1.11.6 Controles de seguridad aplicables 35
1.11.7 Brechas que involucran datos personales 35
1.11.8 Responsabilidades 36
1.11.9 Revisión y cumplimiento 36
2. Usuarios 37
2.1 Política de control de acceso 37
2.1.1 Propósito 37
2.1.2 Alcance 37
2.1.3 Principios generales del control de acceso 38
2.1.4 Gestión del acceso de usuarios 38
2.1.4.1 Registro y baja de usuarios 38
2.1.4.2 Provisión de acceso y gestión de privilegios 38
2.1.4.3 Gestión de la información de autenticación 39
2.1.4.4 Política de contraseñas 39

2.1.4.5 Bloqueo de cuentas por intentos fallidos de inicio de sesión 39
2.1.5 Control de acceso a redes, sistemas y aplicaciones 42
2.1.5.1 Acceso a la red 42
2.1.5.2 Acceso a redes y servicios de red 43
2.1.5.3 Control de acceso lógico a sistemas y aplicaciones 44
2.1.5.4 Vinculación de cuentas de usuario a equipos asignados 44
2.1.6 Responsabilidades del usuario 47
2.1.7 Revisión y cumplimiento 47
2.2 Política de copias de seguridad de software de usuario final 48
2.2.1 Propósito 48
2.2.2 Alcance 48
2.2.3 Contenido 48
2.2.4 Revisión y cumplimiento 48
2.3 Política de uso aceptable de activos 48
2.3.1 Propósito 48
2.3.2 Alcance 49
2.3.3 Normas de uso de los activos 49
2.3.4 Software y seguridad lógica 49
2.3.5 Responsabilidades del usuario 50
2.3.6 Prohibiciones explícitas 50
2.3.7 Monitoreo y privacidad 50
2.3.8 Revisión y cumplimiento 50
2.4 Política de escritorio y pantalla limpios 51
2.4.1 Propósito 51
2.4.2 Alcance 51
2.4.3 Lineamientos de escritorio limpio (información física) 51

2.4.4 Lineamientos de pantalla limpia (información digital) 51
2.4.5 Responsabilidades del usuario 52
2.4.6 Revisión y cumplimiento 52
2.5 Política de restricciones a las instalaciones y uso del software 52
2.5.1 Propósito 52
2.5.2 Alcance 53
2.5.3 Responsabilidades del usuario 53
2.5.4 Revisión y cumplimiento 53
2.6 Política de protección contra software malicioso 54
2.6.1 Propósito 54
2.6.2 Alcance 54
2.6.3 Contenido 54
2.6.4 Responsabilidades del usuario 54
2.6.5 Revisión y cumplimiento 55
2.7 Política de dispositivos móviles 55
2.7.1 Propósito 55
2.7.2 Alcance 55
2.7.3 Responsabilidades del usuario 55
2.7.4 Revisión y cumplimiento 56
2.8 Política de teletrabajo y acceso remoto 56
2.8.1 Propósito 56
2.8.2 Alcance 56
2.8.3 Autorización 56
2.8.4 Requisitos técnicos mínimos 57
2.8.5 Lineamientos para el entorno de trabajo remoto 57
2.8.6 Conexiones y plataformas autorizadas 58

2.8.7 Responsabilidades del usuario 58
2.8.8 Revisión y cumplimiento 58
2.9 Política de uso y regulación de dispositivos de almacenamiento masivo 58
2.9.1 Propósito 58
2.9.2 Alcance 59
2.9.2.1 Dispositivos comprendidos 60
2.9.2.2 Entornos y activos cubiertos 60
2.9.2.3 Exclusiones 60
2.9.3 Contenido 60
2.9.3.1 Principios generales 60
2.9.3.2 Clasificación de los dispositivos 61
2.9.3.3 Uso permitido 61
2.9.3.4 Uso prohibido 62
2.9.3.5 Autorización y registro 62
2.9.3.6 Controles técnicos 63
2.9.3.7 Custodia, transporte y disposición final 63
2.9.3.8 Responsabilidades 64
2.9.4 Revisión y cumplimiento 64
2.9.4.1 Revisión 64
2.9.4.2 Mecanismos de verificación del cumplimiento 65
2.9.4.3 Reporte de incidentes e incumplimientos 65
2.9.4.4 Difusión y aceptación 65
2.9.5 Sanciones 65
2.9.5.1 Niveles de severidad 66
2.9.5.2 Criterios de aplicación 66
2.9.5.3 Procedimiento disciplinario 67

2.10 Política de software seguro 67

2.10.1 Propósito 67

2.10.2 Alcance 67

2.10.3 Responsabilidades del usuario (desarrolladores y adquisiciones) 67

2.10.4 Revisión y cumplimiento 68

GLOSARIO 69

INTRODUCCIÓN

La creciente dependencia de las tecnologías de la información en la gestión pública exige que las instituciones adopten medidas sólidas y sistemáticas para resguardar sus activos, asegurar la continuidad operativa y proteger la información bajo su custodia. En este contexto, la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social reconoce la importancia de establecer un marco integral de seguridad que abarque aspectos físicos, lógicos y operativos, con el propósito de salvaguardar la confidencialidad, integridad y disponibilidad de la información institucional frente a amenazas internas y externas.

El presente Manual de Políticas de la Dirección de Sistema de Información , establece las bases para una gestión efectiva de la seguridad de la información, promoviendo buenas prácticas en el uso de los recursos tecnológicos, el control de accesos, la protección de datos y la respuesta ante incidentes. Asimismo, busca fortalecer la cultura de seguridad entre los usuarios, proveedores y terceros, fomentando la responsabilidad compartida en la protección de los activos institucionales.

A través de la implementación de estos lineamientos, la Dirección de Sistema de Información del Ministerio de Trabajo y Previsión Social se alinea con estándares y buenas prácticas, asegurando una gestión eficiente ante los riesgos tecnológicos y contribuyendo al cumplimiento a la mejora continua de sus procesos y la confianza de los usuarios en los servicios que brinda.

OBJETIVOS

Establecer un marco integral de políticas, controles y lineamientos que garanticen la seguridad física, lógica y operativa de la información, los sistemas, las instalaciones y los activos tecnológicos del Ministerio, asegurando la confidencialidad, integridad y disponibilidad de los recursos institucionales frente a amenazas internas y externas.

Objetivos específicos

- Establecer y aplicar controles de acceso físicos y lógicos que garanticen que solo el personal autorizado pueda ingresar a instalaciones, sistemas, aplicaciones y recursos tecnológicos, bajo los principios de menor privilegio y necesidad de conocer.
- Proteger la información institucional en todo su ciclo de vida, implementando prácticas de clasificación, almacenamiento seguro, transmisión protegida y destrucción adecuada para prevenir fugas, accesos no autorizados y pérdida de datos.
- Regular el uso responsable y seguro de los activos tecnológicos, comunicaciones y software, asegurando que los usuarios, proveedores y terceros cumplan con los lineamientos establecidos para minimizar riesgos de malware, accesos indebidos y compromisos de seguridad.
- Regular el uso de dispositivos de almacenamiento masivo extraíbles y otros medios removibles, para mitigar los riesgos de fuga de información, introducción de software malicioso y pérdida no autorizada de datos.
- Establecer mecanismos formales para la gestión de incidentes, cambios tecnológicos, monitoreo de eventos, protección de datos personales y acceso remoto, alineando la operación de la Dirección de Sistemas de Información con las buenas prácticas internacionales.

1. Dirección de Sistemas de Información (DISI)

Las políticas contenidas en esta sección establecen los lineamientos institucionales que rigen las áreas y procesos directamente administrados por la Dirección de Sistemas de Información, incluyendo el control de acceso físico, la protección del centro de datos, la clasificación de la información, la relación con proveedores, las copias de seguridad, las comunicaciones electrónicas, la navegación en internet, la gestión de incidentes, la gestión de cambios, el monitoreo de eventos y la protección de los datos personales.

1.1 Política de acceso físico a las instalaciones

1.1.1 Propósito

Establecer los lineamientos necesarios para proteger los activos críticos, el personal y la información sensible de la institución mediante la regulación del ingreso y permanencia en las instalaciones. Se busca prevenir accesos no autorizados, daños físicos, robos e interrupciones en la operación de la infraestructura tecnológica.

1.1.2 Alcance

Esta política es aplicable a:

- **Todo el personal:** empleados permanentes, temporales y practicantes.
- **Terceros:** contratistas, consultores, proveedores y visitantes.
- **Instalaciones:** todas las oficinas, centros de datos, áreas de almacenamiento y espacios comunes bajo el control de la institución.

1.1.3 Responsabilidades del usuario

Para que la seguridad sea efectiva, cada individuo debe cumplir con lo siguiente:

- **Identificación visible:** portar el carné o credencial de identidad en un lugar visible en todo momento dentro de las instalaciones.
- **Uso de credenciales:** no prestar, ceder o duplicar las tarjetas de acceso o llaves asignadas.
- **Reporte de incidentes:** informar de inmediato al departamento de seguridad o a la DISI en caso de pérdida de credenciales o si se observa a personas sin identificación en áreas restringidas.
- **Política de no tailgating (anti-seguimiento):** no permitir que ninguna persona ingrese detrás de uno sin haber validado su propio acceso en el lector correspondiente.

- **Acompañamiento de visitas:** los empleados que reciban visitantes son responsables de su conducta y deben asegurar que estos permanezcan en las áreas permitidas.

1.1.4 Revisión y cumplimiento

Actividad	Descripción	Frecuencia
Auditoría de logs	Revisión de los registros de entrada/salida de áreas críticas (centro de datos).	Mensual
Revisión de accesos	Validación de que los empleados actuales aún requieren acceso a las áreas asignadas.	Trimestral
Pruebas de intrusión física	Intentos controlados de acceso no autorizado para evaluar la respuesta del personal.	Anual
Actualización de política	Ajuste de los lineamientos según nuevos riesgos o cambios en la infraestructura.	Anual

Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos en el entorno tecnológico o normativo. El incumplimiento podrá dar lugar a acciones disciplinarias, de acuerdo con la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

1.2 Política de seguridad física y ambiental del centro de datos

1.2.1 Propósito

Garantizar la continuidad de la información del Ministerio de Trabajo y Previsión Social protegiendo el hardware crítico contra amenazas humanas (intrusiones, errores) y ambientales (incendio, inundación, fallos eléctricos) que puedan comprometer la integridad y disponibilidad de los datos.

1.2.2 Alcance

Esta política aplica al centro de datos institucional, su perímetro físico, los equipos de cómputo, redes, almacenamiento y sistemas auxiliares (climatización, suministro eléctrico, detección y supresión de incendios), así como al personal interno y externo que requiera acceso físico al mismo.

1.2.3 Control de acceso físico (seguridad perimetral)

El acceso al centro de datos se rige por el principio de menor privilegio:

- **Zonificación:** el centro de datos debe considerarse una zona de alta seguridad.
- **Autenticación de doble factor:** para ingresar, se requerirá al menos dos métodos de identificación (por ejemplo, tarjeta de proximidad más biometría o PIN).
- **Registro de acceso:** todo ingreso y salida debe quedar registrado automáticamente en una bitácora electrónica inalterable o en el Libro de Ingresos y Egresos al Centro de Datos de la Dirección de Sistemas de Información, incluyendo fecha, identificación, nombre, institución, motivo y firma.
- **Videovigilancia (CCTV):** cámaras de video vigilancia deben monitorear todos los racks y puntos de entrada las 24 horas del día, con grabaciones almacenadas por un mínimo de 30 días.

1.2.4 Controles ambientales (protección del hardware)

Para mitigar riesgos del entorno, se deben implementar y mantener al menos los siguientes controles:

- **Climatización:** mantener una temperatura controlada y una humedad relativa, dado que reduce la degradación térmica de componentes electrónicos, previene fallas por corrosión y descargas electrostáticas, y garantiza condiciones estables de operación, prolongando significativamente la vida útil del hardware y asegurando su confiabilidad.

- **UPS (SAI):** sistemas de alimentación ininterrumpida para filtrar picos y mantener la carga durante cortes breves.

- **Generadores:** deben ser capaces de soportar la carga total por al menos 24 horas y ser probados mensualmente.

1.2.5 Responsabilidades de los administradores y operadores

El personal con acceso autorizado debe cumplir con:

- **Prohibición de alimentos y bebidas:** queda estrictamente prohibido ingresar cualquier tipo de líquido o comida.
- **Orden y limpieza:** los racks deben mantenerse cerrados con llave. No se permite dejar cables sueltos (cableado tipo espagueti) ni cajas de cartón (material inflamable) dentro de la sala.
- **Mantenimiento preventivo:** programar y supervisar las revisiones de los aires acondicionados y generadores.

1.2.6 Gestión de terceros y mantenimiento externo

Cualquier técnico externo (proveedor de internet, mantenimiento de aire acondicionado, etc.) debe:

- Estar autorizado previamente mediante ticket de soporte.
- Presentar identificación oficial.
- Ser escoltado en todo momento por un miembro del personal de la institución.

