SysCafé	DECLARACIÓN DE APLICABILIDAD PARA SEGURIDAD DE LA INFORMACIÓN	Fecha de aprobación	8/01/2025
		Versión	02
	Nivel: 3	Pagina	

Fecha Actualización 27/02/2026

División	Subdivisión	Controles de Seguridad de la Información	Aplica	Justificación	Aplicabilidad
		Controles Organizativos			
5.1	Políticas de Seguridad de la Información	Controlar La política de seguridad de la información y las políticas específicas de cada tema deberán ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal y las partes interesadas pertinentes, y revisadas a intervalos planificados y si se producen cambios significativos.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información •Divulgación en inducción y reinducción •Divulgación Intranet •Jornadas de sensibilización
5.2	Funciones de seguridad de la información y responsabilidades	Controlar Las funciones y responsabilidades en materia de seguridad de la información se definirán y asignarán en función de las necesidades de la organización.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GTH-FRT-013 Perfil Ocupacional del Cargo •Reunión de revisión por la dirección.
5.3	Segregación de funciones	Controlar Deberán separarse las funciones y los ámbitos de responsabilidad contradictorios.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GTH-FRT-013 Perfil Ocupacional del Cargo
5.4	Responsabilidades de gestión	Controlar La dirección exigirá a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas específicas de alto nivel y los procedimientos de la organización.	Si	- Se aplica el control, producto del Análisis de Riesgo - Requerimiento del Negocio	•GTH-FRT-013 Perfil Ocupacional del Cargo •Segregación de funciones según roles.
5.5	Contacto con las autoridades	Controlar La organización establecerá y mantendrá contacto con las autoridades pertinentes.	Si	- Se aplica el control, producto del Análisis de Riesgo	•El área de TIC están en constante comunicación con algunos foros y grupos de interés como: CSIRT, Symantec, Segurinfo, CERT, Microsoft, entre otros. • GID-FRT-021 Matriz de Inteligencia de Amenazas.
5.6	Contacto de especial interés grupos	Controlar La organización establecerá y mantendrá contactos con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.	Si	- Se aplica el control, producto del Análisis de Riesgo	•El área de TIC están en constante comunicación con algunos foros y grupos de interés como: CSIRT, Symantec, Segurinfo, CERT, Microsoft, entre otros. • GID-FRT-021 Matriz de Inteligencia de Amenazas.
5.7	Información sobre amenazas	Controlar La información relativa a las amenazas a la seguridad de la información se recopilará y analizará para producir inteligencia sobre amenazas.	Si	- Se aplica el control, producto del Análisis de Riesgo	• GID-FRT-021 Matriz de Inteligencia de Amenazas.
5.8	Seguridad de la información en la gestión de proyectos	Controlar La seguridad de la información se integrará en la gestión del proyecto.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información
5.9	Inventario de la información y otros activos asociados	Controlar Se elaborará y mantendrá un inventario de la información y otros activos asociados, incluidos sus propietarios.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-005 Procedimiento de Administración de la Configuración de Activos IT •Aplicativo GLPI
5.10	Uso aceptable de la información y otros activos asociados	Controlar Se determinarán, documentarán y aplicarán normas de uso aceptable y procedimientos de tratamiento de la información y otros activos asociados.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información (5.5.7, 5.9.3, 5.10.4) •GSI-PRC-007 Procedimiento de control de información y Datos •Formato de Protección de Datos Personales
5.11	Devolución de activos	Controlar El personal y otras partes interesadas, según proceda, devolverán todos los activos de la organización que estén en su posesión al cambiar o finalizar su empleo, contrato o acuerdo.	Si	- Se aplica el control, producto del Análisis de Riesgo Requerimientos del Negocio	•Políticas de Seguridad de la Información •GSI-PRC-010Procedimiento de Soporte y Mantenimiento de Infraestructura •Aplicativo GLPI
5.12	Clasificación de la información	Controlar La información se clasificará en función de las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-001Procedimiento de Identificación de Activos •Manual del Sistema Integrado de gestión •GSI-FRT-014 Inventario de Activos de información
5.13	Etiquetado de la información	Controlar Se desarrollará y aplicará un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el sistema de clasificación de la información adoptado por la organización.	Si	- Se aplica el control, producto del Análisis de Riesgo Requerimientos del Negocio	•GSI-PRC-001Procedimiento de Identificación de Activos •Manual del Sistema Integrado de gestión •GSI-FRT-014 Inventario de Activos de información
