centria	ANEXO **Objetivos de Seguridad de la Información**	Código: DOC-SI-01-01 Versión: 08 Fecha de Vigencia: 14/02/2027

I. OBJETIVO

Determinar los obietivos del Sistema de Gestión de Seeuridad de la información (SGSI) de CENTRIA (en adelante **LA EMPRESA**).

II. ALCANCE

El presente documento es de aplicación a **LA EMPRESA**

III. ROLES Y RESPONSABILIDADES

-GERENTE DE SEGURIDAD DE LA INFORMACION:

Garantizar la definición, difusión y mantener actualizado los obietivos de seeuridad de la información, así como aseeurar su cumplimiento.

IV. DEFINICIONES

Sistema de Gestión de Seeuridad de la Información:

Conocido también por sus siglas SGSI, es un conunto de políticas, procedimientos y lineamientos iunto a los recursos y actividades asociados que son oestionados colectivamente oor una oroanización, en la búsqueda de proteoer la confidencialidad, inteoridad y disoonibilidad de sus activos de información.

V. DESCRIPCIÓN

Objetivo Estratégico	Política General de Seguridad de la Información	Objetivos de Seguridad de la Información	Proceso	Código del Indicador	Nombre del Indicador	Objetivo del indicador	Formula de Cálculo	Semaforización			Recursos necesarios	Frecuencia de Medición	Responsable de Medición	Frecuencia del Reporte	Responsable del Reporte	Toma de Acción según resultado del Indicador		
								Rojo	Amarillo	Verde						Rojo	Amarillo	Verde
Ser el COE (Center of Excellence) en Ciberseguridad	Cumplir con los requisitos aplicables en seguridad de la información	Verificar el cumplimiento de los requisitos aplicables al SGSI.	Seguridad de la Información	IND_SGSI_01	% de acciones de tratamiento con cerrado eficaz derivadas de la auditoría interna/externa	Medir el grado de cierre eficaz de las acciones de tratamiento respecto a la auditoría interna/externa	(Cantidad de acciones de tratamiento con cerrado eficaz derivadas de la auditoría interna/externa /Cantidad total de acciones de tratamiento derivadas de la auditoría interna/externa)*100 Nota: El cálculo se realiza en base a las acciones de tratamiento planificadas.	[0% - 80%>	[80% - 90%>	[90% - 100%]	1. Informe de Auditoría Interna/Externa 2. Personal CENTRIA que participa de auditorías internas/externas. 3. Presupuesto para la contratación de servicios de auditorías externas	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	*Escalar a Gerencia General para el refuerzo.	*Escalar a Gerencia de Área/Jefatura responsable del tratamiento	* Continuar con el monitoreo establecido.
				IND_SGSI_02	% de acciones de tratamiento con cerrado eficaz derivadas de la inspección de cumplimiento de seguridad de la información.	Medir el grado de cierre eficaz de las acciones de tratamiento respecto a las inspecciones de cumplimiento de seguridad de la información	(Cantidad de acciones de tratamiento con cerrado eficaz derivadas de inspecciones de cumplimiento de seguridad de la información /Cantidad total de acciones de tratamiento derivadas de la inspección de cumplimiento de seguridad de la información)*100 Nota: El cálculo se realiza en base a las acciones de tratamiento planificadas.	[0% - 80%>	[80% - 90%>	[90% - 100%]	1. Informe de Inspeccion de Cumplimiento 2. Personal del área de Gobierno y Riesgos de Seguridad. 3. Personal de áreas inspeccionadas	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	*Escalar a Gerencia General para el refuerzo.	*Escalar a Gerencia de Área/Jefatura responsable del tratamiento	* Continuar con el monitoreo establecido.
	Promover la adopción de una cultura en seguridad de la información que prevenga la ocurrencia o mitigue el impacto de situaciones que atenten contra la confidencialidad, integridad y disponibilidad de la información.	Fortalecer la cultura de seguridad de la información través de actividades de concientización y capacitación en ciberseguridad.	Gestión de Seguridad de la Información	IND_SGSI_03	% de Colaboradores que han completado el entrenamiento definido en el Portal de Concientización y Capacitación en Ciberseguridad (CyberSense)	Medir el nivel de cumplimiento del entrenamiento desplegado a través del Portal de Concientización y Capacitación en Ciberseguridad (CyberSense)	(Cantidad de Colaboradores que completaron el entrenamiento / Cantidad de colaboradores a quienes se les desplegó el entrenamiento) Nota: Solo entra en cálculo de indicador el contenido obligatorio.	[0% - 80%>	[80% - 90%>	[90% - 100%]	1. Portal de Concientización y Capacitación en Ciberseguridad (CyberSense) 2. Programa de Concientiacion en Ciberseguridad 3. Presupuesto para contratar el Portal de Concientización y Capacitación en Ciberseguridad (CyberSense). 4. Personal del área de Gobierno y Riesgos de Seguridad.	Quincenal durante la vigencia del contenido de entrenamiento	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	Al término del contenido de entrenamiento	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	* Requiere intervención, se debe conducir un análisis de causalidad para determinar las razones de no cumplimiento. * Comunicar los resultados (Jefes Directos, Gerentes de Área y al área de Talento) e incentivar la participación. * Reforzar apoyo con Gerentes de Área y Gerente General.	* El indicador debe ser vigilado de cerca debido a posibles desplazamientos al Rojo. * Comunicar los resultados (Jefes Directos, Gerentes de Área y al área de Talento) e incentivar la participación. * Reforzar apoyo con Gerentes de Área y Jefes directos.	* Comunicar los resultados a Jefes Directos, Gerentes de Área y al área de Talento