1.2.7 Revisión y cumplimiento

Control	Estándar de revisión	Frecuencia
Prueba de generadores	Arranque bajo carga real.	Mensual
Sensores de temperatura	Calibración y alertas de umbral.	Trimestral
Inventario de activos	Verificación física de servidores y equipos de red.	Semestral
Auditoría de acceso	Revisión de quién entró y por qué.	Semanal

El incumplimiento de esta política podrá dar lugar a acciones disciplinarias, de acuerdo con la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

1.3 Política de clasificación y manejo de la información

1.3.1 Propósito

Establecer un marco de trabajo para identificar el valor de la información institucional y asegurar que reciba el nivel de protección adecuado de acuerdo con su importancia, confidencialidad y requisitos legales.

1.3.2 Alcance

Esta política aplica a toda la información generada, recibida, almacenada, procesada o transmitida por el Ministerio, en cualquier formato (digital o físico), así como a todo el personal y los terceros que tengan acceso a ella.

1.3.3 Niveles de clasificación

La información se categorizará en cuatro niveles según el impacto que tendría su divulgación no autorizada:

Nivel	Descripción	Ejemplos
Confidencial / Crítica	Información altamente sensible. Su divulgación causaría daño grave (legal, financiero o reputacional).	Estrategias institucionales, contraseñas, datos de salud, información reservada.
Privada	Información relacionada con individuos o procesos internos que no es pública.	Datos personales de empleados.
Uso interno	Información para la operación diaria. No causa daño grave, pero no debe ser pública.	Controles internos.
Pública	Información aprobada para su divulgación general.	Comunicados oficiales, informes anuales públicos.

1.3.4 Etiquetado y manejo

Cada nivel requiere medidas de seguridad específicas durante su ciclo de vida:

- **Etiquetado:** todos los documentos clasificados como Confidencial o Privado deben incluir una marca de agua o encabezado que indique su nivel de clasificación.
- **Almacenamiento físico:** documentos confidenciales bajo llave en archivadores ignífugos.
- **Almacenamiento digital:** cifrado obligatorio (AES-256) y almacenamiento en unidades con control de acceso.
- **Transporte:** la información confidencial no debe enviarse por canales no cifrados (como mensajería instantánea personal o correo personal). Se debe usar VPN y herramientas de transferencia segura.

1.3.5 Responsabilidades del usuario

- **Propietario (owner):** generalmente el jefe de área que genera la información. Es responsable de asignar el nivel de clasificación inicial.
- **Custodio:** la Dirección de Sistemas de Información o seguridad que mantiene los sistemas donde reside la información. Es responsable de aplicar los controles técnicos.
- **Usuario final:** responsable de seguir las reglas de manejo, no dejar documentos sensibles en impresoras y aplicar la política de escritorio limpio.

1.3.6 Disposición final (destrucción segura)

Cuando la información ya no es necesaria, conforme al tiempo de retención legal aplicable, debe eliminarse de forma que sea irrecuperable:

- **Papel:** trituración en partículas finas (corte cruzado), nunca tirarla entera a la basura y no ser legible.
- **Medios digitales:** uso de software de borrado seguro (wiping) o destrucción física de discos duros y memorias USB, conforme a buenas prácticas reconocidas (por ejemplo, NIST SP 800-88 o equivalentes).

1.3.7 Revisión y cumplimiento

- **Auditorías de clasificación:** revisión aleatoria de archivos en servidores para verificar que estén correctamente etiquetados.

- **Capacitación:** sesiones anuales obligatorias para que los empleados sepan distinguir entre los niveles de clasificación.

Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos. El incumplimiento podrá dar lugar a acciones disciplinarias de acuerdo con la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

1.4 Política de relación con proveedores y terceros

1.4.1 Propósito

Establecer los requisitos mínimos de seguridad de la información que deben cumplir los proveedores, contratistas y socios de negocio para garantizar que el acceso a los activos de la institución no comprometa la confidencialidad, integridad o disponibilidad de los datos.

1.4.2 Alcance

Esta política aplica a todas las entidades externas que presten servicios al Ministerio, especialmente aquellas que:

- Tengan acceso físico a las instalaciones.
- Tengan acceso lógico a la red o bases de datos.
- Almacenen, procesen o transmitan información del Ministerio.

1.4.3 Selección y evaluación del proveedor

Antes de firmar cualquier contrato, las áreas de infraestructura juntamente con la de compras deben:

- **Debida diligencia (due diligence):** evaluar las prácticas de seguridad del proveedor mediante un cuestionario técnico y/o revisión de certificaciones (ISO/IEC 27001, SOC 2, etc.).
- **Análisis de riesgo:** determinar el impacto potencial si el proveedor sufre una brecha de seguridad.
- **Acuerdos de confidencialidad (NDA):** es obligatorio por parte del proveedor firmar un compromiso de confidencialidad antes de compartir cualquier información clasificada como Privada o Confidencial.

1.4.4 Responsabilidades y controles durante el servicio

Una vez contratado, el proveedor debe adherirse a los siguientes controles:

- **Acceso remoto seguro:** si el proveedor requiere acceso a los sistemas, se hará mediante una VPN con autenticación de doble factor (MFA) y solo por el tiempo estrictamente necesario.

- **Cumplimiento de políticas:** el proveedor debe aceptar y firmar que conoce y cumplirá con las políticas de seguridad del Ministerio.
- **Propiedad intelectual:** debe quedar claro por contrato que toda la información generada durante la prestación del servicio es propiedad exclusiva del Ministerio.
- **Derecho a auditoría:** el Ministerio se reserva el derecho de realizar auditorías de seguridad a los procesos o sistemas del proveedor que afecten el servicio prestado.

1.4.5 Ciclo de vida del proveedor (gestión de cambios)

Fase	Requisito de seguridad
Inicio	Creación de cuentas individuales (no genéricas) y asignación de privilegios mínimos.
Operación	Revisión trimestral de accesos. Los proveedores solo deben ver lo que necesitan para su trabajo.
Finalización	Revocación inmediata de accesos físicos y lógicos, y devolución o destrucción certificada de la información institucional.

1.4.6 Revisión y cumplimiento

- **Monitoreo de desempeño:** evaluar periódicamente si el proveedor mantiene los niveles de seguridad acordados (SLA).
- **Gestión de incidentes:** el proveedor tiene la obligación de notificar al Ministerio cualquier incidente de seguridad en sus sistemas dentro de las primeras 24 horas de su detección.

Nota crítica: el incumplimiento de estas normas por parte del proveedor será causa de rescisión inmediata del contrato sin responsabilidad para el Ministerio.

1.5 Política de copias de seguridad de los sistemas

1.5.1 Propósito

Garantizar la disponibilidad y recuperabilidad de la información institucional mediante un esquema formal de respaldo, custodia y restauración de los sistemas administrados por la Dirección de Sistemas de Información.

1.5.2 Alcance

Aplica a los servidores, bases de datos, aplicaciones, repositorios y sistemas críticos administrados directamente por la DISI.

1.5.3 Contenido

Los lineamientos operativos, técnicos, de periodicidad, custodia y restauración aplicables a los respaldos de los sistemas se encuentran desarrollados en el documento *Manual de Resguardo de la Información de la Dirección de Sistemas de Información*, el cual forma parte integral de la presente política como anexo técnico de referencia.

1.5.4 Revisión y cumplimiento

La DISI verificará periódicamente la ejecución de los respaldos, la integridad de los medios y la efectividad de los procedimientos de restauración, conforme a lo establecido en el manual de referencia.

1.6 Política de seguridad de las comunicaciones

1.6.1 Propósito

Establecer las normas de uso seguro de las herramientas de comunicación electrónica y colaboración para proteger la información institucional contra accesos no autorizados, interceptación o pérdida de datos, asegurando que se utilicen exclusivamente para fines profesionales.

1.6.2 Alcance

Esta política aplica a todo el personal interno, contratistas y terceros que utilicen el correo electrónico institucional, las plataformas de colaboración corporativa, los sistemas de mensajería instantánea oficiales y cualquier otro medio de comunicación provisto por el Ministerio.

1.6.3 Uso del correo electrónico institucional

- **Uso exclusivo:** la cuenta de correo institucional debe utilizarse únicamente para actividades laborales. Está prohibido registrarse con esta cuenta en sitios web personales o de entretenimiento.
- **Prohibición de reenvío automático:** no se permite configurar el reenvío automático de correos institucionales a cuentas personales (Gmail, Outlook personal, etc.).

- **Identificación oficial:** todos los correos deben incluir la firma institucional estándar, sin modificar logos ni añadir frases personales que comprometan la imagen del Ministerio.
- **Cifrado de contenido:** si es estrictamente necesario enviar información clasificada como Confidencial, el cuerpo del mensaje o los archivos adjuntos deben estar cifrados y protegidos por contraseña (enviada por un canal distinto).

1.6.4 Sistemas de colaboración institucional

Las plataformas de trabajo en equipo deben gestionarse bajo los siguientes controles:

- **Creación de canales y grupos:** la creación de grupos de trabajo públicos o privados debe estar justificada por un proyecto o área. Se realizarán purgas semestrales de canales inactivos.
- **Invitados externos:** el acceso a terceros (proveedores) a los sistemas de colaboración debe ser aprobado por el responsable del área y limitado a los archivos específicos de su proyecto.
- **Compartición de archivos:** se debe priorizar el uso de enlaces con permisos específicos (solo lectura o edición caduca) en lugar de enviar copias de archivos por chat.
- **Grabación de sesiones:** las reuniones grabadas que contengan información sensible deben almacenarse en repositorios oficiales y su acceso debe restringirse solo a los asistentes originales.

1.6.5 Responsabilidades del usuario

Todo colaborador tiene el deber de:

- **Verificación de destinatarios:** revisar cuidadosamente la dirección del destinatario antes de enviar información, especialmente si el sistema sugiere nombres autocompletados.
- **Alerta de phishing:** reportar inmediatamente al área de seguridad cualquier correo sospechoso que solicite credenciales, datos bancarios o incluya archivos adjuntos extraños.
- **Autenticación reforzada:** mantener habilitado el segundo factor de autenticación (MFA) de forma obligatoria en todas las plataformas de comunicación sin excepción.

1.6.6 Consideraciones legales y de privacidad

- **Propiedad de la información:** todos los mensajes y archivos transmitidos a través de los sistemas institucionales son propiedad del Ministerio.
- **Derecho de monitoreo:** el Ministerio se reserva el derecho de monitorear y auditar las comunicaciones electrónicas para garantizar el cumplimiento de esta política, respetando la legislación local vigente sobre privacidad laboral.

1.6.7 Revisión y cumplimiento

Control	Descripción	Frecuencia
Filtro antispam/malware	Revisión de reglas de filtrado y bloqueo de dominios maliciosos.	Semanal
Auditoría de DLP	Monitoreo de herramientas de prevención de fuga de datos para detectar envío de información sensible.	Continua
Revisión de accesos externos	Eliminación de cuentas de invitados de terceros que ya no tienen proyectos activos.	Mensual
Simulacros de phishing	Pruebas controladas para medir la capacidad de detección de los empleados.	Semestral

1.7 Política de navegación en internet

1.7.1 Propósito

Establecer los lineamientos para el uso responsable, seguro y productivo de los recursos de internet proporcionados por el Ministerio, minimizando los riesgos de infecciones por código malicioso (malware), robo de identidad y fugas de información.

1.7.2 Alcance

Esta política aplica a todos los empleados, contratistas y terceros que utilicen la red institucional (cableada o Wi-Fi) o dispositivos propiedad del Ministerio para acceder a internet.

1.7.3 Categorización y filtrado de contenidos

El Ministerio implementará herramientas de filtrado web para gestionar el acceso a diferentes sitios basándose en las siguientes categorías:

1.7.3.1 Sitios permitidos

Se considera de uso permitido el acceso a sitios web vinculados con las funciones laborales, tales como portales gubernamentales, herramientas institucionales en la nube, repositorios técnicos, fuentes de información oficial, capacitación profesional y servicios provistos por el Ministerio.

1.7.3.2 Sitios restringidos (bajo demanda)

Redes sociales y servicios de streaming, los cuales podrán ser limitados en horarios laborales o habilitados únicamente a áreas que los requieran para el cumplimiento de sus funciones (por ejemplo, Comunicación Social).

1.7.3.3 Sitios prohibidos

- Contenido pornográfico o sexualmente explícito.
- Sitios de apuestas y juegos de azar.
- Páginas que promuevan la violencia, odio o actividades ilegales.
- Sitios de descarga de software ilegal (piratería) o intercambio de archivos P2P.
- Criptominería y portales de hacking.

1.7.4 Normas de navegación segura

Para proteger los activos del Ministerio, los usuarios deben cumplir con lo siguiente:

- **Descarga de archivos:** queda prohibida la descarga de archivos ejecutables (.exe, .bat, .msi, .sh) sin autorización expresa de la DISI.
- **Uso de protocolos seguros:** se debe priorizar el uso de sitios con protocolo HTTPS. El sistema de seguridad podrá bloquear automáticamente sitios con certificados SSL inválidos o expirados.
- **Extensiones del navegador:** los usuarios no deben instalar extensiones o complementos en los navegadores que no hayan sido previamente aprobados por la Dirección de Sistemas de Información, ya que pueden contener software espía.
- **Almacenamiento en la nube personal:** queda prohibido el uso de servicios de almacenamiento personal (como Dropbox o Google Drive personal) para cargar o descargar información institucional clasificada.

