Centro de Especializaciones Noeder

Diploma de Especialización Internacional

IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

MÓDULO II

IMPLEMENTACIÓN DE LA NORMA ISO 27001

CLASE 02

Mg. Ing. Julio Pereyra Rosales

1. Planificación del sistema de gestión

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades

PROBABILIDAD DE OCURRENCIA	
VALOR	FRECUENCIA
5	Muy Frecuente
4	Frecuente
3	Normal
2	Poco Frecuente
1	Raramente

IMPACTO			
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL IMPACTO

IMPACTO

Extremo	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
		1	2	3	4	5
		Raramente	Poco Frecuente	Normal	Frecuente	Muy Frecuente

PROBABILIDAD

CRITERIO DE ACEPTACIÓN DEL RIESGO		
NIVEL	RANGO	DESCRIPCIÓN
ALTO	[15 – 25]	Riesgo no aceptable
MEDIO	[9 – 12]	Riesgo no aceptable
BAJO	[1 – 8]	Riesgo aceptable

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
						IMPACTO							CRITERIOS DE EVALUACIÓN				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	[C]	[I]	[D]	VALOR DEL IMPACTO	RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	FINANCIERO	OPERATIVO	LEGAL	IMAGEN	PRIORIDAD
Base de Datos BDPRD11G, BDPRD11G2, BDPRD11G3, BDPRD11G4, etc	DATOS E INFORMACIÓN	AME001	ACCESO LOGICO NO AUTORIZADO	Incumplimiento de permisos, privilegios y control de acceso / No se tiene sistema de bloqueo de ataques	3	5	4	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	4	3	3	14
	DATOS E INFORMACIÓN	AME002	ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN	SQL Injection	3		5		5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	4	3	3	14
	DATOS E INFORMACIÓN	AME003	DIVULGACION DE INFORMACION	El personal no tiene claro la función de la gestión de la seguridad de la información	3	5			5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	4	14
	DATOS E INFORMACIÓN	AME004	ERRORES DEL ADMINISTRADOR DEL EQUIPO O SISTEMA	Procedimientos de operación no documentados	4	4	4	5	5	20	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	7
	DATOS E INFORMACIÓN	AME005	MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	Políticas de Seguridad	3		5		5	15	ALTO	Jefe de la Oficina de	NO	2	3	3	3	22

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
						IMPACTO							CRITERIOS DE EVALUACIÓN				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	[C]	[I]	[D]	VALOR DEL IMPACTO	RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	FINANCIERO	OPERATIVO	LEGAL	IMAGEN	PRIORIDAD
Servidores físicos y Appliance	HARDWARE	AME017	FALLA DEL FUNCIONAMIENTO DEL HARDWARE	Antigüedad del Equipo / Mantenimientos No Son Planificados	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	46
	HARDWARE	AME018	ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE)	Temperatura y Humedad no controlados	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	1	2	3	2	46
	HARDWARE	AME019	ACCESO FISICO NO AUTORIZADO	Acceso Físico no controlado / No se tienen controles para la seguridad física	3	4	3		4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	61
	HARDWARE	AME020	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS (SATURACIÓN)	Errores de gestión de recursos	4			5	5	20	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	3	7
	HARDWARE	AME021	ABUSO DE PRIVILEGIOS DE ACCESO	Incumplimiento de permisos, privilegios y control de acceso	3	4	3	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	37
	HARDWARE	AME022	VIBRACIONES, POLVO, SUCIEDAD,...	Falta de Mantenimiento Preventivo / No se tienen mecanismos para evitar los	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	46

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME002	Mitigar	Se realizan pruebas de ética hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada	12.6.1 Gestión de las vulnerabilidades técnicas	Pd	Pv	At	65%	Jefe de Producción	Abr-24	Ago-24	BAJO	SI	CERRADO
AME003	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto, así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-24	Ago-24	BAJO	SI	CERRADO
AME004	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-24	Ago-24	BAJO	SI	CERRADO
AME005	Mitigar	Se elaborará la Política de seguridad de la información y será difundida al personal por diversos medios (Correo, capacitaciones, murales, etc.)	5.1.1 Política de seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-24	Ago-24	BAJO	SI	CERRADO
AME006	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto, así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-24	Ago-24	BAJO	SI	CERRADO