				IND_SGSI_04	% de Colaboradores que cayeron en la prueba de Ingeniería Social.	Medir el grado de vulnerabilidad de la unidad de negocio ante ciberataques de ingeniería social.	(Cantidad de Colaboradores de que cayeron en la prueba de Ingeniería Social/Cantidad de Colaboradores que formaron parte de la prueba de Ingeniería Social)*100	[100% - 35%>	[35%-5%>	[0%-5%]	1. Portal de Concientización y Capacitación en Ciberseguridad (CyberSense) 2. Programa de Concientiacion en Seguridad de la Informacion 3. Presupuesto para contratar el Portal de Concientización y Capacitación en Ciberseguridad (CyberSense). 4. Personal del área de Gobierno y Riesgos de Seguridad.	Al término de la prueba de ingeniería social	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	Al término de la prueba de ingeniería social	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	* Requiere intervención, se debe conducir un análisis de causalidad para determinar las razones y aplicar un plan de remediación. * Reforzar con un contenido a los Colaboradores que han caído en la prueba de ingeniería social. * Refuerzo de Comité Ejecutivo de Seguridad de la Información. * Comunicar los resultados a Jefes Directos y Gerentes de Área y al área de Talento	* El indicador debe ser vigilado de cerca debido a posibles desplazamientos al Rojo. * Reforzar con un contenido a los Colaboradores que han caído en la prueba de ingeniería social. * Comunicar los resultados a Jefes Directos y Gerentes de Área y al área de Talento.	* Subir la complejidad de la prueba de ingeniería social. * Comunicar los resultados a Jefes Directos y Gerentes de Área y al área de Talento
		Reducir los incidentes de seguridad de la información mediante su tratamiento oportuno.	Gestión de Seguridad de la Información	IND_SGSI_05	% de incidentes de seguridad de información en estado cerrado en el mes anterior	Medir la eficacia en la atención de los incidentes de seguridad de la información reportados.	(Cantidad de incidentes de seguridad de la información en estado cerrado en el mes anterior/Cantidad total de incidentes de seguridad de la información reportados en el mes)*100	[0% - 80%>	[80% - 90%>	[90% - 100%]	1. Portal de Mesa de Servicios (ServiceNow) 2. Personal del proceso de Seguridad de la Informacion.	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	*Escalar al Gerente de Seguridad de la Información.	*Escalar a Líder de área de Seguridad de la Información	* Continuar con el monitoreo establecido.
	Mejorar continuamente nuestro SGSI, evaluando permanentemente su desempeño.	Mejorar el desempeño del Sistema de Gestión de Seguridad de la Información (SGSI)	Gestión de Seguridad de la Información	IND_SGSI_06	% de acciones de tratamiento con cerrado eficaz respecto a los hallazgos detectados	Medir el grado de cierre eficaz de las acciones de tratamiento respecto a los hallazgos detectados.	(Cantidad de acciones de tratamiento con cierre eficaz respecto a los hallazgos detectados/Cantidad total de acciones de tratamiento respecto a los hallazgos detectados)*100	[0% - 80%>	[80% - 90%>	[90% - 100%]	1. Registro de Acciones Correctivas y Preventivas 2. Personal resolutor de acciones de tratamiento. 3. Personal del área de Gobierno y Riesgos de Seguridad.	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	*Escalar a Gerencia General para el refuerzo.	*Escalar a Gerencia de Área/Jefatura responsable del tratamiento	* Continuar con el monitoreo establecido.
				IND_SGSI_07	% de acciones de tratamiento con cerrado eficaz para tratar riesgos del nivel no tolerable de la gestión de riesgos (de procesos)	Medir la eficacia de las acciones de tratamiento para tratar los riesgos del nivel no tolerable de la gestión de riesgos (de procesos).	(Cantidad de Acciones de tratamiento con cerrado eficaz/ Total de acciones de tratamiento con cierre planificado)*100 Nota: El cálculo se realiza en base a las acciones de tratamiento planificadas.	[0% - 80%>	[80% - 90%>	[90% - 100%]	1. Matriz de Gestión de Riesgos (de procesos) 2. Personal resolutor de acciones de tratamiento. 3. Owners de procesos de negocio CENTRIA 4. Personal del área de Gobierno y Riesgos de Seguridad.	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	Mensual	Jefe de Gobierno y Riesgos de Seguridad (CENTRIA) o quien designe	*Escalar a Gerencia General para el refuerzo.	*Escalar a Gerencia de Área/Jefatura responsable del tratamiento	* Continuar con el monitoreo establecido.