1.7.5 Responsabilidades del usuario

- **Sentido común:** no hacer clic en enlaces sospechosos o ventanas emergentes que anuncien premios o alertas de seguridad falsas.
- **Credenciales:** nunca ingresar las cuentas de correo ni contraseñas institucionales en sitios web externos que no sean los sistemas oficiales del Ministerio.
- **Reporte de bloqueos:** si un sitio necesario para el trabajo está bloqueado, el usuario debe solicitar su apertura mediante un ticket formal, justificando la necesidad institucional.

1.7.6 Revisión y cumplimiento

Actividad	Descripción	Frecuencia
Monitoreo de tráfico	Revisión de los sitios más visitados y detección de anomalías en el consumo de datos.	Semanal
Actualización de filtros	Actualización de las listas de reputación de dominios y categorías de bloqueo.	Diaria (automática)
Auditoría de logs	Revisión de intentos de acceso a sitios prohibidos por parte de usuarios.	Mensual

1.8 Política de gestión de incidentes de seguridad de la información

1.8.1 Propósito

Establecer un marco formal para la identificación, reporte, clasificación, contención, erradicación, recuperación y aprendizaje ante eventos e incidentes de seguridad de la información, con el fin de minimizar su impacto sobre la confidencialidad, integridad y disponibilidad de los activos del Ministerio y restablecer la operación normal en el menor tiempo posible.

1.8.2 Alcance

Esta política aplica a todos los eventos e incidentes de seguridad de la información, físicos o lógicos, que afecten a:

- Personal interno, contratistas, proveedores y terceros.

- Sistemas, aplicaciones, redes, bases de datos y servicios en la nube administrados por el Ministerio.
- Infraestructura física, centro de datos, estaciones de trabajo y dispositivos móviles.
- Información en cualquier formato (digital o físico).

1.8.3 Definiciones

- **Evento de seguridad:** ocurrencia identificada en un sistema, servicio o red que indica una posible violación de la política de seguridad o un fallo en los controles.
- **Incidente de seguridad:** uno o varios eventos relacionados que tienen una probabilidad significativa de comprometer las operaciones del Ministerio o amenazar la seguridad de la información.
- **Brecha de datos:** incidente que resulta en la divulgación, alteración, pérdida o acceso no autorizado a información clasificada como Privada o Confidencial.

1.8.4 Clasificación de incidentes

Severidad	Descripción	Tiempo de respuesta objetivo
Crítica	Compromete sistemas críticos, expone información confidencial o detiene la operación institucional.	Respuesta inmediata (<1 hora). Notificación a la alta dirección.
Alta	Afecta servicios importantes o un grupo significativo de usuarios, con riesgo de propagación.	Respuesta en <4 horas hábiles.
Media	Afecta servicios no críticos o usuarios individuales, con riesgo contenido.	Respuesta en <1 día hábil.
Baja	Eventos menores, intentos fallidos sin impacto, anomalías controladas.	Respuesta en <3 días hábiles.

1.8.5 Ciclo de gestión del incidente

Detección e identificación: los eventos pueden ser detectados por usuarios, herramientas de monitoreo, alertas automatizadas, terceros o proveedores. Todo usuario tiene la obligación de reportar.

Reporte: el reporte debe realizarse de inmediato a la DISI a través de los canales oficiales (ticket, correo, línea de soporte). Para incidentes que involucren datos personales o información clasificada, el reporte debe efectuarse en un plazo máximo de 1 hora desde la detección.

Registro y clasificación: la DISI registrará el incidente en una bitácora con un identificador único, asignará severidad y responsable de atención.

Contención: acciones inmediatas para limitar el alcance del incidente (aislamiento de equipos, revocación de accesos, bloqueo de cuentas, segmentación de red).

Erradicación: eliminación de la causa raíz (malware, accesos no autorizados, vulnerabilidades explotadas).

Recuperación: restauración de servicios desde respaldos verificados y verificación de integridad antes de retornar a operación.

Lecciones aprendidas: elaboración de un informe post-incidente con hallazgos, causas, impacto y acciones correctivas y preventivas. Los incidentes críticos y altos requieren reunión formal de cierre.

1.8.6 Equipo de respuesta a incidentes

La DISI coordinará un Equipo de Respuesta a Incidentes de Seguridad (CSIRT interno), integrado por personal técnico designado, con el apoyo de las áreas jurídica, recursos humanos, comunicación y dirección, según la naturaleza del incidente.

1.8.7 Comunicación y notificación

- Las comunicaciones externas (medios, autoridades, titulares de datos afectados) deberán ser coordinadas exclusivamente por las áreas de comunicación y dirección, nunca por el personal técnico.
- En caso de brechas que involucren datos personales, se evaluará la obligación de notificación a las autoridades competentes y a los titulares afectados, conforme a la legislación aplicable.
- La confidencialidad sobre los detalles del incidente debe mantenerse hasta su resolución y la difusión oficial.

1.8.8 Responsabilidades del usuario

- Reportar de inmediato cualquier evento sospechoso (correos de phishing, accesos no reconocidos, comportamiento anormal de equipos, pérdida de dispositivos, etc.).
- Cooperar plenamente con la investigación, preservando evidencia y absteniéndose de manipular el equipo o sistema afectado.
- No divulgar información sobre el incidente fuera de los canales autorizados.

1.8.9 Revisión y cumplimiento

- La DISI mantendrá un registro consolidado de incidentes y publicará indicadores periódicos (cantidad, severidad, tiempos de respuesta, causas).
- Se realizarán ejercicios de simulación (tabletop exercises) al menos una vez al año para evaluar la capacidad de respuesta.
- Esta política será revisada anualmente o tras cualquier incidente crítico que evidencie necesidades de mejora.

La omisión deliberada del reporte de un incidente, su encubrimiento o la manipulación de evidencia serán considerados faltas graves y darán lugar a las acciones disciplinarias correspondientes, conforme a la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

1.9 Política de gestión de cambios en tecnología de la información

1.9.1 Propósito

Establecer un proceso formal y controlado para la planificación, autorización, ejecución y verificación de los cambios sobre la infraestructura tecnológica, los sistemas, las aplicaciones y los servicios administrados por la Dirección de Sistemas de Información, con el fin de minimizar riesgos operativos, interrupciones de servicio y afectaciones a la seguridad de la información.

1.9.2 Alcance

Esta política aplica a todo cambio que se realice sobre:

- Hardware: servidores, equipos de red, equipos de cómputo, dispositivos de almacenamiento e infraestructura del centro de datos.
- Software: sistemas operativos, bases de datos, aplicaciones institucionales, parches y actualizaciones.
- Configuraciones: reglas de firewall, listas de control de acceso, configuraciones de red, políticas de seguridad.

- Servicios en la nube y servicios prestados por proveedores externos.
- Procedimientos operativos que afecten la prestación de servicios tecnológicos.

1.9.3 Tipos de cambio

Tipo	Descripción
Estándar	Cambios preaprobados, repetitivos y de bajo riesgo (por ejemplo, instalación rutinaria de actualizaciones de seguridad, alta de usuarios, asignación de equipos estándar).
Normal	Cambios planificados que requieren evaluación y aprobación formal antes de su ejecución.
Emergente	Cambios urgentes derivados de incidentes o vulnerabilidades críticas que requieren ejecución inmediata, con autorización abreviada y documentación posterior.

1.9.4 Ciclo de gestión del cambio

Solicitud (RFC): toda solicitud de cambio debe formalizarse a través del sistema de tickets institucional, incluyendo justificación, descripción técnica, sistemas afectados, plan de implementación y plan de retorno (rollback).

Evaluación de impacto y riesgo: la DISI evaluará el impacto operativo, de seguridad y dependencias del cambio, así como el plan de mitigación de riesgos identificados.

Aprobación: los cambios deben ser autorizados conforme a un esquema de aprobación basado en su tipo, criticidad e impacto, registrado en la herramienta de gestión correspondiente.

Ventana de ejecución: los cambios deben ejecutarse preferentemente en ventanas de mantenimiento programadas, fuera de horarios críticos, comunicando con anticipación a las áreas afectadas.

Pruebas: todo cambio significativo debe probarse en ambientes de desarrollo o preproducción antes de aplicarse en producción, salvo excepciones documentadas.

Implementación: ejecución del cambio conforme al plan aprobado, con monitoreo activo durante y después de su aplicación.

Verificación y cierre: validación de que el cambio cumple sus objetivos, actualización de documentación técnica y cierre formal del ticket.

Reversión (rollback): si el cambio falla o produce efectos no deseados, se ejecutará el plan de reversión y se registrará como cambio fallido para revisión.

1.9.5 Cambios emergentes

Los cambios emergentes podrán ejecutarse con una autorización abreviada del responsable técnico, dejando constancia inmediata mediante ticket. La documentación completa del cambio y su justificación deberá completarse dentro de las 48 horas posteriores a su ejecución.

1.9.6 Segregación de ambientes

- Se mantendrán ambientes separados de desarrollo, pruebas y producción para los sistemas críticos.
- Los datos productivos no deben ser utilizados en ambientes de desarrollo o pruebas sin un proceso previo de enmascaramiento o anonimización.
- Solo el personal autorizado puede realizar despliegues en producción.

1.9.7 Responsabilidades

- **DISI:** diseñar, administrar y supervisar el proceso de gestión de cambios; mantener la herramienta de tickets; evaluar impactos y autorizar cambios.
- **Solicitantes (áreas o proveedores):** presentar solicitudes formales con la información requerida y participar en las pruebas.
- **Responsables técnicos:** ejecutar el cambio conforme al plan aprobado y documentar el resultado.

1.9.8 Revisión y cumplimiento

- La DISI mantendrá un registro histórico de todos los cambios ejecutados, con indicadores de éxito, fallas y reversiones.
- Revisión mensual de cambios emergentes para validar su justificación y completitud documental.
- Auditorías periódicas sobre el cumplimiento del proceso.

La ejecución de cambios no autorizados o sin documentación adecuada será considerada una falta a esta política y dará lugar a las acciones disciplinarias correspondientes.

1.10 Política de registro y monitoreo de eventos (logs y auditoría)

1.10.1 Propósito

Establecer los lineamientos para la generación, recolección, almacenamiento, protección, análisis y conservación de los registros de eventos (logs) producidos por los sistemas, aplicaciones, redes y dispositivos del Ministerio, con el fin de detectar actividades anómalas, respaldar la investigación de incidentes, soportar auditorías y demostrar el cumplimiento de los controles de seguridad.

1.10.2 Alcance

Esta política aplica a todos los activos tecnológicos administrados por el Ministerio que generen o puedan generar registros de eventos, incluyendo:

- Servidores, sistemas operativos y bases de datos.
- Aplicaciones institucionales (incluyendo desarrollos propios y de terceros).
- Dispositivos de red, firewalls, IDS/IPS, soluciones VPN y herramientas de DLP.
- Estaciones de trabajo y dispositivos móviles administrados.
- Servicios en la nube y plataformas de colaboración institucionales.

1.10.3 Eventos mínimos a registrar

Los sistemas y aplicaciones deberán registrar, como mínimo, los siguientes eventos cuando técnicamente sea posible:

- Intentos de autenticación exitosos y fallidos.
- Creación, modificación y eliminación de cuentas de usuario.
- Cambios y uso de privilegios elevados (administrador, root, sudo).
- Accesos a información clasificada como Privada o Confidencial.
- Cambios de configuración en sistemas críticos.
- Inicio, detención y reinicio de servicios críticos.
- Conexiones de medios removibles (cuando aplique la política de almacenamiento masivo).
- Eventos de seguridad detectados por antimalware, EDR, firewall, IDS/IPS.
- Accesos remotos y eventos de VPN.
- Errores y fallos relevantes del sistema.

1.10.4 Contenido mínimo de los registros

Cada registro deberá contener, como mínimo:

- Fecha y hora del evento (sincronizadas mediante NTP).
- Identificador del usuario o sistema involucrado.
- Origen del evento (dirección IP, hostname, aplicación).
- Tipo de evento y descripción.
- Resultado (éxito, falla, denegación).

1.10.5 Sincronización temporal

Todos los dispositivos y sistemas que generen logs deberán estar sincronizados con una fuente de tiempo confiable (NTP), preferentemente bajo la zona horaria oficial del Ministerio, para garantizar la correlación correcta de eventos.

1.10.6 Almacenamiento, protección y retención

- **Centralización:** los logs de sistemas y servicios críticos deberán ser enviados a una plataforma centralizada (SIEM o equivalente) administrada por la DISI.
- **Integridad:** los registros deberán protegerse contra modificación o eliminación no autorizada, mediante controles de acceso, cifrado en tránsito y, cuando aplique, mecanismos de no repudio.
- **Retención mínima:** los registros de seguridad deberán conservarse por un mínimo de 12 meses, salvo que la normativa aplicable o el análisis de riesgo establezcan un periodo mayor.
- **Respaldo:** los logs centralizados deberán incluirse en los esquemas de respaldo conforme al Manual de Resguardo de la Información.