5.14	Transferencia de información	Controlar Se establecerán normas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-007 Procedimiento de Control de Información y Datos, que incluye la Política de Intercambio de la información •Acuerdo de Confidencialidad colaboradores y proveedores
5.15	Control de acceso	Controlar Se establecerán y aplicarán normas para controlar el acceso físico y lógico a la información y a otros activos asociados en función de los requisitos de seguridad de la empresa y de la información.	Si	- Se aplica el control, producto del Análisis de Riesgo Requerimientos del Negocio	•GSI-PRC-014 Procedimiento De Control De Acceso Y Seguridad De Redes •GSI-PRC-012 Procedimiento De Control De Seguridad Física Y Acceso •Políticas de Seguridad de la Información •Política de Bien Estar Laboral •Usuario en Directorio activo •Autorizacion accesos a aplicativos por rol (Azure - CRM Licencias)

5.16	Gestión de identidades	Controlar Se gestionará el ciclo de vida completo de las identidades.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-013 Procedimiento de administración de usuarios y contraseñas •Usuario en Directorio Activo •Usuario en Microsoft 365
5.17	Información de autenticación	Controlar La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, que incluirá el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-013 Procedimiento de Administración de usuarios y contraseñas •Revisión periódica de usuarios en aplicativos •Solicitud de accesos mediante caso con autorización de superior.
5.18	Derechos de acceso	Controlar Los derechos de acceso a la información y a otros activos asociados se asignarán, revisarán, modificarán y eliminarán de acuerdo con la política específica de la organización y las normas de control de acceso.	Si	- Se aplica el control, producto del Análisis de Riesgo Requerimientos del Negocio	•GSI-PRC-014 Procedimiento De Control De Acceso Y Seguridad De Redes •GSI-PRC-013 Procedimiento de Administración Usuarios y Contraseñas •Políticas de Seguridad de la Información •Configuración Contraseñas seguras. •Revisión de accesos periodicamente
5.19	Seguridad de la información en las relaciones con los proveedores	Controlar Se definirán y aplicarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados al uso de los productos o servicios del proveedor.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Política de seguridad de la información, 5.16.2 Política de Riesgos asociados a los proveedores críticos •Procedimiento De Compras Y Adquisiciones De Bienes Y Servicios •Contratos con proveedores
5.20	Seguridad de la información en los acuerdos con los proveedores	Controlar Se establecerán y acordarán con cada proveedor los requisitos pertinentes en materia de seguridad de la información en función del tipo de relación con el proveedor.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Política de seguridad de la información, (5.16.2Política de Riesgos asociados a los proveedores críticos) •GAF-PRC-001Procedimiento De Compras Y Adquisiciones De Bienes Y Servicios •Contratos con proveedores
5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y la comunicación (TIC)	Controlar Se definirán y aplicarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Política de seguridad de la información, 5.16.2Política de Riesgos asociados a los proveedores críticos •GAF-PRC-001 Procedimiento De Compras Y Adquisiciones De Bienes Y Servicios •Contratos con proveedores
5.22	Seguimiento, revisión y gestión de cambios de los servicios de los proveedores	Controlar La organización supervisará, revisará, evaluará y gestionará periódicamente los cambios en las prácticas de seguridad de la información y la prestación de servicios de los proveedores.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GAF-PRC-001 Procedimiento De Compras Y Adquisiciones De Bienes Y Servicios •Contratos con proveedores
5.23	Seguridad de la información para el uso de servicios en la nube	Controlar Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se establecerán de acuerdo con los requisitos de seguridad de la información de la organización.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Declaración de Privacidad Microsoft Azure •GSI-FRT-020 Prestación de Servicios Azure-2025
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Controlar La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, funciones y responsabilidades de la gestión de incidentes de seguridad de la información.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-004 Procedimiento De Gestión de Incidentes de Seguridad de la Información • Acta Comité Directivo •Aplicativo GLPI
5.25	Evaluación y decisión sobre incidentes de seguridad interna	Controlar La organización evaluará los sucesos de seguridad de la información y decidirá si deben clasificarse como incidentes de seguridad de la información.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-004 Procedimiento De Gestión de Incidentes de Seguridad de la Información •Aplicativo GLPI
