



Elaboró: CST
Fecha emisión: Marzo 2017
Última revisión: octubre 2025
Versión: 05
Código: MAP SIS 001

MAPA DE PROCESO DE SISTEMAS

La impresión en papel de este DOCUMENTO, o su consulta en cualquier otro medio diferente a Intranet, no es válida como documento oficial de nuestra Organización. Por lo que su uso es responsabilidad de la persona que lo imprima o consulte.

INDICADOR DEL PROCESO:		OBJETIVO DEL PROCESO:	EQUIPO E INFRAESTRUCTURA DEL PROCESO		
			Hardware	Software	Mobiliario
Nombre	1. Cumplimiento de los SLA. 2. Incidentes Críticos Reportados por el Usuario. 3. Cumplimiento del PMP.	Administrar software y hardware de la Organización para la buena prestación de nuestros servicios.	Equipo de cómputo. Servidores. Conmutador PBX. Switch. Firewall. Alarmas. Sistema de Video Vigilancia. Multifuncionales. Equipos celulares. Diademas. Teléfono. Checador biométrico. No Breaks. Proyectores. Monitores.	Correo electrónico. Office. BlueMessaging. Bonsaif. SICOB. Opti-risks. Internet. ERP. Windows. McAfee. Checador Biométrico. Conmutador PBX. CIA-Desk.	Escritorios. Sillas. Rack y charolas. Archiveros. Botes de Basura.
Monitoreo	1. Mensual. 2. Mensual. 3. Mensual.	ALCANCE DEL PROCESO:	Consumible	Otro	Herramientas
		El presente Mapa de Proceso aplica a todo el personal de Sistemas que va desde la planificación, administración de usuarios y contraseñas, mantenimiento preventivo, sistema de Tickets, infraestructura hasta la medición, análisis y mejora.	Tóner. Artículos de papelería. Espumas. Plugs. Jack's. Chips.	Cable de red y de teléfono.	Pinzas. Ponchadoras RJ45. Desarmadores. Cinta de aislar. Cautín. Pelador de Cable. Aspiradora. Martillo. Dados Milimetricos.
Meta	1. Cumplir con los tiempos del SLA. 2. No tener ninguna incidencia que ponga en riesgo la confidencialidad, disponibilidad e integridad de la información. 3. Cumplir al 100% el Programa de Mantenimiento.	DOCUMENTOS DE REFERENCIA:	PERSONAL INVOLUCRADO:		
		Ley Federal de Protección de Datos Personales en Posesión de Particulares. UNE EN ISO IEC 27001:2013. UNE EN ISO IEC 27001:2022. Procedimiento de sistemas PRO SIS 001. Políticas generales de seguridad de la información POL GSI 001. Procedimiento de Gestión de activos, clasificación y control de la información PRO GSI 015. Procedimiento de Control de accesos PRO GSI 016. Procedimiento de Continuidad de la seguridad de la información PRO GSI 019. Procedimiento de Gestión de incidentes PRO GSI 020. Procedimiento de Respalos y eliminación de información PRO GSI 032. Procedimiento de Operativo para las TIC PRO GSI 039. Procedimiento de Desarrollo seguro PRO GSI 046. Procedimiento de Plan de Recuperación de Desastres PRO GSI 100. Manual del Sistema de Gestión de Seguridad de la Información MAN GSI 001. Procedimiento para el Tratamiento de Riesgos y Oportunidades del SGC y SGSI PRO CAL 009.	Coordinador de Sistemas TI, Auxiliar de Sistemas, Desarrollador, Coordinador de Sistemas de Gestión, Gerente Administrativo, Dirección General.		