1.10.7 Monitoreo y análisis

- La DISI realizará monitoreo continuo de los eventos críticos mediante alertas automatizadas.
- Se efectuarán revisiones periódicas para detectar patrones anómalos, intentos de intrusión y comportamiento sospechoso.
- Los hallazgos relevantes generarán un incidente y se gestionarán conforme a la Política de Gestión de Incidentes (sección 1.8).

1.10.8 Acceso a los registros

- El acceso a los registros estará restringido al personal autorizado de la DISI bajo el principio de menor privilegio.
- Las consultas a los registros con fines de investigación o auditoría deberán quedar formalmente documentadas.

- El acceso a logs por parte de auditores internos o externos requerirá autorización formal.

1.10.9 Privacidad y proporcionalidad

El monitoreo de eventos se realizará exclusivamente con fines legítimos de seguridad de la información, operación y cumplimiento, respetando los derechos de privacidad del personal y observando la legislación aplicable. El alcance del monitoreo es comunicado al personal mediante la presente política y los avisos institucionales correspondientes.

1.10.10 Revisión y cumplimiento

Actividad	Descripción	Frecuencia
Verificación de cobertura	Validar que los sistemas críticos estén enviando logs al SIEM.	Mensual
Revisión de alertas	Análisis de alertas críticas y ajuste de reglas.	Continua
Auditoría de integridad	Verificación de que los logs no han sido alterados o eliminados.	Trimestral
Prueba de sincronización	Validar la sincronización NTP de los activos.	Trimestral

La desactivación, manipulación o eliminación no autorizada de registros de eventos será considerada falta grave y dará lugar a las acciones disciplinarias correspondientes.

1.11 Política de privacidad y protección de datos personales

1.11.1 Propósito

Establecer los principios, lineamientos y controles para el tratamiento legítimo, seguro y responsable de los datos personales que el Ministerio recopila, almacena, procesa, transmite o conserva en cumplimiento de sus funciones, protegiendo los derechos de los titulares y minimizando los riesgos de uso indebido, fuga o divulgación no autorizada.

1.11.2 Alcance

Esta política aplica al tratamiento de cualquier dato personal, en formato físico o digital, que sea recopilado o gestionado por el Ministerio, incluyendo:

- Datos personales del personal interno, contratistas y proveedores.
- Datos personales de usuarios externos, ciudadanos y solicitantes de servicios.
- Datos sensibles (cuando se manejen): información de salud, biométrica, de seguridad social u otra protegida por la legislación aplicable.

Aplica además a todo el personal interno, contratistas, proveedores y terceros que tengan acceso a datos personales bajo administración del Ministerio.

1.11.3 Principios rectores

- **Licitud y lealtad:** el tratamiento de datos personales debe contar con una base legal o consentimiento, y debe realizarse de manera transparente.
- **Finalidad:** los datos solo pueden ser tratados para los fines explícitos, legítimos y previamente informados; el cambio de finalidad requiere nueva autorización o base legal.
- **Proporcionalidad y minimización:** se recolectarán únicamente los datos estrictamente necesarios para los fines establecidos.
- **Exactitud:** los datos deberán mantenerse exactos y actualizados, corrigiéndolos o eliminándolos cuando sean inexactos.
- **Conservación limitada:** los datos serán conservados solo por el tiempo necesario para cumplir los fines o las obligaciones legales aplicables.
- **Integridad y confidencialidad:** los datos serán protegidos mediante controles técnicos y organizativos adecuados.
- **Responsabilidad demostrable:** el Ministerio debe poder demostrar el cumplimiento de los principios y obligaciones.
-

1.11.4 Derechos de los titulares

El Ministerio reconoce y atenderá, conforme a la legislación aplicable, los derechos de los titulares de los datos personales, incluyendo:

- Acceso a sus datos personales y a la información sobre su tratamiento.
- Rectificación de datos inexactos o incompletos.
- Cancelación o supresión cuando legalmente proceda.

- Oposición al tratamiento por motivos legítimos.
- Información clara sobre los fines, destinatarios y bases del tratamiento.

Las solicitudes de los titulares se atenderán a través de los canales formales definidos por el Ministerio, dentro de los plazos legales.

1.11.5 Tratamiento por terceros y encargados

Cuando el Ministerio comparta datos personales con proveedores o terceros (encargados del tratamiento), deberán observarse las siguientes condiciones:

- Suscripción de acuerdos de confidencialidad y, cuando aplique, contratos de tratamiento de datos.
- Verificación de que el tercero implementa medidas de seguridad equivalentes a las del Ministerio.
- Prohibición al tercero de utilizar los datos para fines distintos a los pactados.
- Compromiso del tercero de devolver o destruir los datos al finalizar el servicio.

1.11.6 Controles de seguridad aplicables

El tratamiento de datos personales estará sujeto a los controles definidos en las demás políticas del presente manual, en particular:

- Clasificación y manejo de la información (sección 1.3): los datos personales serán tratados al menos como Privados; los datos sensibles como Confidenciales.
- Control de acceso (sección 2.1): aplicación estricta de los principios de mínimo privilegio y necesidad de conocer.
- Comunicaciones (sección 1.6) y almacenamiento masivo (sección 2.8): cifrado obligatorio para la transmisión y traslado fuera de la institución.
- Registro y monitoreo (sección 1.10): registro de los accesos a sistemas que contengan datos personales.
- Gestión de incidentes (sección 1.8): tratamiento especial de las brechas que involucren datos personales.

1.11.7 Brechas que involucran datos personales

Toda incidencia que implique pérdida, acceso, divulgación o alteración no autorizada de datos personales será considerada una brecha de datos y será gestionada conforme a la Política de Gestión de Incidentes (sección 1.8). Adicionalmente:

- Deberá evaluarse el impacto sobre los titulares afectados.

- Cuando corresponda, se notificará a las autoridades competentes y a los titulares, conforme a la legislación aplicable, en los plazos previstos por esta.
- Se documentarán las causas, el alcance y las medidas correctivas adoptadas.

1.11.8 Responsabilidades

- **Alta dirección:** definir el marco institucional de privacidad, asignar recursos y supervisar su cumplimiento.
- **DISI:** implementar los controles técnicos para proteger los datos personales y soportar la atención de derechos e incidentes.
- **Áreas usuarias:** tratar los datos personales conforme a esta política y solo para los fines de su competencia.
- **Personal y terceros:** respetar la confidencialidad, reportar incidentes y abstenerse de divulgar datos fuera de los fines autorizados.

1.11.9 Revisión y cumplimiento

- Revisión anual de los inventarios de tratamientos de datos personales y de las medidas aplicables.
- Capacitación obligatoria al personal sobre privacidad y protección de datos.
- Auditorías periódicas para verificar el cumplimiento de la política.

El uso indebido, la divulgación no autorizada o el tratamiento de datos personales fuera de los fines establecidos serán considerados faltas graves y darán lugar a las acciones disciplinarias correspondientes, sin perjuicio de las responsabilidades civiles o penales que en su caso resulten aplicables conforme a la legislación vigente.

2. Usuarios

Las políticas contenidas en esta sección establecen los lineamientos institucionales aplicables a todas las personas usuarias de los sistemas, equipos y servicios provistos por el Ministerio, incluyendo el control de acceso, el uso aceptable de activos, el manejo de información en el puesto de trabajo, los dispositivos móviles, el teletrabajo, los medios de almacenamiento removibles y el software.

2.1 Política de control de acceso

2.1.1 Propósito

Establecer los principios y responsabilidades para la gestión del control de acceso a la información, sistemas, aplicaciones, redes y servicios del Ministerio de Trabajo y Previsión Social.

Busca garantizar la confidencialidad, integridad y disponibilidad de los activos de información, previniendo el acceso no autorizado y asegurando que solo el personal debidamente autorizado pueda acceder a los recursos necesarios para el cumplimiento de sus funciones.

Asimismo, establece los criterios y controles para gestionar las identidades digitales y los permisos de acceso, garantizando que el acceso a las aplicaciones, redes y sistemas se conceda con base en la necesidad de saber y el principio de menor privilegio.

2.1.2 Alcance

Esta política aplica a:

- Todo el personal del Ministerio (empleados permanentes, temporales, contratistas, consultores, practicantes y cualquier tercero con acceso a los recursos del Ministerio).
- Todos los sistemas de información, aplicaciones, bases de datos, redes y equipos tecnológicos propiedad del Ministerio o gestionados por este, independientemente de su ubicación física o lógica.
- Toda la información del Ministerio, en cualquier formato (digital o físico), clasificada como pública, interna, privada o confidencial.

2.1.3 Principios generales del control de acceso

El Ministerio se compromete a implementar un control de acceso basado en los siguientes principios:

- **Necesidad de conocer (need-to-know):** el acceso a la información y los sistemas se otorgará únicamente cuando sea estrictamente necesario para el desempeño de las funciones laborales.
- **Privilegios mínimos (least privilege):** a los usuarios se les otorgarán los niveles de acceso y privilegios más bajos posibles que les permitan realizar sus tareas asignadas. No se concederán privilegios de acceso excesivos.
- **Segregación de funciones (segregation of duties):** las responsabilidades críticas y sensibles se dividirán entre diferentes individuos para reducir el riesgo de fraude o error no detectado.
- **Responsabilidad individual:** cada usuario es responsable de proteger sus credenciales de acceso y de cualquier actividad realizada bajo su identidad de usuario.
- **Revisión periódica:** los derechos de acceso de los usuarios se revisarán periódicamente y se ajustarán cuando haya cambios de rol, transferencias o cese de relación laboral.

2.1.4 Gestión del acceso de usuarios

2.1.4.1 Registro y baja de usuarios

- Se establecerán procedimientos formales para el registro y la provisión de acceso de nuevos usuarios, incluyendo la autorización del director correspondiente y la Dirección de Sistemas de Información (DISI).
- Se implementarán procedimientos expeditos para la modificación o baja de acceso de usuarios que cambien de rol, se ausenten temporalmente o finalicen su relación laboral con el Ministerio, garantizando que el acceso se retire de forma oportuna.

2.1.4.2 Provisión de acceso y gestión de privilegios

- Todo acceso a sistemas y recursos sensibles requerirá una justificación documentada y la aprobación explícita de la Dirección responsable.
- Los privilegios de acceso (por ejemplo, acceso de administrador o superusuario) se otorgarán y supervisarán con especial rigor, limitándolos al mínimo necesario y registrando su uso.

2.1.4.3 Gestión de la información de autenticación

- Se requerirá el uso de contraseñas robustas que cumplan con criterios de complejidad, longitud mínima y cambios periódicos.
- Queda estrictamente prohibido compartir credenciales de acceso (contraseñas, PIN, tarjetas, etc.) entre usuarios.
- La DISI gestiona sistemas seguros para la creación, almacenamiento y recuperación de contraseñas de acceso a los equipos.
- Será de uso obligatorio la autenticación de dos factores (MFA) o más para el acceso a sistemas críticos y redes remotas, cuando sea aplicable.

2.1.4.4 Política de contraseñas

Se establecen los siguientes parámetros técnicos mínimos para todos los sistemas:

Parámetro	Requerimiento
Longitud mínima	Al menos 12 caracteres.
Complejidad	Combinación de mayúsculas, minúsculas, números y símbolos.
Vigencia	Cambio obligatorio cada 90 días (o según análisis de riesgo).
Historial	No se pueden repetir las últimas 10 contraseñas utilizadas.
Bloqueo	La cuenta se bloqueará automáticamente tras 5 intentos fallidos consecutivos (ver subsección 2.1.4.5).

2.1.4.5 Bloqueo de cuentas por intentos fallidos de inicio de sesión

Con el propósito de proteger las credenciales del personal frente a ataques de fuerza bruta, intentos de adivinación de contraseñas, acceso no autorizado y uso indebido, el Ministerio adopta un mecanismo de bloqueo automático de cuentas tras un número determinado de intentos fallidos de inicio de sesión.

Parámetros aplicables. Los sistemas, aplicaciones y servicios institucionales que permitan autenticación de usuarios deberán configurarse, cuando técnicamente sea posible, conforme a los siguientes parámetros mínimos:

Parámetro	Valor
Umbral de intentos fallidos	5 intentos consecutivos.
Tipo de bloqueo	Permanente, hasta desbloqueo manual por parte de la DISI.
Contador	Los intentos fallidos se acumulan por cuenta de usuario, independientemente del equipo o ubicación desde el cual se intente el acceso.
Reinicio del contador	El contador se reinicia tras un inicio de sesión exitoso o tras un desbloqueo formal.
Notificación	El usuario recibirá un mensaje genérico de bloqueo, sin detalles que puedan facilitar ataques. La DISI será notificada automáticamente del evento.

Alcance. El mecanismo de bloqueo aplica a todas las cuentas de usuario gestionadas por el Ministerio, incluyendo:

- Cuentas de usuario final para inicio de sesión en equipos institucionales (dominio Active Directory o servicio de identidad equivalente).
- Cuentas para acceso a sistemas, aplicaciones y bases de datos institucionales.
- Cuentas para acceso al correo institucional y plataformas de colaboración.
- Cuentas para acceso remoto vía VPN.
- Cuentas privilegiadas (administradores, superusuarios), las cuales aplicarán los mismos parámetros con tratamiento prioritario en su desbloqueo y atención.