5.26	Respuesta a la seguridad de la información incidentes	Controlar Se responderá a los incidentes de seguridad de la información de conformidad con los procedimientos documentados.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-004 Procedimiento De Gestión de Incidentes de Seguridad de la Información •Aplicativo GLPI
5.27	Aprender de los incidentes de seguridad de la información	Controlar Los conocimientos obtenidos de los incidentes de seguridad de la información se utilizarán para reforzar y mejorar los controles de seguridad de la información.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-004 Procedimiento De Gestión de Incidentes de Seguridad de la Información •Aplicativo GLPI
5.28	Recogida de pruebas	Controlar La organización establecerá y aplicará procedimientos para la identificación, recogida, adquisición y conservación de pruebas relacionadas con sucesos de seguridad de la información.	Si	- Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-004 Procedimiento De Gestión de Incidentes de Seguridad de la Información •Aplicativo GLPI
5.29	Seguridad de la información durante perturbación	Controlar La organización deberá planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Plan de Disponibilidad y Continuidad •GSI-PRC-004 Procedimiento De Gestión de Incidentes de Seguridad de la Información
5.30	Preparación de las TIC para la continuidad empresarial	Controlar La preparación de las TIC se planificará, aplicará, mantendrá y probará en función de los objetivos de continuidad de las actividades y los requisitos de continuidad de las TIC.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Plan de Disponibilidad y Continuidad
5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Controlar Se identificarán, documentarán y mantendrán actualizados los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir estos requisitos.	Si	- Se aplica el control, producto del Análisis de Riesgo - Se aplica el control por Requerimientos Legales	•Matriz Legal
5.32	Derechos de propiedad intelectual	Controlar La organización aplicará los procedimientos adecuados para proteger los derechos de propiedad intelectual.	Si	- Se aplica el control, producto del Análisis de Riesgo - Se aplica el control por Requerimientos Legales	•Registro de derechos de autor del software •Acuerdos de confidencialidad •Contrato de Trabajo
5.33	Protección de documentos	Controlar Los registros se protegerán contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Acuerdos de Confidencialidad •Copias de seguridad redundantes •Archivo central •Servidores (Estructuras de Carpetas)

5.34	Privacidad y protección de la información personal identificable (IPI)	Controlar La organización identificará y cumplirá los requisitos relativos a la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.	Si	- Se aplica el control, producto del Análisis de Riesgo - Se aplica el control por Requerimientos Legales	•Politica de Uso de Datos •Acuerdo de Confidencialidad •Archivo central •Servidores •Copias de Seguridad
5.35	Revisión independiente de la seguridad de la información	Controlar El enfoque de la organización para gestionar la seguridad de la información y su aplicación, incluyendo personas, procesos y tecnologías, se revisarán de forma independiente a intervalos planificados, o cuando se produzcan cambios significativos.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Audiorias Internas •GSI-FRT-019 Hacking Ético
5.36	Cumplimiento de las políticas, reglas y normas de seguridad de la información	Controlar Se revisará periódicamente el cumplimiento de la política de seguridad de la información de la organización, así como de las políticas, reglas y normas específicas de la alta dirección.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Seguimiento Periódico a las políticas •Auditorias •Control de los Procesos •Revisión por la Dirección
5.37	Procedimientos operativos documentados	Controlar Los procedimientos operativos de las instalaciones de tratamiento de la información deberán documentarse y ponerse a disposición del personal que los necesite.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Instituto Virtual SysCafé-Curso SIG •Sitio SIG •Mapa de Operación por Procesos •Procedimientos del SIG
Control de Personas					
6.1	Cribado	Controlar Las comprobaciones de los antecedentes de todos los candidatos a personal se llevarán a cabo antes de su incorporación a la organización y de forma continuada, teniendo en cuenta las leyes, reglamentos y normas éticas aplicables, y serán proporcionales a los requisitos de la empresa, la clasificación de la información a la que se va a acceder y los riesgos percibidos.	Si	- Se aplica el control, producto del Análisis de Riesgo - Se aplica el control por Requerimientos Legales	•GTH-PRC-001 Procedimiento Gestión de Talento Humano. •Política de Contratación •Política de Reclutamiento y Selección