REQUISITOS DE ENTRADA			ELABORACIÓN DEL PROCESO		REQUISITOS DE SALIDA	
PROVEEDOR (ES)		INSUMOS DE ENTREGA	ACTIVIDAD(ES) REALIZADA(S)	PRODUCTO FINAL	REQUISITO (S) DEL PRODUCTO	CLIENTE (S)
Interacciones	1. Recursos Humanos	1. Administración del personal.	El proceso de Sistemas utiliza todos los insumos entregados por los procesos antes mencionados para administrar cada una de las etapas de las establecidas en este mismo mapa.	Software y hardware con funcionamiento óptimo para desarrollar la operación.	Software y hardware con funcionamiento óptimo para desarrollar la operación.	Todo el personal
	2. Compras	2. Insumos necesarios para la operación.				
	3. Procesos operativos	3. Tickets.				
	4. Contabilidad y tesorería	4. Pagos, nómina.				
Software y hardware	Dirección General	Necesidad de descargar, instalar y actualizar los software y hardware.	El personal de Sistemas realiza las actividades necesarias para descargar, instalar y actualizar los software y/o hardware de acuerdo al procedimiento de Sistemas PRO SIS 001 .	Software y hardware con funcionamiento óptimo para desarrollar la operación.	Software y hardware con funcionamiento óptimo para desarrollar la operación.	Todo el personal
	Gerente Administrativo					
Monitoreos y Recertificación de Accesos	Dirección General	Necesidad de monitoreo y recertificación de accesos.	El personal de Sistemas realiza el monitoreo y corroboración del control de accesos de acuerdo al procedimiento de Sistemas PRO SIS 001 .	Control y supervisión de los accesos.	Correcto manejo y control de accesos.	Todo el personal
	Gerente Administrativo					
Mantenimiento preventivo	Dirección General	Necesidad de mantenimiento a los equipos e instalaciones.	El personal de Sistemas realiza el plan de mantenimiento y el mantenimiento a los equipos y servidores de acuerdo al procedimiento de Sistemas PRO SIS 001 .	Mantenimiento a los equipos y servidores.	Correcto funcionamiento de los equipos y servidores de la organización.	Todo el personal
Sistema de Tickets	Usuario/ Encargado de área	Necesidad de solicitar: mantenimiento correctivo, asignación de privilegios, generar reporte o carga de bases de procesos operativos.	1. Coordinador de Sistemas TI / Auxiliar de Sistemas recibe la notificación por medio de CIA-Desk, del usuario / Encargado de área, solicitando: mantenimiento correctivo.	1 y 2. Ticket	1 y 2. Ticket cerrado eficazmente	Usuario/ Encargado de área
			2. Coordinador de Sistemas TI / Auxiliar de Sistemas clasifican por prioridades, solicita autorizaciones (de Dirección o Gerente Administrativo) cuando aplique, actualiza estatus y da seguimiento hasta su cierre en CIA-Desk, de acuerdo al procedimiento de Sistemas PRO SIS 001 .			
Gestión de activos y clasificación y control de información	Dirección General	Necesidad de gestionar los activos de la información, la responsabilidad sobre los activos, así como la clasificación y etiquetado de la información.	El personal de Sistemas gestiona los activos de la información, clasifica y etiqueta de la información, de acuerdo al procedimiento de gestión de activos y clasificación y control de información PRO GSI 015 .	1. Activos clasificados. 2. Información clasificada y etiquetada.	1. Activos controlados 2. Información controlada, clasificada y etiquetada.	Dirección General
	Gerente Administrativo					

	PROVEEDOR (ES)	INSUMOS DE ENTREGA	ACTIVIDAD(ES) REALIZADA(S)	PRODUCTO FINAL	REQUISITO (S) DEL PRODUCTO	CLIENTE (S)
Control de accesos	Personal de Recursos Humanos Gerentes o jefes de área	Necesidad de dar de alta o modificar los privilegios al personal.	El personal de sistemas recibe del personal de Recursos Humanos o Gerentes o Jefes de área para solicitar la asignación a un personal de nuevo ingreso o actualizar los privilegios del personal. El personal de sistemas realiza la asignación de los accesos de acuerdo al procedimiento de Control de accesos PRO GSI 016 .	Asignación de accesos.	Asignación de accesos, autorizados y monitoreados.	Todo el personal
Respaldos y eliminación de información	Clientes Dirección General	Necesidad de respaldar y eliminar información.	El personal de sistemas realiza el respaldo y eliminación de la información de acuerdo al procedimiento de continuidad de la información PRO GSI 019 y al procedimiento de respaldos y eliminación de información PRO GSI 032 .	Información respaldada o eliminada.	Información correctamente respaldada o eliminada, de acuerdo a lo solicitado por el cliente.	Clientes
Simulacros	Dirección General	Fechas de simulacro.	El personal de Sistemas o brigadistas realizan los simulacros establecidos, de acuerdo al procedimiento de continuidad de la información PRO GSI 019 para simulacros de sistemas o el procedimiento de Plan de protección civil CIA PRO DIR 001 .	Realizan de simulacros y plan de acción FOR CAL 002 , cuando se requiera.	Simulacro, de acuerdo a lo planificado y plan de acción FOR CAL 002 , cuando se requiera.	Todo el personal
Incidentes	Todo el personal	Reporte o incidentes.	Cuando cualquier personal de la organización reporte un incidente de seguridad, el personal de sistemas actuará de acuerdo al procedimiento gestión de incidentes PRO GSI 020 . Cuando cualquier personal de la organización reporte un incidente referente a desastre natural, el personal de sistemas actuará de acuerdo al procedimiento de plan de recuperación de desastres PRO GSI 100 .	Contención del incidente.	Accidente contenido y plan de acción FOR CAL 002 , cuando se requiera.	Todo el personal
Cumplimiento Legal	Gerente Administrativo Coordinador de Sistemas TI	Necesidad de cumplir obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.	Cuando se establezcan nuevas obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información, el personal de sistemas cumplirá de acuerdo al procedimiento de Cumplimiento Legal PRO GSI 029 .	Adecuaciones al sistema para el cumplimiento legal.	Adecuaciones al sistema para el cumplimiento legal.	Todo el personal
Proveedores	Clientes	Necesidad de protección de los activos de la Organización.	Cuando algún activo sea accesible a los proveedores, el personal de sistemas realizará las acciones descritas en el procedimiento de Proveedores PRO GSI 030 , para proteger su integridad y confidencialidad.	Activos de la Organización protegidos.	Activos de la Organización protegidos.	Dirección General
Desarrollo	Todo el personal	Necesidad de desarrollo de aplicaciones.	Cuando se requiera el desarrollo de nuevas aplicaciones, el desarrollador, realizará las actividades descritas en el procedimiento Desarrollo seguro PRO GSI 046 .	Desarrollo seguro de las aplicaciones.	Aplicaciones seguras y funcionales para la organización.	Todo el personal