Procedimiento de desbloqueo. El desbloqueo de la cuenta no se realizará de manera automática por tiempo; requerirá la intervención manual de la DISI conforme al siguiente procedimiento:

- El usuario afectado deberá comunicarse con el área de soporte técnico de la DISI a través de los canales oficiales (línea telefónica de soporte, sistema de tickets o presencialmente).
- El usuario deberá identificarse mediante los mecanismos definidos por la DISI, los cuales podrán incluir verificación de identidad por datos personales, código

de empleado, validación con su jefatura inmediata u otro mecanismo equivalente, según el nivel de criticidad de la cuenta.

- La DISI verificará la legitimidad de la solicitud, revisará el evento que originó el bloqueo en las bitácoras del sistema y, en su caso, procederá al desbloqueo.
- Si durante la verificación se detectan indicios de un intento de acceso no autorizado, el desbloqueo quedará suspendido y el evento será escalado conforme a la Política de Gestión de Incidentes (sección 1.8).
- Toda solicitud de desbloqueo quedará registrada en el sistema de tickets con identificación del usuario, fecha, hora, causa y responsable que ejecuta el desbloqueo.

Tiempos de atención. El desbloqueo de cuentas se atenderá conforme a los siguientes tiempos objetivo, dentro del horario de operación de la DISI:

- Cuentas de usuario final: atención dentro de 1 hora hábil desde la recepción de la solicitud.
- Cuentas privilegiadas o de personal directivo: atención prioritaria dentro de 30 minutos hábiles.
- Cuentas de servicio o cuentas vinculadas a procesos críticos: atención inmediata bajo el procedimiento de incidentes.

Cuentas de servicio y cuentas técnicas. Las cuentas de servicio (no asociadas a personas, utilizadas por sistemas o procesos automatizados) estarán sujetas a un esquema diferenciado de monitoreo. Su bloqueo se tratará como un incidente operativo y será atendido directamente por la DISI sin requerir solicitud del usuario, debiendo investigarse la causa raíz antes de su desbloqueo.

Registro y monitoreo. Todo evento de bloqueo de cuenta deberá:

- Quedar registrado en las bitácoras del sistema de autenticación correspondiente.
- Ser remitido a la plataforma de registro y monitoreo centralizado conforme a la Política de Registro y Monitoreo de Eventos (sección 1.10).
- Generar alertas automáticas cuando se detecten patrones anómalos, como bloqueos múltiples de distintas cuentas en periodos cortos, bloqueos de cuentas privilegiadas o intentos desde ubicaciones inusuales.
- Ser tratado como un evento de seguridad potencial, escalable a incidente conforme a la Política de Gestión de Incidentes (sección 1.8) cuando existan indicios de compromiso.

Responsabilidades del usuario. El personal del Ministerio tiene las siguientes responsabilidades en relación con esta norma:

- Custodiar y memorizar sus credenciales de acceso, evitando intentos repetidos basados en suposición.
- Utilizar los mecanismos institucionales de recuperación o restablecimiento de contraseña antes de agotar los intentos disponibles.
- Reportar de inmediato a la DISI cualquier bloqueo de cuenta que no haya originado o que considere sospechoso, ya que podría indicar un intento de acceso no autorizado por terceros.
- No solicitar el desbloqueo de cuentas ajenas, salvo cuando se actúe en representación formalmente autorizada (por ejemplo, jefatura inmediata reportando por personal ausente).

Prohibiciones. Queda estrictamente prohibido:

- Eludir, deshabilitar o manipular el mecanismo de bloqueo de cuentas en cualquier sistema.
- Configurar excepciones al mecanismo de bloqueo sin la aprobación formal de la DISI.
- Solicitar desbloqueos suplantando la identidad de otro usuario.
- Realizar desbloqueos sin la verificación de identidad prevista en el procedimiento.

Revisión y cumplimiento. La DISI mantendrá indicadores periódicos sobre la cantidad de bloqueos, tiempos de atención y eventos escalados a incidentes; revisará trimestralmente los patrones de bloqueo para identificar posibles ataques o necesidades de capacitación al personal; y verificará anualmente que los sistemas críticos mantengan correctamente configurados los parámetros establecidos en la presente norma. La manipulación o elusión deliberada de este control será considerada falta grave y se atenderá conforme a la normativa interna del Ministerio.

2.1.5 Control de acceso a redes, sistemas y aplicaciones

2.1.5.1 Acceso a la red

- **Segmentación:** la red debe estar segmentada (VLAN). Los usuarios de áreas administrativas no deben tener acceso a la red de servidores o bases de datos a menos que sea estrictamente necesario.
- **Control de admisión (NAC):** solo dispositivos autorizados por el Ministerio pueden conectarse a la red cableada o Wi-Fi corporativa.

2.1.5.2 Acceso a redes y servicios de red

El acceso a las redes y servicios de red del Ministerio será gestionado bajo estrictos principios de seguridad para salvaguardar la información y la infraestructura. Se implementarán los siguientes controles:

- **Mecanismos robustos de autenticación y autorización:** todo intento de acceso a las redes del Ministerio requerirá el uso de mecanismos de autenticación fuertes, como credenciales únicas de usuario y contraseña y, donde sea posible, la autenticación multifactor (MFA). La autorización para acceder a recursos específicos se basará en el principio de privilegios mínimos.
- **Segmentación de red para aislamiento crítico:** se implementará y mantendrá una segmentación lógica de la red, dividiendo la red en zonas o segmentos aislados para entornos críticos como servidores de bases de datos, sistemas financieros o información altamente sensible.
- **Acceso remoto seguro y controlado:** el acceso remoto a la red y a los sistemas del Ministerio (incluyendo modalidades de teletrabajo) se permitirá exclusivamente a través de conexiones seguras y cifradas, como las redes privadas virtuales (VPN), utilizando equipos y software aprobados y configurados por la DISI.
- **Control de acceso a dispositivos de red:** el acceso a routers, switches, firewalls y puntos de acceso inalámbricos estará estrictamente restringido al personal autorizado de la DISI, con credenciales robustas y únicas; se deshabilitarán las cuentas por defecto.
- **Protección de puertos y servicios innecesarios:** se desactivarán los puertos y servicios de red que no sean estrictamente necesarios. La apertura requerirá justificación, análisis de riesgo y aprobación formal de la DISI.

- **Gestión segura de redes inalámbricas (Wi-Fi):** las redes inalámbricas deberán estar protegidas con mecanismos de cifrado fuertes (por ejemplo, WPA3) y autenticación segura. Se implementará segmentación entre redes para invitados y redes corporativas, y se prohibirá el uso de redes Wi-Fi personales no autorizadas para conectar dispositivos corporativos.
- **Control de acceso de proveedores externos:** se permitirá solo cuando sea estrictamente necesario, bajo acuerdo formal de confidencialidad y seguridad, limitado en alcance, temporal y monitoreado de cerca.

2.1.5.3 Control de acceso lógico a sistemas y aplicaciones

El Ministerio implementará controles rigurosos para gestionar el acceso lógico a todos sus sistemas de información, bases de datos y aplicaciones:

- **Gestión de acceso por dueños de sistemas:** los accesos serán gestionados por los responsables designados de cada sistema, quienes definen los perfiles de usuario y privilegios en función de las funciones laborales. La DISI brindará el soporte técnico para implementar estos controles.
- **Autenticación de usuario individual obligatoria:** todos los sistemas y aplicaciones del Ministerio exigirán una autenticación de usuario individual, evitando el uso de cuentas compartidas o genéricas.
- **Procedimientos de inicio de sesión seguros:** incluyen información mínima en mensajes de error que no faciliten ataques, gestión de sesiones con tiempos de inactividad y prohibición de sesiones concurrentes en sistemas críticos. La protección contra ataques de fuerza bruta se desarrolla en la subsección 2.1.4.5.
- **Control y monitoreo de utilidades privilegiadas:** el uso de utilidades que otorgan privilegios elevados o que pueden eludir los controles de seguridad será restringido al personal técnico autorizado de la DISI, con justificación documentada y registro de su uso.
- **Restricción de acceso al código fuente:** el acceso al código fuente de las aplicaciones se restringirá estrictamente al personal autorizado y se implementarán sistemas de control de versiones para asegurar trazabilidad e integridad.

2.1.5.4 Vinculación de cuentas de usuario a equipos asignados

Con el propósito de reforzar la trazabilidad, reducir la superficie de ataque y garantizar la responsabilidad individual sobre el uso de los equipos institucionales, el Ministerio adopta un modelo de vinculación de cuentas de usuario a equipos específicos, bajo un esquema flexible de un equipo principal y, cuando corresponda, equipos secundarios autorizados.

Principio general. Cada cuenta de usuario tendrá asociado un equipo principal en el cual se le habilitará el inicio de sesión de manera predeterminada. El acceso desde equipos distintos al asignado quedará bloqueado a menos que medie una autorización formal.

Equipo principal. Es el equipo de cómputo (de escritorio o portátil institucional) asignado formalmente al usuario al momento de su contratación o cambio de rol. Será el único equipo donde la cuenta podrá iniciar sesión sin restricción adicional.

Equipos secundarios autorizados. El usuario podrá solicitar la habilitación de equipos secundarios cuando existan razones operativas legítimas, tales como rotación entre puestos, uso de estaciones especializadas, participación en proyectos específicos o respaldo temporal por mantenimiento del equipo principal. La habilitación procederá mediante el siguiente procedimiento:

- Solicitud formal del usuario ante su jefatura inmediata, justificando la necesidad y el período de uso.
- Aval de la jefatura y remisión a la DISI.
- Evaluación técnica por parte de la DISI y, en su caso, habilitación con vigencia definida.
- Registro en el inventario de vinculaciones, con identificador del usuario, equipos asociados, vigencia y motivo.

Equipos compartidos. Los equipos compartidos institucionales (kioscos, estaciones de consulta, salas de capacitación, equipos de uso colectivo, equipos de sala de reuniones, entre otros) quedan exceptuados del principio de equipo único, pero se les aplicarán los siguientes controles:

- Inicio de sesión únicamente con cuentas individuales nominales; queda prohibido el uso de cuentas genéricas o compartidas.
- Limitación del acceso únicamente a las cuentas previamente autorizadas para utilizar dicho equipo, conforme a las funciones del usuario.
- Cierre automático de sesión por inactividad en un periodo no mayor a 5 minutos.
- Prohibición de almacenar archivos institucionales de manera local; toda la información deberá residir en los repositorios institucionales correspondientes.
- Registro detallado de los inicios y cierres de sesión para fines de auditoría.

Equipos institucionales portátiles (laptops). Las laptops institucionales asignadas a un usuario se considerarán su equipo principal y conservarán la vinculación incluso fuera de las instalaciones, en concordancia con la Política de teletrabajo y acceso remoto (sección 2.8).

Excepciones y casos especiales. Las siguientes situaciones serán tratadas mediante el procedimiento de habilitación temporal:

- Mantenimiento, reparación o reemplazo del equipo principal: la DISI habilitará un equipo de respaldo y registrará la vinculación temporal.
- Comisiones, capacitaciones o asignaciones en sedes distintas a la habitual: habilitación por el periodo correspondiente.
- Personal directivo o de soporte técnico cuyo rol requiera movilidad: podrá contar con un perfil de movilidad ampliada, autorizado por la dirección del área y la DISI, con registro y revisión periódica.
- Cuentas administrativas o de servicio: se vinculan a los servidores o estaciones técnicas correspondientes a su función y no podrán utilizarse para inicio de sesión interactivo en equipos de usuario final.

Conductas prohibidas. Queda estrictamente prohibido:

- Iniciar sesión con la cuenta propia en equipos no autorizados para el usuario.
- Permitir que otra persona inicie sesión con sus credenciales en cualquier equipo, autorizado o no.
- Utilizar la cuenta de un compañero, aun con su consentimiento, para iniciar sesión en cualquier equipo.
- Intentar eludir, deshabilitar o manipular los controles técnicos que limitan el inicio de sesión a los equipos autorizados.

Controles técnicos. La DISI implementará y mantendrá los controles necesarios para hacer efectiva la vinculación, entre ellos:

- Restricción de inicio de sesión por equipo a nivel de directorio activo (Active Directory) u otro servicio de identidad, mediante el atributo de estaciones de trabajo autorizadas u objetos de política de grupo equivalentes.
- Mantenimiento del inventario de equipos asignados y de las vinculaciones usuario–equipo.
- Registro y monitoreo de intentos de inicio de sesión en equipos no autorizados; estos serán tratados como eventos relevantes conforme a la Política de Registro y Monitoreo de Eventos (sección 1.10).
- Alertas automáticas para intentos reiterados de acceso desde equipos no autorizados, conforme a la Política de Gestión de Incidentes (sección 1.8).

Revisión. La DISI revisará semestralmente las vinculaciones vigentes para detectar autorizaciones que ya no sean necesarias y proceder a su revocación. Adicionalmente, las vinculaciones temporales serán revocadas automáticamente al vencimiento de su plazo.