6.2	Condiciones de empleo	Controlar Los acuerdos contractuales de empleo establecerán las responsabilidades del personal y de la organización en materia de seguridad de la información.	Si	- Se aplica el control, producto del Análisis de Riesgo	•Reglamento Interno de Trabajo •Sitio SIG (RIT) •GTH-FRT-013 Perfil Ocupacional del Cargo
6.3	Concienciación, educación y formación en seguridad de la información	Controlar El personal de la organización y las partes interesadas pertinentes recibirán una concienciación, educación y formación adecuadas en materia de seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización y de las políticas y procedimientos específicos de cada tema, según corresponda a su función laboral.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GTH-FRT-013 Perfil Ocupacional del Cargo •Inducción •Reinducción •Instituto Virtual SysCafé- Curso SIG •Plan de Capacitación •Cursos Externos •Cursos Internos
6.4	Proceso disciplinario	Controlar Se formalizará y comunicará un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una infracción de la política de seguridad de la información.	Si	- Se aplica el control, producto del Análisis de Riesgo Requerimientos del Negocio	•Reglamento Interno de Trabajo •Roles y Responsabilidades •Procedimiento Disciplinatio
6.5	Responsabilidades tras el cese o el cambio de empleo	Controlar Las responsabilidades y obligaciones en materia de seguridad de la información que sigan siendo válidas tras el cese o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y a otras partes interesadas.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Contrato de Trabajo •Reglamento Interno de Trabajo
6.6	Acuerdos de confidencialidad o de no divulgación	Controlar Los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización en materia de protección de la información deberán ser identificados, documentados, revisados periódicamente y firmados por el personal y otras partes interesadas pertinentes.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Acuerdo de Confidencialidad
6.7	Trabajo a distancia	Controlar Se aplicarán medidas de seguridad cuando el personal trabaje a distancia para proteger la información a la que se acceda, procese o almacene fuera de los locales de la organización.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información •GTH-PRC-003 Procedimiento de Trabajo en Casa-Teletrabajo •Políticas de Talento Humano •Acuerdo de Confidencialidad •VPN •Máquina Virtual •Aplicativo GLPI
6.8	Gestión de incidentes de seguridad de la información	Controlar La organización proporcionará un mecanismo para que el personal notifique oportunamente los sucesos de seguridad de la información observados o sospechosos a través de los canales adecuados.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-004 Gestión de Incidentes de Seguridad de la Información •Aplicativo GLPI
Controles Fisicos					
7.1	Perímetros de seguridad física	Controlar Se definirán y utilizarán perímetros de seguridad para proteger las zonas que contengan información y otros activos asociados.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Encerramiento de muros •Cámaras CCTV •Sensores de Movimiento •Rejas
7.2	Entrada física	Controlar Las zonas seguras estarán protegidas por controles de entrada y puntos de acceso adecuados.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Video Portero •Área de Recepción •Camaras CCTV
7.3	Seguridad de oficinas, salas e instalaciones	Controlar La seguridad física de las oficinas, salas e instalaciones se diseñará y implementado.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Camaras CCTV •Encerramiento •Puertas de Acceso
7.4	Vigilancia de la seguridad física	Controlar Los locales se vigilarán continuamente para evitar accesos físicos no autorizados.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Camaras CCTV •Seguridad Privada •Sensores de Movimiento •Seguimiento a las cámaras de CCTV

7.5	Protección frente a amenazas físicas y medioambientales	Controlar Se diseñará y aplicará la protección contra amenazas físicas y medioambientales, como catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas para las infraestructuras.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Aire Acondicionado •Canales de Desague •Tanques de Reserva de Agua •Sensor de temperatura •Edificio Sismoresistente
7.6	Trabajar en zonas seguras	Controlar Las medidas de seguridad para trabajar en zonas seguras se diseñarán y implementado.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Infomación (5.17) •GSI-PRC-012 Procedimiento de Control de Seguridad Fisica y Acceso
7.7	Escritorio y pantalla despejados	Controlar Se definirán y aplicarán adecuadamente normas de escritorio claro para papeles y soportes de almacenamiento extraíbles y normas de pantalla clara para las instalaciones de tratamiento de la información.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información (5.5.2) •Política de escritorio y pantalla limpia. •Bloqueo mediante el directorio activo.