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME007	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-24	Ago-24	BAJO	SI	CERRADO
AME008	Mitigar	Se elaborará la Política de seguridad de la información y será difundida al personal por diversos medios (Correo, capacitaciones, murales, etc.)	5.1.1 Política de seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-24	Ago-24	BAJO	SI	CERRADO
AME009	Mitigar	Se elaborará la Política de seguridad de la información y será difundida al personal por diversos medios (Correo, capacitaciones, murales, etc.)	5.1.1 Política de seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-24	Ago-24	BAJO	SI	CERRADO
AME010	Mitigar	Programar y ejecutar los mantenimientos preventivos (anual)	A.11.2.4 Mantenimiento del equipamiento	Pd	Pv	Sa	65%	Coordinador de Centro de Datos	Abr-24	Ago-24	BAJO	SI	CERRADO
AME011	Mitigar	Se llevará un control de ingreso a las instalaciones del data center. Los operadores acompañaran a las visitantes durante su permanencia en las instalaciones El ingreso será con anticipación al data center mínimo de 4 días. El acceso al data center cuenta con los siguientes controles: 1. Puerta eléctrica con tarjetas de proximidad. 2. Cámaras de videovigilancias.	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-24	Ago-24	BAJO	SI	CERRADO

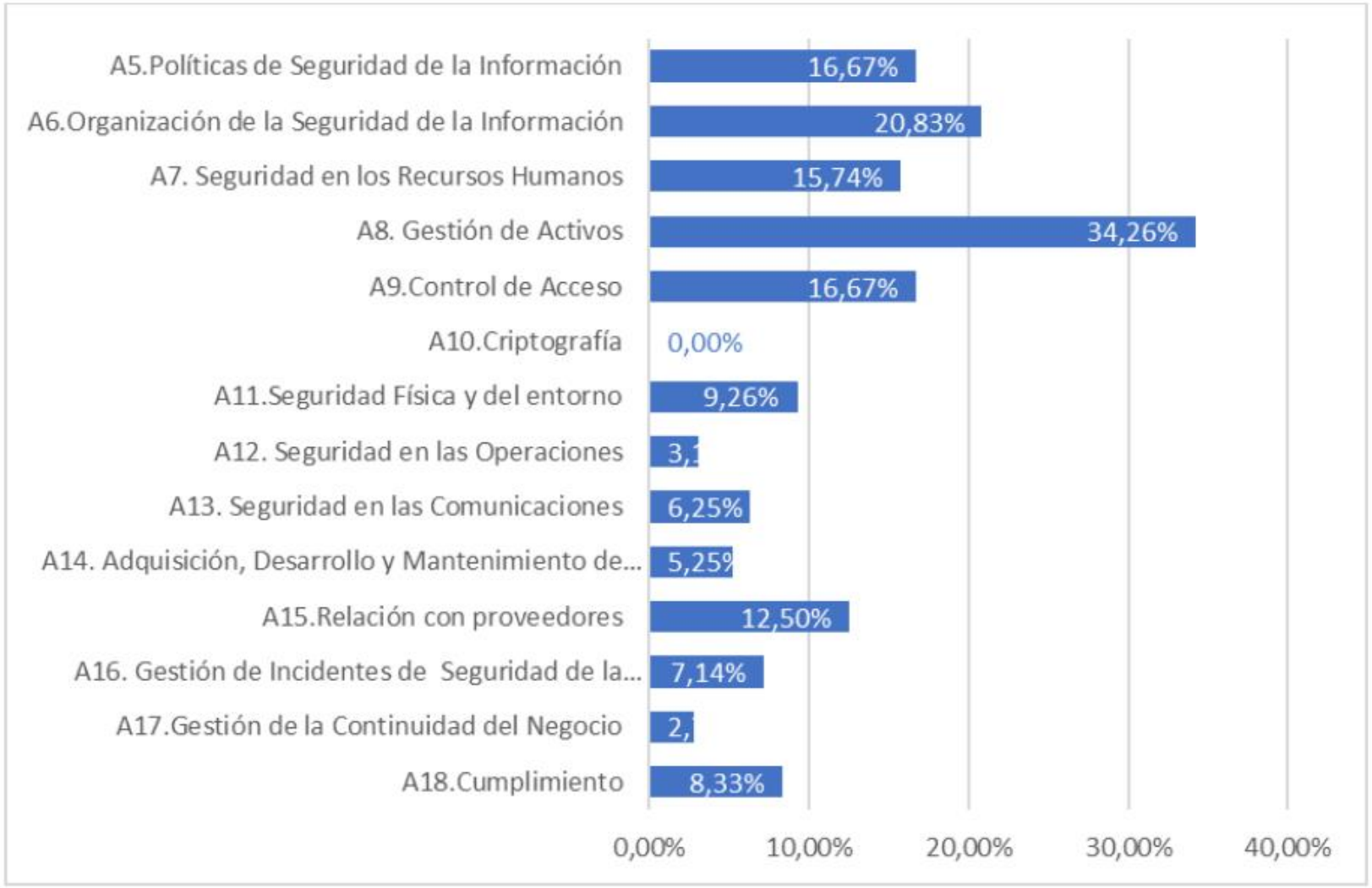
6. Planificación

6.1 Acciones para abordar riesgos y oportunidades (declaración de no aplicabilidad)

Dominio	Objetivos de control	Controles	Descripción
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	A.5.1.1 Políticas de seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	A.7.1 Antes de asumir el empleo	A.7.1.1 Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
		A.7.1.2 Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
	A.7.2 Durante la ejecución del empleo	A.7.2.1 Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
		A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A.8 GESTIÓN DE ACTIVOS	A.8.2 Clasificación de la información	A.8.2.1 Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y suceptibilidad a divulgación o a modificación no autorizada.

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades (declaración de no aplicabilidad)



2. Gestión de objetivos

6. Planificación

6.2 Objetivos de seguridad de la información y planeación para su consecución

POLITICA / OBJETIVOS DEL SGSI	LINEAMIENTOS ESTRATÉGICOS	INDICADOR	FORMULA	META
Contar con una política de seguridad de la información que sea entendible y esté disponible a todo el personal	PRESTIGIO	Conocimiento de la política de seguridad de la información	Cantidad de personas que conocen la política / cantidad total de personas	100%