2.1.6 Responsabilidades del usuario

Todo el personal del Ministerio tiene la responsabilidad de:

- **Protección y confidencialidad de credenciales:** cada usuario debe proteger sus credenciales de acceso y en ninguna circunstancia compartirlas con terceros, incluido el personal de soporte técnico. El uso de credenciales ajenas o el acceso no autorizado son faltas graves.
- **Cumplimiento de políticas y procedimientos:** conocer y adherirse estrictamente a todas las políticas, estándares y procedimientos de seguridad de la información establecidos por el Ministerio.
- **Reporte de incidentes de seguridad:** reportar de manera inmediata a la DISI cualquier incidente, sospecha de acceso no autorizado, vulnerabilidad, pérdida o robo de equipos, o cualquier actividad que ponga en riesgo la información.
- **Uso aceptable y ético de recursos:** utilizar los recursos tecnológicos exclusivamente para fines oficiales conforme a la política de uso aceptable de activos.
- **Cierre de sesiones y bloqueo de dispositivos:** cerrar sesiones o bloquear estaciones de trabajo cada vez que se ausenten del puesto, incluso por breves periodos.
- **Apagado de equipos al retirarse:** al finalizar la jornada laboral, apagar completamente los equipos de cómputo. Esto contribuye a la seguridad y a la eficiencia energética.

- **Conciencia de seguridad:** mantenerse informado sobre las mejores prácticas y estar atento a intentos de fraude (phishing, ingeniería social, etc.).

2.1.7 Revisión y cumplimiento

- **Revisión de privilegios (user access review):** semestralmente, los responsables de cada proceso deben revisar la lista de usuarios con acceso a sus aplicaciones para confirmar que sigan siendo válidos.
-

- **Auditoría de logs de acceso:** monitoreo activo de intentos de inicio de sesión fallidos o accesos en horarios inusuales.
- **Cuentas huérfanas:** escaneo mensual para detectar y eliminar cuentas de usuarios que ya no pertenecen al Ministerio.

Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos en el entorno tecnológico o normativo. El incumplimiento, como el préstamo de credenciales o la creación de cuentas no autorizadas (shadow accounts), será considerado una falta grave de seguridad y podrá dar lugar a acciones disciplinarias de acuerdo con la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

2.2 Política de copias de seguridad de software de usuario final

2.2.1 Propósito

Establecer los lineamientos para el respaldo y recuperación de la información almacenada por los usuarios finales en sus equipos de cómputo asignados, garantizando la disponibilidad y recuperabilidad de los datos institucionales en caso de fallas, pérdidas o incidentes.

2.2.2 Alcance

Aplica a la información institucional almacenada en equipos de cómputo de escritorio, portátiles y dispositivos asignados al personal del Ministerio.

2.2.3 Contenido

Los lineamientos operativos y técnicos aplicables al respaldo de la información de usuarios finales se encuentran desarrollados en el documento *Manual de Resguardo de la Información de la Dirección de Sistemas de Información*, el cual forma parte integral de la presente política como anexo técnico de referencia.

2.2.4 Revisión y cumplimiento

La DISI verificará periódicamente el cumplimiento de los procedimientos de respaldo por parte de los usuarios finales y proveerá las herramientas y orientaciones necesarias para su correcta ejecución.

2.3 Política de uso aceptable de activos

2.3.1 Propósito

Establecer las normas que rigen el uso de los activos de hardware y software proporcionados por el Ministerio. El fin es garantizar que estos recursos se utilicen de

manera ética, legal y segura, protegiendo la reputación y la continuidad operativa de la institución.

2.3.2 Alcance

Esta política aplica a todos los empleados, consultores y terceros que tengan asignado o utilicen cualquier activo informático propiedad del Ministerio, incluyendo:

- Dispositivos finales (laptops, equipos de escritorio, tabletas, teléfonos inteligentes).
- Periféricos (monitores, impresoras, discos externos).
- Software y licencias institucionales.

2.3.3 Normas de uso de los activos

- **Propiedad institucional:** todos los activos son propiedad exclusiva del Ministerio. El usuario tiene la custodia, pero no la propiedad de los mismos.
- **Uso profesional:** los activos están destinados primordialmente al cumplimiento de las funciones laborales. El uso personal ocasional está permitido siempre que no interfiera con la productividad ni comprometa la seguridad.
- **Cuidado físico:** el usuario es responsable del cuidado físico del equipo. No debe dejarse en vehículos, lugares públicos sin supervisión o áreas de alto riesgo de robo o daño.
- **Modificaciones prohibidas:** no se permite la apertura física de los equipos ni la alteración de los componentes de hardware (memoria RAM, discos, etc.) sin autorización de la DISI.

2.3.4 Software y seguridad lógica

- **Instalación de software:** queda estrictamente prohibida la instalación de software que no cuente con una licencia institucional o que no haya sido aprobado por la DISI (evitando el shadow IT).
- **Protección de endpoint:** el usuario no debe desactivar, modificar o desinstalar el software de seguridad (antivirus, EDR, firewall local) instalado en el equipo.
- **Cifrado de datos:** en dispositivos móviles (laptops y teléfonos celulares), el cifrado de disco debe estar activo en todo momento para proteger la información en caso de pérdida o robo.

2.3.5 Responsabilidades del usuario

Acción	Responsabilidad del usuario
Transporte	Utilizar mochilas o fundas protectoras adecuadas para el traslado.
Custodia	No prestar el equipo a familiares, amigos o terceros no autorizados.
Notificación	Reportar cualquier pérdida, robo o daño físico de forma inmediata (máximo 2 horas después del evento).
Devolución	Entregar el equipo en condiciones óptimas al cese de la relación laboral o cambio de rol.

2.3.6 Prohibiciones explícitas

El uso de los activos para las siguientes actividades resultará en medidas disciplinarias:

- Realizar actividades ilegales o fraudulentas.
- Almacenar o distribuir material ofensivo, discriminatorio o pornográfico.
- Intentar vulnerar la seguridad de sistemas propios o ajenos (hacking).
- Minería de criptomonedas.
- Descarga de contenido protegido por derechos de autor (música o películas piratas).

2.3.7 Monitoreo y privacidad

El Ministerio se reserva el derecho de auditar cualquier activo informático para asegurar el cumplimiento de esta política. El usuario no debe tener expectativa de privacidad total sobre la información almacenada en los activos institucionales.

Compromiso de responsabilidad: al recibir un activo, el usuario deberá firmar una carta de responsabilidad donde acepta los términos de esta política y se compromete a su cumplimiento.

2.3.8 Revisión y cumplimiento

Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos. El incumplimiento podrá dar lugar a acciones disciplinarias de acuerdo con la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

2.4 Política de escritorio y pantalla limpios

2.4.1 Propósito

Establecer los lineamientos para reducir el riesgo de acceso no autorizado, pérdida o daño de la información durante y después de la jornada laboral. Esta política busca asegurar que la información sensible, tanto en formato físico como digital, no quede expuesta a personas no autorizadas.

2.4.2 Alcance

Esta política es obligatoria para todo el personal (empleados, contratistas y visitantes) que trabaje en las oficinas del Ministerio, así como para quienes realicen trabajo remoto en espacios compartidos.

2.4.3 Lineamientos de escritorio limpio (información física)

Se refiere a la gestión de documentos y objetos en el espacio de trabajo:

- **Documentos sensibles:** todo documento clasificado como Privado o Confidencial debe ser guardado en cajones o archivadores bajo llave cuando el usuario no esté en su puesto.
- **Retiro de impresiones:** está prohibido dejar documentos en las bandejas de las impresoras o escáneres. El usuario debe recoger sus impresiones de inmediato.
- **Notas adhesivas:** queda estrictamente prohibido escribir contraseñas en notas adhesivas y pegarlas en el monitor, teclado o debajo del escritorio.
- **Limpieza al final del día:** al terminar la jornada, el escritorio debe quedar completamente libre de documentos institucionales. Solo se permiten objetos personales mínimos y material de oficina básico.
- **Destrucción de información:** los documentos que ya no sean necesarios y contengan datos institucionales deben ser destruidos en trituradoras de papel, nunca desechados íntegros al basurero.

2.4.4 Lineamientos de pantalla limpia (información digital)

Se refiere a la protección de la información visible en monitores y dispositivos:

- **Bloqueo de sesión:** los usuarios deben bloquear su sesión (tecla Windows + L en PC o Control + Command + Q en Mac) cada vez que se levanten de su puesto, aunque sea por un breve momento.
- **Bloqueo automático:** se configurará mediante política de grupo (GPO) un bloqueo automático de pantalla tras 5 minutos de inactividad.

- **Uso de filtros de privacidad:** para empleados que manejan datos altamente sensibles en áreas de alto tráfico, se recomienda el uso de filtros de privacidad físicos en los monitores.
- **Notificaciones:** se deben configurar las notificaciones de pantalla bloqueada para que no muestren el contenido de los mensajes (correos, chats) mientras el equipo esté bloqueado.

2.4.5 Responsabilidades del usuario

Situación	Acción requerida
Ausencia breve	Bloquear la computadora y guardar documentos sensibles fuera de la vista.
Fin de jornada	Guardar bajo llave toda información física y apagar/bloquear el equipo.
Reuniones	Al finalizar una reunión, borrar pizarrones y retirar notas o copias distribuidas.

2.4.6 Revisión y cumplimiento

Para asegurar que esta política se convierta en un hábito, el Ministerio realizará:

- **Rondas de inspección:** el personal de seguridad o de la DISI realizará recorridos aleatorios fuera del horario laboral para verificar que no queden documentos expuestos o equipos desbloqueados.
- **Reporte de hallazgos:** se dejará una tarjeta de aviso (o aviso educativo equivalente) en los puestos que incumplan, notificando al responsable del área correspondiente.
- **Campaña de concientización:** envío de recordatorios visuales y correos electrónicos sobre la importancia de proteger el espacio de trabajo.

2.5 Política de restricciones a las instalaciones y uso del software

2.5.1 Propósito

Minimizar los riesgos de seguridad derivados del uso de software no autorizado o malicioso, garantizando que todo el software en los activos del Ministerio sea legal, seguro y productivo, protegiendo la integridad de los datos y la estabilidad de la red corporativa.

2.5.2 Alcance

Esta política aplica a:

- Todos los empleados, contratistas y terceros con acceso a equipos del Ministerio.
- Todo dispositivo propiedad del Ministerio (laptops, servidores, móviles).
- Cualquier software instalado, incluyendo aplicaciones de escritorio, extensiones de navegador y servicios en la nube (SaaS) que manejen datos institucionales.

2.5.3 Responsabilidades del usuario

Los usuarios finales desempeñan el papel de primera línea de defensa. Sus responsabilidades incluyen:

- **Prohibición de auto instalación:** no intentar instalar software, controladores o scripts sin la aprobación previa de la DISI.
- **Uso exclusivo profesional:** utilizar únicamente aplicaciones que tengan una justificación institucional clara.
- **Reporte de anomalías:** notificar inmediatamente a soporte técnico si un software solicita permisos inusuales o presenta comportamientos sospechosos.
- **Respeto a las licencias:** no utilizar software personal con licencias del tipo Home/Student para fines institucionales, ya que esto infringe los términos legales del proveedor.

2.5.4 Revisión y cumplimiento

Actividad	Descripción	Frecuencia
Auditoría de inventario	Escaneo automático de los equipos para detectar software no autorizado.	Trimestral
Gestión de privilegios	Eliminación de permisos de administrador local para usuarios estándar.	Permanente
Lista blanca (allowlist)	Mantenimiento de un catálogo de software preaprobado y seguro.	Actualización continua

Cualquier violación a esta política (como el uso de software vulnerado o herramientas de hackeo) será sujeta a medidas disciplinarias, que pueden incluir la revocación de accesos o la terminación del contrato laboral.

2.6 Política de protección contra software malicioso

2.6.1 Propósito

Establecer los lineamientos y controles para prevenir, detectar y responder ante la presencia de software malicioso (malware) que pueda comprometer la confidencialidad, integridad o disponibilidad de los activos de información del Ministerio.

2.6.2 Alcance

Aplica a todos los equipos de cómputo, servidores, dispositivos móviles y elementos de infraestructura tecnológica administrados por el Ministerio, así como a todo el personal y terceros que los utilicen.

2.6.3 Contenido

- **Software de protección obligatorio:** todos los equipos deberán contar con soluciones antimalware/antivirus, EDR o equivalentes, instaladas, actualizadas y administradas centralmente por la DISI.

- **Actualizaciones:** las definiciones de malware y los motores de detección deberán mantenerse actualizados de forma automática.
- **Escaneo periódico:** se realizarán escaneos automáticos programados, así como escaneos al conectar medios removibles y al abrir archivos adjuntos.
- **Bloqueo de elementos no autorizados:** queda prohibida la desactivación, modificación o desinstalación de las herramientas de protección por parte del usuario.
- **Atención de incidentes:** ante la detección de malware, la DISI ejecutará los protocolos de aislamiento, análisis, contención, erradicación y recuperación.

2.6.4 Responsabilidades del usuario

- No abrir archivos adjuntos sospechosos ni hacer clic en enlaces de origen desconocido.
- No descargar software de fuentes no oficiales.
- Reportar de inmediato a la DISI cualquier comportamiento anómalo en su equipo (lentitud súbita, ventanas emergentes, archivos cifrados, etc.).