7.8	Emplazamiento y protección de los equipos	Controlar El equipo deberá estar situado en un lugar seguro y protegido.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información (5.17) •GSI-PRC-012 Procedimiento de Control de Seguridad Fisica y Acceso •Monitoreo de cámaras •Areas independientes
7.9	Seguridad de los activos fuera de los locales	Controlar Se protegerán los bienes situados fuera de las instalaciones.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información (5.5) •GSI-PRC-010 Procedimiento de Soporte y Mantenimiento de Infraestructura •Retiro de equipos mediante Autorización •Copias de Respaldo
7.10	Medios de almacenamiento	Controlar Los soportes de almacenamiento se gestionarán a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información •GSI-PRC-010 Procedimiento de Soporte y Mantenimiento de Infraestructura
7.11	Servicios de apoyo	Controlar Las instalaciones de procesamiento de la información deberán estar protegidas de los cortes de electricidad y otras interrupciones causadas por fallos en los servicios públicos de apoyo.	Si	-Se aplica el control, producto del Análisis de Riesgo	•UPS Independiente en cada piso •Planta Eléctrica •Varios proveedores ISP y de RadioTelecomunicación
7.12	Seguridad del cableado	Controlar Los cables que transporten energía, datos o servicios de información de apoyo deberán estar protegidos contra interceptaciones, interferencias o daños.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Ductos de Cableado Independiente •La conexión con los equipos activos se realiza con patch cord certificado de fábrica para categoría 6 como lo especifica el estándar ISO/IEC 11801 y la ANSI/TIA 568, en su centro de cableado
7.13	Mantenimiento de los equipos	Controlar Los equipos se mantendrán correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-002 Procedimiento de Soporte Y Mantenimiento De Activos •Aplicativo GLPI •Plan de Mantenimiento Anual •Procedimiento De Compras Y Adquisiciones De Bienes Y Servicios
7.14	Eliminación segura o reutilización de equipos	Controlar Antes de su eliminación o reutilización, se verificarán los equipos que contengan soportes de almacenamiento para asegurarse de que se han eliminado o sobrescrito de forma segura todos los datos confidenciales y el software con licencia.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información (5.6) •GSI-PRC-010 Procedimiento de Soporte y Mantenimiento de Infraestructura
Controles Tecnológicos					
8.1	Dispositivos de punto final de usuario	Controlar Se protegerá la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Servidor de Archivos •Control de Acceso por Roles
8.2	Derechos de acceso privilegiado	Controlar La asignación y el uso de derechos de acceso privilegiados deberán restringirse y gestionarse.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Política de Seguridad de la Información (5.7) •GSI-PRC-013 Procedimeinto de Administración de Usuarios y Contraseñas •Directorio Activo •Control de Accesos a Aplicativos
8.3	Restricción del acceso a la información	Controlar El acceso a la información y a otros activos asociados se restringirá de acuerdo con la política específica establecida en materia de control de acceso.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Política de Seguridad de la Información (5.7) •GSI-PRC-013 Procedimeinto de Administración de Usuarios y Contraseñas •Directorio Activo •Control de Accesos a Aplicativos
8.4	Acceso al código fuente	Controlar Se gestionará adecuadamente el acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Acceso Servidor Independiente •Directorio Activo •GTH-FRT-013 Perfil Ocupacional del Cargo
8.5	Autenticación segura	Controlar Las tecnologías y procedimientos de autenticación segura se aplicarán en función de las restricciones de acceso a la información y de la política específica del tema sobre control de acceso.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-013Procedimiento de Administración de Usuarios y Contraseñas •Directorio Activo •Control de Accesos a Aplicativos
8.6	Gestión de la capacidad	Controlar La utilización de los recursos se supervisará y ajustará en función de las necesidades de capacidad actuales y previstas.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-016 Procedimiento de Gestión de Capacidad •Plan de Capacidad •Aplicativo GLPI