PROVEEDOR (ES)		INSUMOS DE ENTREGA	ACTIVIDAD(ES) REALIZADA(S)	PRODUCTO FINAL	REQUISITO (S) DEL PRODUCTO	CUENTE (S)
Medición, análisis y mejora	Dirección	Resultados de indicadores, acciones correctivas y mejora continua.	1. Gerente Administrativo realiza el cálculo de los indicadores de desempeño FOR CAL 003 y envía por medio de correo electrónico al coordinador de Sistemas de Gestión para su publicación en el SGC.	1. Indicadores de desempeño FOR CAL 003 . 2 y 3. Plan de acción FOR CAL 002 o FOR CAL 003 . Plan de cambios y mejoras FOR CAL 011 .	1. Indicadores de desempeño FOR CAL 003 con cálculos vigentes, acciones correctivas cuando se requieran y entregados en tiempo y forma. 2 y 3. Plan de acción FOR CAL 002 debidamente requisitados con seguimientos hasta su cierre. Plan de cambios y mejoras FOR CAL 011 debidamente requisitado y con seguimientos hasta su cierre.	Todo el personal
	Gerente Administrativo		2. Coordinador de Sistemas TI analiza los resultados de indicadores en caso de no cumplir por 3 periodos consecutivos se realiza un plan de acción en el formato indicadores de desempeño FOR CAL 003, para los resultados de encuesta de satisfacción y cuando se requiera genera un plan de acción se debiera realizar en FOR CAL 002 o Plan de cambios y mejoras FOR CAL 011 , según aplique. 3. Coordinador de Sistemas TI / Gerente Administrativo dará seguimiento a las acciones generadas o mejoras.			

Consideraciones de Seguridad de la Información			
Información referida en este documento	Tipo de información	Medio	Personal que puede tener acceso a la información
Documentación referente al Sistema de Gestión de Seguridad de la Información.	Interna	Físico / Electrónico	Solo el personal que esté indicado en el presente mapa de proceso.
Documentación e información de accesos a zonas restringidas.	Restringida	Físico	Solo el personal que esté indicado en el presente mapa de proceso.
Contratos proveedores.	Restringida	Físico / Electrónico	Solo el personal que esté indicado en el presente mapa de proceso.
Documentos controlados por códigos, registros con información de cliente / proveedores / colaboradores, bases de datos.	Restringida	Físico / Electrónico	Solo el personal que esté indicado en el presente mapa de proceso.
Información verbal que se tenga que transmitir para la prestación del proceso.	Restringida	Directo o vía telefónica	Solo el personal que esté indicado en el presente mapa de proceso.
Información consultada o descargada del SGC, SGSI y cualquier información que se genere, pero que no contenga información crítica.	Interna	Físico / Electrónico	Todo el personal de la Organización.
Toda la documentación referida en este documento queda restringida solo a uso del personal de este proceso y si se hiciera mal uso de la misma se aplicarán las sanciones correspondientes.			