2.6.5 Revisión y cumplimiento

La DISI mantendrá indicadores de cobertura, actualización y atención de incidentes de malware, los cuales serán revisados periódicamente. El incumplimiento podrá dar lugar a acciones disciplinarias de acuerdo con la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

2.7 Política de dispositivos móviles

2.7.1 Propósito

Establecer los lineamientos de seguridad necesarios para proteger la información institucional a la que se accede desde dispositivos móviles (teléfonos inteligentes y tabletas). El fin es prevenir la fuga de datos, el acceso no autorizado y la pérdida de activos ante robos o extravíos.

2.7.2 Alcance

Esta política aplica a todos los usuarios que vinculen sus correos institucionales, aplicaciones de gestión (CRM, ERP) o archivos del Ministerio en:

- Dispositivos proporcionados por el Ministerio.
- Dispositivos personales autorizados para uso laboral (BYOD).

2.7.3 Responsabilidades del usuario

Para mantener el acceso a los recursos del Ministerio, el usuario se compromete a:

- **Autenticación obligatoria:** mantener activo un método de bloqueo robusto (PIN de mínimo 6 dígitos, patrón complejo o biometría).
- **Actualizaciones de sistema:** instalar las actualizaciones de seguridad del sistema operativo (iOS / Android) en un plazo no mayor a 7 días tras su liberación.
- **Conexiones seguras:** evitar el uso de redes Wi-Fi públicas abiertas para acceder a datos sensibles. Se exige el uso de VPN institucional o datos móviles.
- **Prohibición de alteraciones:** no realizar procesos de jailbreak o rooting en el dispositivo, ya que esto elimina las capas de seguridad de fábrica.
- **Notificación inmediata:** informar a la DISI en menos de 2 horas en caso de robo, pérdida o sospecha de compromiso del dispositivo.

2.7.4 Revisión y cumplimiento

Control	Descripción	Aplicación
Borrado remoto	Capacidad de eliminar los datos institucionales si el dispositivo se pierde o el empleado deja el Ministerio.	Obligatorio
Cifrado de datos	El almacenamiento del dispositivo debe estar cifrado por defecto.	Obligatorio
Contenedores de datos	Separación lógica entre aplicaciones personales y profesionales.	Recomendado

2.8 Política de teletrabajo y acceso remoto

2.8.1 Propósito

Establecer los lineamientos de seguridad que el personal del Ministerio debe observar cuando realice sus funciones desde ubicaciones distintas a las instalaciones oficiales o acceda remotamente a los sistemas, servicios e información institucional, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos involucrados.

2.8.2 Alcance

Esta política aplica a todo el personal que, de manera permanente, parcial o excepcional, realice teletrabajo o acceda remotamente a los recursos del Ministerio desde:

- Su domicilio o residencia particular.
- Espacios públicos, oficinas compartidas (coworking) u hoteles.
- Centros de operación de proveedores externos autorizados.
- Cualquier ubicación distinta a las instalaciones oficiales del Ministerio.

Aplica además al uso de dispositivos institucionales y, cuando esté autorizado, al uso de dispositivos personales (BYOD).

2.8.3 Autorización

- El teletrabajo y el acceso remoto requerirán autorización formal de la jefatura inmediata, la dirección del área correspondiente y, cuando aplique, de la DISI para la habilitación técnica.

- La autorización tendrá una vigencia definida, podrá ser revocada en cualquier momento por razones de seguridad o cambio de funciones, y deberá renovarse periódicamente.
- El personal con acceso remoto debe firmar un compromiso de cumplimiento de la presente política.

2.8.4 Requisitos técnicos mínimos

- **Conexión:** el acceso a los recursos del Ministerio se realizará exclusivamente a través de la VPN institucional con autenticación de doble factor (MFA), salvo para servicios diseñados específicamente para acceso público (por ejemplo, portal web institucional).
- **Equipo:** preferentemente, equipo institucional cifrado, con antimalware activo y actualizaciones al día. Cuando se autorice BYOD, el equipo personal deberá cumplir con los requisitos mínimos definidos por la DISI.
- **Red doméstica:** el usuario debe asegurar que su red doméstica cuente con contraseña robusta, cifrado WPA2 o WPA3 y firmware actualizado del enrutador.
- **Redes públicas:** queda prohibido el acceso a información institucional desde redes Wi-Fi públicas abiertas sin VPN. Para tareas críticas se exige el uso de datos móviles o redes confiables.
- **Almacenamiento:** la información institucional debe permanecer dentro de los sistemas y repositorios institucionales; no debe almacenarse en discos locales no cifrados ni en servicios en la nube personales.

2.8.5 Lineamientos para el entorno de trabajo remoto

- **Confidencialidad del entorno:** el usuario debe procurar un entorno físico que evite la observación o escucha por terceros, especialmente en llamadas o videoconferencias con información sensible.
- **Bloqueo de pantalla:** aplica la política de escritorio y pantalla limpios (sección 2.4) también en el entorno remoto.
- **Impresión:** se evitará la impresión de documentos institucionales en el entorno remoto; cuando sea indispensable, se garantizará la destrucción segura conforme a la política de clasificación de la información (sección 1.3).
- **Custodia:** el equipo institucional y los documentos físicos deben mantenerse bajo custodia personal, no compartidos con familiares ni terceros.

2.8.6 Conexiones y plataformas autorizadas

- Solo se utilizarán las plataformas de videoconferencia, mensajería, almacenamiento en la nube y herramientas colaborativas aprobadas por el Ministerio.
- No se permite la instalación de software personal con fines laborales sin aprobación de la DISI.
- El acceso a sistemas críticos podrá restringirse según la ubicación geográfica o el perfil de riesgo del usuario remoto.

2.8.7 Responsabilidades del usuario

- Cumplir todas las políticas del presente manual, incluso fuera de las instalaciones.
- Notificar a la DISI de inmediato la pérdida, robo o compromiso del equipo o de las credenciales.
- No permitir el uso de equipos o credenciales institucionales por parte de terceros, incluidos familiares.
- Mantener actualizado el equipo y la VPN conforme a las indicaciones de la DISI.
- Devolver el equipo institucional y eliminar la información del Ministerio de los equipos personales al terminar la modalidad de teletrabajo o el vínculo laboral.

2.8.8 Revisión y cumplimiento

- La DISI monitoreará periódicamente las conexiones VPN, sesiones remotas y eventos asociados al teletrabajo.
- Las autorizaciones de acceso remoto serán revisadas al menos semestralmente.
- Esta política será revisada anualmente o cuando cambien las condiciones operativas o tecnológicas.

El incumplimiento podrá dar lugar a la revocación inmediata del acceso remoto y a las acciones disciplinarias correspondientes, conforme a la normativa interna del Ministerio y la legislación laboral vigente en Guatemala.

2.9 Política de uso y regulación de dispositivos de almacenamiento masivo

2.9.1 Propósito

Establecer los lineamientos, responsabilidades y controles que regulan el uso de dispositivos de almacenamiento masivo extraíbles dentro del Ministerio, con la finalidad de proteger la confidencialidad, integridad y disponibilidad de la información

institucional, y de mitigar los riesgos asociados a la fuga de datos, la introducción de software malicioso y la pérdida no autorizada de información.

Esta política se encuentra alineada con los principios y buenas prácticas establecidos por la familia de normas ISO/IEC 27000, en particular los controles relacionados con la gestión de medios removibles, la protección de la información y el control de acceso. Sin embargo, el Ministerio no se rige de manera obligatoria ni integral por dicha normativa; los controles aquí descritos se adoptan como referencia técnica y guía de mejores prácticas, ajustados al contexto, recursos y necesidades operativas de la institución.

De manera específica, esta política busca:

- Establecer reglas claras y de cumplimiento obligatorio sobre el uso de dispositivos USB, discos duros externos, memorias SD y microSD, y cualquier otro medio removible de almacenamiento masivo.
- Reducir el riesgo de fuga, copia o transferencia no autorizada de información institucional.
- Prevenir la introducción de malware, ransomware y software no autorizado a través de medios removibles.
- Definir los mecanismos de autorización, registro, control y monitoreo del uso de estos dispositivos.
- Establecer las consecuencias derivadas del incumplimiento de la presente política.

2.9.2 Alcance

Esta política es de observancia obligatoria para todo el personal vinculado con el Ministerio, sin excepción, incluyendo:

- Personal permanente, temporal, por contrato, honorarios o cualquier figura contractual.
- Personal directivo, mandos medios y operativos.
- Personal externo, proveedores, prestadores de servicios profesionales, consultores, becarios y personal en prácticas profesionales que tengan acceso, manejo o tránsito de información institucional.
- Visitantes que, de manera excepcional y autorizada, requieran conectar dispositivos de almacenamiento en infraestructura del Ministerio.

2.9.2.1 Dispositivos comprendidos

La política aplica a todo dispositivo capaz de almacenar, transportar o transferir información digital de forma extraíble, incluyendo de manera enunciativa más no limitativa:

- Memorias USB (pendrives, USB flash drives) en cualquier capacidad e interfaz (USB-A, USB-C, USB 2.0, 3.x, etc.).
- Discos duros externos (HDD y SSD externos), tanto magnéticos como de estado sólido.
- Tarjetas de memoria SD, miniSD, microSD, CompactFlash, Memory Stick y similares, así como sus adaptadores y lectores.
- Dispositivos híbridos con función de almacenamiento masivo (teléfonos móviles, tabletas, cámaras digitales, reproductores multimedia y wearables) cuando se conecten en modo de almacenamiento.
- Cualquier otro medio removible que pueda ser reconocido por los sistemas operativos como unidad de almacenamiento.

2.9.2.2 Entornos y activos cubiertos

La política aplica al uso de los dispositivos antes descritos sobre cualquier activo de información o infraestructura tecnológica propiedad, en arrendamiento o bajo administración del Ministerio, incluyendo equipos de cómputo de escritorio, portátiles, servidores, equipos de impresión, estaciones de trabajo especializadas, equipos de control, kioscos, equipos de videoconferencia y cualquier punto de conexión disponible en las instalaciones.

2.9.2.3 Exclusiones

No se encuentran dentro del alcance de esta política los dispositivos de almacenamiento fijos internos (discos duros internos de servidores y equipos de cómputo), los respaldos gestionados por la DISI conforme al Manual de Resguardo de la Información, ni los servicios de almacenamiento en la nube institucionales, los cuales son regulados por políticas específicas.

2.9.3 Contenido

2.9.3.1 Principios generales

El uso de dispositivos de almacenamiento masivo en el Ministerio se rige por los siguientes principios:

- **Mínimo privilegio:** el acceso al uso de dispositivos removibles se otorga únicamente al personal que lo requiera para el desempeño de sus funciones.
- **Necesidad de conocer:** la información transferida a estos dispositivos se limita a aquella estrictamente necesaria para la actividad autorizada.
- **Trazabilidad:** todo uso autorizado debe quedar registrado de forma que sea posible reconstruir el qué, quién, cuándo y para qué.
- **Protección por defecto:** los dispositivos que contengan información institucional deben encontrarse cifrados y protegidos.
- **Responsabilidad individual:** cada persona usuaria es responsable del uso, custodia y consecuencias derivadas del manejo de los dispositivos autorizados a su cargo.

2.9.3.2 Clasificación de los dispositivos

Para efectos de control, los dispositivos de almacenamiento masivo se clasifican en tres categorías:

Categoría	Descripción	Tratamiento
Institucional	Dispositivo adquirido, asignado y registrado por el Ministerio para uso oficial.	Uso permitido bajo autorización, cifrado obligatorio y registro en inventario.
Personal autorizado	Dispositivo propiedad del personal, autorizado de manera excepcional para fines específicos.	Uso restringido, requiere autorización formal y escaneo previo. No para información clasificada.
No autorizado	Cualquier dispositivo no perteneciente a las dos categorías anteriores.	Uso estrictamente prohibido en infraestructura institucional.

2.9.3.3 Uso permitido

Se considera uso permitido de los dispositivos de almacenamiento masivo únicamente cuando se cumplan todas las siguientes condiciones:

- El dispositivo se encuentra registrado y autorizado por la DISI.
- La persona usuaria cuenta con autorización vigente para utilizar este tipo de medios.

- El propósito de uso está vinculado directamente a funciones laborales legítimas y documentadas.
- El dispositivo cuenta con cifrado de almacenamiento conforme a los estándares definidos por la DISI (por ejemplo, AES-256 o equivalente).
- El dispositivo es sometido a un escaneo antimalware actualizado antes de cualquier transferencia de información.
- La información transferida cumple con la Política de Clasificación y Manejo de la Información (sección 1.3).

2.9.3.4 Uso prohibido

Queda estrictamente prohibido:

- Conectar dispositivos de almacenamiento masivo no autorizados a cualquier equipo o infraestructura del Ministerio.
- Extraer, copiar, transferir o transportar información clasificada como Confidencial o Privada en dispositivos no cifrados o no autorizados.
- Compartir, prestar o ceder a terceros los dispositivos institucionales asignados.
- Utilizar dispositivos de almacenamiento masivo encontrados, regalados, promocionales o de origen desconocido.
- Almacenar información personal no relacionada con las funciones laborales en dispositivos institucionales.
- Almacenar información institucional en dispositivos personales sin la autorización correspondiente.
- Eludir, deshabilitar o manipular los mecanismos de control de puertos USB, cifrado, antimalware o cualquier control técnico implementado por la DISI.
- Utilizar dispositivos de almacenamiento como medio para introducir software no licenciado, malicioso o no autorizado.
- Conservar información institucional en dispositivos personales tras la conclusión del vínculo laboral o contractual.