8.7	Protección contra el malware	Controlar La protección contra programas maliciosos deberá aplicarse y apoyarse en una concienciación adecuada de los usuarios.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-008Procedimiento de Prevención Contra Codigos Maliciosos y Moviles •Plan de Capacitación •Firewall
8.8	Gestión de vulnerabilidades técnicas	Controlar Se obtendrá información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se evaluará la exposición de la organización a dichas vulnerabilidades y se tomarán las medidas adecuadas.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Hacking Etico •GSI-FRT-019 - Informe de Prueba de Hacking Ético

8.9	Gestión de la configuración	Controlar Se establecerán, documentarán, aplicarán, supervisarán y revisarán las configuraciones, incluidas las configuraciones de seguridad, del hardware, el software, los servicios y las redes.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-005 Procedimiento de Admininistración de la Configuración IT •Aplicativo GLPI
8.10	Eliminación de información	Controlar La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-010 Procedimiento De Soporte Y Mantenimiento De Infraestructura
8.11	Enmascaramiento de datos	Controlar El enmascaramiento de datos se utilizará de acuerdo con la política temática de la organización sobre control de acceso y otras políticas temáticas relacionadas, así como con los requisitos empresariales, teniendo en cuenta la legislación aplicable.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Politicas de Seguridad De La Informacion •GSI-PRC-007 Procedimiento De Control De Información Y Datos
8.12	Prevención de fugas de datos	Controlar Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-007 Procedimiento De Control De Información Y Datos •Controles de acceso •Control de desarrollo •Control de Versiones •Bloqueo por Directorio Activo
8.13	Copia de seguridad de la información	Controlar Las copias de seguridad de la información, el software y los sistemas se mantendrán y comprobarán periódicamente de acuerdo con la política específica acordada sobre copias de seguridad.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-011 Procedimiento de Copias de Respaldo •Plan de Copias de Seguridad
8.14	Redundancia de las instalaciones de procesamiento de información	Controlar Las instalaciones de procesamiento de la información se implementarán con la redundancia suficiente para cumplir los requisitos de disponibilidad.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-007 Procedimiento de Copias de Respaldo •Plan de Copias de Seguridad •Servidor Externo •Máquina Virtual •Copia de Seguridad Azure
8.15	Registro	Controlar Se producirán, almacenarán, protegerán y analizarán registros que recojan actividades, excepciones, fallos y otros eventos relevantes.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Log de Eventos Servidor •Check List Licencias Servidores •Monitoreo de Red
8.16	Actividades de seguimiento	Controlar Se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se adoptarán las medidas adecuadas para evaluar posibles incidentes relacionados con la seguridad de la información.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-004 Procedimiento de Gestión de incidentes de seguridad de la Información •GSI-PRC-008 Procedimiento contra Códigos Maliciosos y Móviles •Aplicativo GLPI •Monitoreo Infraestructura tecnológica •Firewall
8.17	Sincronización de relojes	Controlar Los relojes de los sistemas de tratamiento de la información utilizados por la organización deberán estar sincronizados con las fuentes horarias aprobadas.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Servidor Horario NTP INM Colombia
8.18	Uso de programas de utilidades privilegiadas	Controlar El uso de programas de utilidades que puedan ser capaces de anular los controles del sistema y de las aplicaciones deberá estar restringido y estrictamente controlado.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad •Por medio del Directorio Activo se controla que no se tengan programas utilitarios privilegiados.