Cumplir con las regulaciones aplicables en torno a la seguridad de la información.		Clientes satisfechos con el servicio	% Satisfacción del Cliente Interno	>=90%
		SLA establecidos que se han cumplidos	∑ SLAs cumplidos/ ∑ SLAs totales	100%
		Penalidades por incumplimiento contractuales	Monto de penalidades (S/.)	S/. 0
Mejorar continuamente el SGSI		Análisis de Brechas / GAP	Análisis GAP / Brechas Promedio (cláusulas y controles)	>=80%
Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información		Cantidad de personas capacitadas en temas de seguridad de la información	Personas capacitadas / Total personas en el proyecto	>=90%
		Cantidad de Personas que aprobaron el examen de las charlas de seguridad de la información	Personas que aprobaron el examen / Personas que dieron el examen)	>=90%

6. Planificación

6.2 Objetivos de seguridad de la información y planeación para su consecución

POLITICA / OBJETIVOS DEL SGSI	LINEAMIENTOS ESTRATÉGICOS	INDICADOR	FORMULA	META
Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad	**VALOR**	Riesgos atendidos	Riesgos registrados / Riesgos atendidos	>=85%
		Pruebas de continuidad ejecutadas	Pruebas ejecutadas / Total de Pruebas planificadas	100%
Dar respuesta inmediata a los incidentes que se presenten	**ESTABILIDAD**	Incidentes reportados correctamente	Número de incidentes reportados / Total de incidentes ocurridos	>=90%
		Incidentes atendidos correctamente	Número de incidentes reportados / Total de incidentes atendidos	>=90%

6. Planificación

6.2 Objetivos de seguridad de la información y planeación para su consecución

Indicador K1

INDICADOR: K1	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de riesgos de seguridad de la información para los cuales se han implantado controles	Responsable Seguridad de la Información	Anual	Mediciones	100%	100%										
			%Media Anual	100%											
			Objetivo	100%											
MÉTODO DE CÁLCULO: Numero de riesgos identificados sobre los que se ha aplicado controles.															

Indicador K2

INDICADOR: K2	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de cambios aprobados con error conocido por incidencias	Responsable Seguridad de la Información	Mensual	Mediciones	0%	0%										
			%Media Anual	0%											
			Objetivo	<10%											
MÉTODO DE CÁLCULO: Total de cambios implementados en el entorno de producción que han dado lugar a una incidencia, calculado en % sobre el total de cambios implementados en el entorno de producción.															