2.9.3.5 Autorización y registro

El uso de dispositivos de almacenamiento masivo requerirá autorización previa y por escrito conforme al siguiente procedimiento:

- La persona usuaria deberá presentar una solicitud formal ante su jefatura inmediata, justificando la necesidad operativa.

- La jefatura inmediata validará y endosará la solicitud y la remitirá a la DISI.
- La DISI evaluará la solicitud, verificará el cumplimiento de los requisitos técnicos y, en su caso, emitirá la autorización correspondiente.
- El dispositivo autorizado será registrado en el inventario de medios removibles, con identificador único, asignatario, fecha de asignación y propósito.
- La autorización tendrá una vigencia definida y podrá ser revocada en cualquier momento por razones de seguridad o cambio de funciones.

2.9.3.6 Controles técnicos

La DISI implementará y mantendrá los siguientes controles técnicos como parte de esta política:

- Bloqueo predeterminado de puertos USB y lectores de tarjetas en equipos institucionales, habilitándose únicamente mediante autorización.
- Lista blanca de dispositivos autorizados a nivel de sistema operativo o herramienta de control de endpoints (Endpoint Protection / DLP).
- Cifrado obligatorio de los dispositivos institucionales mediante mecanismos como BitLocker, VeraCrypt o equivalentes.
- Escaneo automático antimalware al conectar cualquier dispositivo de almacenamiento masivo.
- Registro y monitoreo (logs) de conexiones, transferencias y eventos relacionados con medios removibles.
- Borrado seguro de los dispositivos antes de su reasignación, baja o disposición final.

2.9.3.7 Custodia, transporte y disposición final

- **Custodia:** los dispositivos asignados deben permanecer bajo resguardo del usuario autorizado, evitando dejarlos desatendidos en áreas de acceso público o sin protección.
- **Transporte:** el traslado fuera de las instalaciones debe realizarse con el cifrado activo y, cuando aplique, mediante medios de transporte y empaque adecuados.
- **Pérdida o robo:** todo extravío, robo o sospecha de compromiso debe ser reportado a la DISI dentro de las 24 horas siguientes al hecho.

- **Disposición final:** los dispositivos en desuso, dañados o al término de su vida útil deberán ser entregados a la DISI para su borrado seguro o destrucción física, conforme a buenas prácticas reconocidas (por ejemplo, NIST SP 800-88 o equivalentes).

2.9.3.8 Responsabilidades

De la Dirección de Sistemas de Información: diseñar, implementar, mantener y actualizar la presente política y sus controles técnicos asociados; llevar el inventario de dispositivos institucionales autorizados; evaluar y emitir las autorizaciones de uso; realizar el monitoreo, auditorías periódicas y atención a incidentes; capacitar y difundir esta política entre el personal.

De las jefaturas y mandos medios: validar la pertinencia de las solicitudes de uso del personal a su cargo; vigilar el cumplimiento de la política dentro de su área; reportar incumplimientos o incidentes detectados.

De las personas usuarias: conocer, comprender y cumplir la presente política; utilizar los dispositivos exclusivamente para los fines autorizados; resguardar los dispositivos asignados y la información contenida en ellos; reportar de manera inmediata cualquier pérdida, robo, sospecha de compromiso o incidente; devolver los dispositivos al concluir el vínculo laboral o cuando así sea requerido.

2.9.4 Revisión y cumplimiento

2.9.4.1 Revisión

La presente política será revisada de manera ordinaria al menos una vez cada doce (12) meses por la DISI, con la finalidad de mantener su vigencia, pertinencia y alineación con el contexto operativo, tecnológico y normativo del Ministerio, así como con las buenas prácticas derivadas de la familia ISO/IEC 27000.

Se realizarán revisiones extraordinarias en cualquiera de los siguientes supuestos:

- Cambios significativos en la infraestructura tecnológica o en los procesos del Ministerio.
- Materialización de incidentes de seguridad relevantes relacionados con medios removibles.
- Actualizaciones relevantes en marcos normativos, regulatorios o estándares de referencia.
- Resultados de auditorías internas o externas que sugieran ajustes a la política.

2.9.4.2 Mecanismos de verificación del cumplimiento

La verificación del cumplimiento se realizará mediante:

- Auditorías periódicas, programadas o no programadas, sobre el uso de medios removibles.
- Revisión de bitácoras y registros generados por las herramientas de control de endpoints y prevención de fuga de información (DLP).
- Inspecciones físicas en sitios y áreas de trabajo.
- Pruebas de cumplimiento como parte de los ejercicios de evaluación de riesgos.
- Revisión y atención de reportes de incidentes.

2.9.4.3 Reporte de incidentes e incumplimientos

Cualquier persona que detecte un posible incumplimiento de la presente política, un uso indebido de dispositivos de almacenamiento masivo o un incidente relacionado, deberá reportarlo de inmediato a través de los canales oficiales establecidos por la DISI. La identidad de la persona que reporte de buena fe será tratada con confidencialidad.

2.9.4.4 Difusión y aceptación

La política será difundida formalmente entre todo el personal y los terceros que se encuentren dentro de su alcance. Toda persona usuaria, al recibir la asignación de equipo de cómputo, dispositivos institucionales o accesos a la infraestructura, deberá manifestar por escrito o por medios electrónicos su conocimiento y aceptación de la presente política.

2.9.5 Sanciones

El incumplimiento de la presente política dará lugar a la aplicación de las medidas correctivas y disciplinarias correspondientes, conforme a la normativa interna del Ministerio y la legislación laboral vigente en Guatemala, sin perjuicio de las responsabilidades administrativas, civiles o penales que en su caso resulten aplicables.

2.9.5.1 Niveles de severidad

Para efectos de aplicación de sanciones, los incumplimientos se clasifican en los siguientes niveles:

Nivel	Tipo de incumplimiento	Medida aplicable (referencial)
Leve	Uso de dispositivo personal sin autorización, sin afectación a la confidencialidad o disponibilidad de la información.	Llamada de atención por escrito, retiro inmediato de la conexión, capacitación obligatoria en seguridad de la información.
Moderado	Almacenamiento de información institucional en dispositivos no autorizados o no cifrados; reincidencia en faltas leves; elusión de controles técnicos.	Amonestación formal con anotación en expediente, revocación temporal o definitiva de la autorización de uso de medios removibles, restricción de privilegios de acceso.
Grave	Fuga, extracción o transferencia no autorizada de información clasificada; introducción intencional de software malicioso; reincidencia en faltas moderadas; encubrimiento de incidentes.	Procedimiento disciplinario conforme a la normativa interna y la legislación laboral vigente en Guatemala, que podrá incluir la separación del cargo, terminación del vínculo laboral o contractual, y denuncia ante las autoridades competentes.

2.9.5.2 Criterios de aplicación

La aplicación de las sanciones considerará, entre otros, los siguientes criterios:

- La gravedad e impacto del incumplimiento sobre la confidencialidad, integridad o disponibilidad de la información.
- La intencionalidad o negligencia de la conducta.
- La reincidencia de la persona usuaria.
- La afectación a terceros, a la imagen institucional o al cumplimiento de obligaciones legales o contractuales.
- La cooperación de la persona involucrada para mitigar el incidente.

2.9.5.3 Procedimiento disciplinario

La aplicación de las medidas previstas se llevará a cabo conforme al procedimiento disciplinario interno del Ministerio, garantizando en todo momento el derecho de audiencia y debido proceso de la persona involucrada. La DISI actuará como instancia técnica y aportará los elementos probatorios derivados de bitácoras, registros y análisis forenses, según corresponda.

Cuando los hechos pudieran configurar responsabilidades legales, se dará vista a las áreas jurídica y de recursos humanos, así como a las autoridades competentes.

2.10 Política de software seguro

2.10.1 Propósito

Garantizar que todo el software utilizado o desarrollado por el Ministerio cumpla con estándares de seguridad que minimicen la existencia de vulnerabilidades. El objetivo es integrar la seguridad en el ciclo de vida del software (SDLC) y no solo como una revisión final.

2.10.2 Alcance

Esta política aplica a:

- Equipos de desarrollo interno (desarrolladores, QA, DevOps).
- Proveedores externos de software y consultorías de desarrollo.
- Procesos de adquisición de software comercial (COTS).

2.10.3 Responsabilidades del usuario (desarrolladores y adquisiciones)

En esta política, los usuarios son perfiles técnicos o de adquisiciones. Sus responsabilidades son:

- **Seguridad desde el diseño:** los desarrolladores deben seguir marcos de trabajo seguros (como OWASP Top 10) para evitar errores comunes como inyección SQL o XSS.
- **Gestión de dependencias:** validar que las librerías de código abierto (open source) estén actualizadas y no tengan vulnerabilidades conocidas antes de integrarlas.
- **Manejo de credenciales:** queda estrictamente prohibido incluir contraseñas, llaves de API o tokens directamente en el código fuente (hardcoding). Se deben usar bóvedas de secretos.

- **Revisiones de seguridad:** todo código debe pasar por una revisión por pares (peer review) y pruebas de seguridad antes de ser desplegado en producción.

2.10.4 Revisión y cumplimiento

Para asegurar que el software sea efectivamente seguro, se establecen los siguientes controles:

Fase del ciclo	Control de seguridad	Responsable
Desarrollo	Análisis de código estático (SAST) para buscar errores de lógica.	Equipo de desarrollo
Pruebas	Pruebas de penetración (pentests) en entornos de preproducción.	Seguridad de la información
Adquisición	Evaluación de seguridad del proveedor y revisión de certificaciones (ISO/IEC 27001, SOC 2).	Compras / DISI
Producción	Parcheo crítico en menos de 24-48 horas tras detectar una vulnerabilidad.	Operaciones de la DISI

GLOSARIO

DI: Documento Interno

Wiping: Es el proceso de eliminar información de un dispositivo de almacenamiento (como discos duros, USB, laptops o servidores) de manera que no pueda ser recuperada, ni siquiera con herramientas especializadas.

IP: Es un identificador único que se asigna a cada dispositivo conectado a una red (como Internet o una red interna), para que pueda comunicarse con otros dispositivos.

Hostname: Es el nombre único que identifica a un dispositivo dentro de una red. Sirve como una forma más fácil de reconocer equipos, en lugar de usar direcciones IP numéricas.

Tabletop exercises: son simulaciones teóricas de situaciones de emergencia o incidentes, en las que los participantes analizan y discuten cómo responderían ante distintos escenarios, sin ejecutar acciones reales en sistemas o infraestructuras.

Superusuarios: son personas que tienen accesos y permisos avanzados dentro de un sistema informático.

Hardcoding: es una práctica de programación en la que se insertan valores fijos directamente dentro del código fuente, en lugar de usar configuraciones externas o variables dinámicas.

GOBIERNO DE LA REPÚBLICA · GUATEMALA

Ministerio de
Trabajo y Previsión Social

Ministerio de Trabajo y Previsión Social

UTZ SAMAJ

Guatemala 23 de junio de 2026
-DISI-OF-611-2026-EOCG/fa

Licenciada
Alma Leticia Maldonado Mérida
Jefa de la Unidad de Planificación y Cooperación
Ministerio de Trabajo y Previsión Social
Presente

Estimada Licenciada Maldonado:

Por este medio traslado el **"Manual de Políticas de la Dirección de Sistemas de Información" -DISI-, versión 1**, se adjunta impreso únicamente en su lado anverso, incorporando las observaciones realizadas por la Unidad de Planificación y Cooperación así como las del Vice Despacho Administrativo financiero, las cuales han sido debidamente atendidas.

Sin otro particular, me suscribo.

CI-UPC-1081-2026
MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE PLANIFICACIÓN Y COOPERACIÓN
RECIBIDO
24 JUN 2026
FIRMA: EDWOM HORA: 14:33
GUATEMALA, C. A.

Atentamente,

Ing. Edwin Omar de la Cruz García
Director de Sistemas de Información
Ministerio de Trabajo y Previsión Social

CC. Archivo
70 Folios
Página 1/1

Ministerio de Trabajo y Previsión Social

UTZ SAMAJ

Guatemala 29 de mayo de 2026
-DISI-OF-534-2026-EPCG/fa

CI-UPC-969-2026
MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE PLANIFICACIÓN Y COOPERACIÓN
RECIBIDO
02 JUN 2026
FIRMA
HORA 12:42
GUATEMALA, C. A.

Licenciada
Alma Leticia Maldonado Mérida
Jefa de la Unidad de Planificación y Cooperación
Ministerio de Trabajo y Previsión Social
Presente

Estimada Licenciada Maldonado:

Por este medio, me permito trasladar el documento **de Políticas de la Dirección de Sistemas de Información -DISI-**, Versión 01, en formato impreso, el cual también será remitido posteriormente por correo electrónico a la dirección upc@mintrabajo.gob.gt.

Sin otro particular, me suscribo atentamente.

Atentamente,

Ing. Edwin Omar de la Cruz García
Director de Sistemas de Información
Ministerio de Trabajo y Previsión Social

C.C. Archivo
C.C. Vice despacho Administrativo Financiero
Anexos. 36 Folios