8.19	Instalación de software en sistemas operativos	Controlar Se aplicarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información •Directorio Activo
8.20	Seguridad de las redes	Controlar Las redes y los dispositivos de red deberán estar protegidos, gestionados y controlados para proteger la información de los sistemas y aplicaciones.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-014 Procedimiento de Control de Acceso y Seguridad de Redes •Directorio Activo •VPN •Firewall •Acceso inhalámbrico Controlado
8.21	Seguridad de los servicios de red	Controlar Se determinarán, aplicarán y supervisarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Políticas de Seguridad de la Información •GSI-PRC-014 Procedimiento de Control de Acceso y Seguridad de Redes •Recursos tecnológicos (Uso aceptable de los activos) •Acceso Inhalámbrico Controlado
8.22	Segregación de redes	Controlar Los grupos de servicios de información, usuarios y sistemas de información deberán estar segregados en las redes de la organización.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-014 Procedimiento de Control de Acceso y Seguridad de Redes •Políticas de seguridad de la Información •Acceso Inalámbrico Controlado
8.23	Filtrado web	Controlar El acceso a sitios web externos se gestionará para reducir la exposición a contenidos maliciosos.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Firewall
8.24	Uso de la criptografía	Controlar Se definirán y aplicarán normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.	Si	- Se aplica el control, producto del Análisis de Riesgo - Se aplica el control por Requerimientos Legales	•Política de Seguridad de la Información (5,11,1) •GSI-PRC-007 Procedimiento de Control de Informacion y Datos
8.25	Ciclo de vida del desarrollo seguro	Controlar Se establecerán y aplicarán normas para el desarrollo seguro de software y sistemas.	Si	-Se aplica el control, producto del Análisis de Riesgo	•DDS-PRC-001 Procedimiento de Gestión de Desarrollo •Políticas de Desarrollo
8.26	Requisitos de seguridad de las aplicaciones	Controlar Los requisitos de seguridad de la información se identificarán, especificarán y aprobarán cuando se desarrollen o adquieran aplicaciones.	Si	-Se aplica el control, producto del Análisis de Riesgo	•DDS-PRC-001 Procedimiento de Gestión de Desarrollo •Políticas de desarrollo

8.27	Arquitectura de sistemas seguros y principios de ingeniería	Controlar Se establecerán, documentarán, mantendrán y aplicarán principios de ingeniería de sistemas seguros a todas las actividades de desarrollo de sistemas de información.	Si	-Se aplica el control, producto del Análisis de Riesgo	•DDS-PRC-001 Procedimiento de Gestión de Desarrollo •Políticas de desarrollo •Visual Fox Pro
8.28	Codificación segura	Controlar Se aplicarán principios de codificación segura al desarrollo de software.	Si	-Se aplica el control, producto del Análisis de Riesgo	•DDS-PRC-001 Procedimiento de Gestión de Desarrollo; procedimiento que incluye las políticas de desarrollo
8.29	Pruebas de seguridad en el desarrollo y la aceptación	Controlar Los procesos de pruebas de seguridad se definirán y aplicarán en el ciclo de vida del desarrollo.	Si	-Se aplica el control, producto del Análisis de Riesgo	•DDS-PRC-001 Procedimiento de Gestión de Desarrollo
8.30	Desarrollo externalizado	Controlar La organización debe dirigir, supervisar y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.	No	Todos los desarrollos de Software son InHouse, no se cuenta con un desarrollador Externo	
8.31	Separación de los entornos de desarrollo, prueba y producción	Controlar Los entornos de desarrollo, pruebas y producción deben estar separados y protegidos.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Fuentes individuales: Fuente Producción, Fuente Beta y Fuente Dev
8.32	Gestión del cambio	Controlar Los cambios en las instalaciones de tratamiento de la información y en los sistemas de información estarán sujetos a procedimientos de gestión de cambios.	Si	-Se aplica el control, producto del Análisis de Riesgo	•GSI-PRC-006 Procedimiento de Gestión del Cambio de TI •DDS-PRC-002 Procedimiento de Gestión de cambios versiones e implementaciones •Aplicativo GLPI •CRM Licencias
8.33	Información de la prueba	Controlar La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Canales de Comunicación •Aplicativo GLPI •CRM Licencias
8.34	Protección de los sistemas de información durante las pruebas de auditoría	Controlar Las pruebas de auditoría y otras actividades de garantía que impliquen la evaluación de los sistemas operativos se planificarán y acordarán entre la persona encargada de las pruebas y la dirección correspondiente.	Si	-Se aplica el control, producto del Análisis de Riesgo	•Canales de Comunicación •Aplicativo GLPI •Planificación en un entorno seguro