6. Planificación

6.2 Objetivos de seguridad de la información y planeación para su consecución

Indicador K3

INDICADOR: K3	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de cambios aprobados con error conocido que han necesitado marcha atrás	Responsable Seguridad de la Información	Mensual	Mediciones	0%	0%										
			%Media Anual	0%											
			Objetivo	<5%											

MÉTODO DE CÁLCULO:

Total de cambios implementados en el entorno de producción aprobados por el Responsable de Seguridad y que han necesitado el proceso de marcha.atrás, calculado en % sobre el total de cambios implementados mensualmente.

Indicador K4

INDICADOR: K4	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de incidencias críticas de seguridad atendidas en 24 horas	Responsable Seguridad de la Información	Mensual	Mediciones	100%	100%										
			%Media Anual	100%											
			Objetivo	<95%											

MÉTODO DE CÁLCULO:

Porcentaje de incidencias identificadas como críticas para seguridad, y que han sido atendidas en menos de 24 horas (días laborables), calculado en % , SE CONSIDERA PARA EL CÁLCULO QUE SI NO HAY INCIDENCIAS EN ESE MES , EL PORCENTAJE DE ATENCIÓN ES DEL 100 %

6. Planificación

6.3 Planificación de cambios

CAMBIOS	PROPÓSITO	CONSECUENCIAS POTENCIALES	RECURSOS NECESARIOS	RESPONSABLE	2024			
					SEP	OCT	NOV	DIC
Adquisición de nuevos servidores	Proteger la información del proceso comercial y productivo	1. Reducción de los mantenimientos correctivos. 2. Aumento en la satisfacción del grupo de interés	1. Proveedores de servicios de almacenamiento	Gerente de TI				
Rediseñar nueva arquitectura de información	Reducir los eventos invasivos de protección	1. Mejora en la toma de conciencia. 2. Resistencia al cambio.	1. Proveedor externo 2. Presupuesto.	Gerente de Desarrollo				
Mejorar la cartera de proveedores de servicios de desarrollo	Mejorar la continuidad del servicio	Mejoramiento en la satisfacción del grupo de interés y usuario.	1. Inventario de aplicativos. 2. Personal en los procesos. 3. Presupuesto.	Gerente de Servicios				

3. Gestión de recursos

7. Soporte

7.1 Recursos

CLASIFICACIÓN	ACTIVO
Procesos de negocio	Contabilidad Nomina Planeación Recepción y digitalización de información
Servicios de TI	WhatsApp Correo electrónico corporativo Chat Connect Capacitaciones Servicio de ticket Internet Descargas Digitalización Fotocopiado
Datos, información, conocimiento	Archivo de contabilidad físico y digital Archivo de nómina físico y digital Digitalización de información físico y digital
Sistemas de información transaccionales	Compassion Connect – CRM Salesforce Service Now PPIF – plataforma financiera y contable CO-RED
Sistemas de información de soporte	WhatsApp Service Now Chat Connect BeneficiaryPhotos Carpeta compartida en Drive Avast Free Antivirus
Motores de base de datos	La organización no cuenta con motores de base de datos, sus datos los guardan en libros de Excel.
Sistemas operativos	Windows 10 Pro Windows 11 Pro
Pc´s de escritorios e impresoras	1 pc de escritorio Noc, 1 pc de escritorio LG, 1 pc de escritorio Acer, 2 pc de escritorio Janus, 1 pc de escritorio todo en uno Lenovo, 1 pc portátil Hp, 1 impresora Epson L5290, 1 impresora Epson L365, 1 impresora Epson L495, 1
Servidores	La organización no cuenta con servidores
Centro de redes y cableado	Plan internet 100 megas 11 cámaras de seguridad (no se encuentran en uso)
Centro de computo	La organización no cuenta con centro de computo
Sistemas de energía	7 ups Powest 500Va Planta eléctrica

7. Soporte

7.2 Competencia

Puesto: Especialista en Seguridad de la información

REQUISITOS	DETALLE
Formación Académica, Grado Académico o nivel de estudios	• Título profesional en Ingeniería Informática y/o de Sistemas o carreras afines, colegiado y habilitado. • Egresado de Maestría en Tecnologías de la Información y Comunicaciones, y/o Gobierno de TI y/o Ingeniería de Sistemas o afines.
Cursos y/o programas de especialización	• Programa de Especialización y/o Diplomado en Gestión de Proyectos y/o Gerencia de Proyectos y/o Administración de Proyectos. • Curso de la norma ISO/IEC 27001, CISSP o similares. • Curso en Gestión de Servicios de TI como ITIL u otros.
Conocimientos (No requiere sustentar con documentos)	• Conocimientos Técnicos: Administración de redes y comunicaciones. Administración de centros de datos Administración de soluciones de virtualización Administración de Bases de Datos SQL Server, MySQL, Oracle, entre otros. NTP-ISO 12207, NTP-ISO 27001, NTP-ISO 9001 Ciberseguridad Herramientas de análisis de vulnerabilidades, Ethical Hacking Herramientas para monitoreo de servicios y servidores TI. • Conocimientos Informáticos: Procesador de textos a nivel intermedio Hojas de cálculo a nivel intermedio Programa de presentaciones a nivel intermedio
Experiencia	• Experiencia General: Experiencia mínima de cinco (03) años en instituciones públicas y/o privadas. • Experiencia específica: Experiencia mínima de tres (02) años en implementación y/o mantenimiento de sistemas de gestión de seguridad de la información y/o analista de seguridad de la información y/o auditoria de seguridad de la información y/o monitoreo de controles de seguridad de la información en instituciones públicas y/o privadas
Habilidades o competencias	• Competencias: Vocación de servicio, trabajo en equipo, orientación a resultados. • Habilidades: empatía, capacidad de organización del trabajo y comunicación a todo nivel.
Requisitos adicionales o Certificaciones	• Certificación como ISO27001 Lead Implementer o similares (indispensable) • Certificación como ISO27001 Lead Auditor o similares (deseable) • Certificación en Gestión de Proyectos como Project Management Professional (deseable)

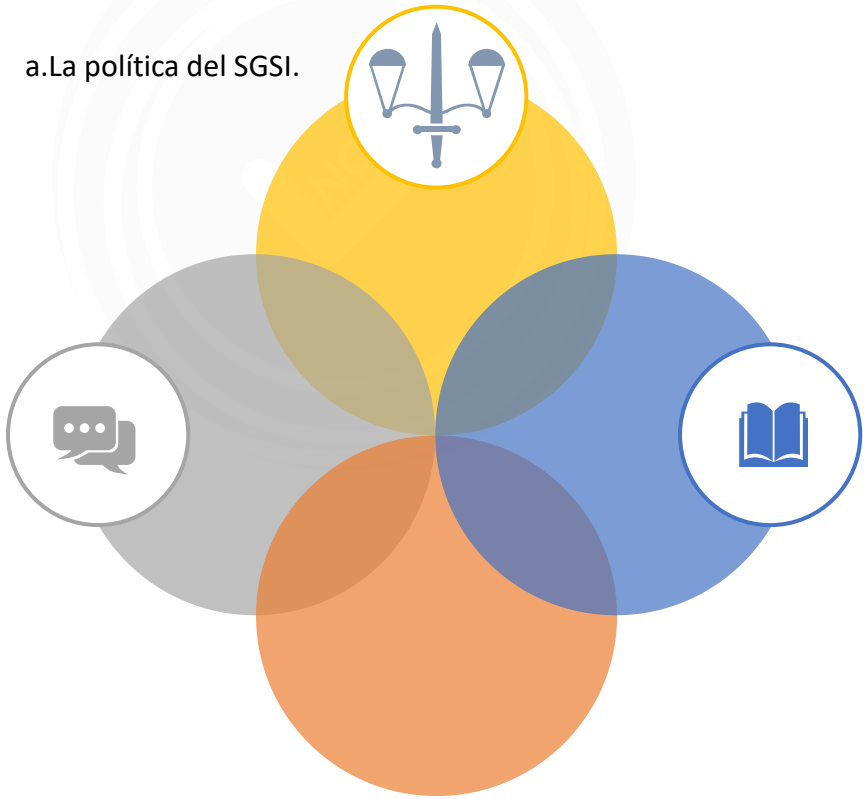
7. Soporte

7.3 Concienciación

Las personas que realizan el trabajo bajo el control de la organización deben ser conscientes de :

a.La política del SGSI.

Las implicaciones del incumplimiento de los requisitos del SGSI.



b. Su contribución a la eficacia del SGSI, incluidos los beneficios de una mejora del desempeño de la SI.

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón