Centro de Especializaciones Noeder

Diploma de Especialización Internacional

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

CLASE 02

IMPLEMENTACIÓN DE LA NORMA ISO 27001

Mg. Ing. Julio Pereyra Rosales

Información documentada mínima en el SGSI

Alcance del Sistema de Gestión

Solicitado en la cláusula 4.3, requiere que la organización defina todos los aspectos, internos y externos, que tengan la capacidad de impedir el logro de los objetivos. Estos aspectos son **condiciones, circunstancias, leyes, acuerdos, requisitos de un organismo regulador, expectativas o solitudes de partes interesadas**.

Política de Seguridad de la Información

La Política de Seguridad de la Información es requerida en la cláusula 5.2 y la responsabilidad compete a la Alta Dirección. Es el documento que expresa la voluntad y el compromiso de la organización por preservar la Seguridad de la Información y cumplir con las obligaciones regulatorias. En ese sentido, debe **expresar también unos objetivos generales, en concordancia con los compromisos asumidos**.

Proceso de Gestión de Riesgos de SI

Este es un requisito establecido en la cláusula 6.1.2. El objetivo es documentar todo el trabajo de planificación, desarrollo de metodologías y herramientas de evaluación, así como el resultado de la Gestión de Riesgos de Seguridad de la Información.

Declaración de aplicabilidad

La declaración de aplicabilidad de la que habla la cláusula 6.1.3 d. es, dentro de la documentación en ISO 27001:2022, un documento obligatorio si se espera certificar el sistema. La aplicabilidad está directamente relacionada con los objetivos y los controles del Anexo A que la organización necesite para alcanzar esos objetivos.

Plan de gestión de riesgos

Las cláusulas 6.1.3 e, 6.2 y 8.3 solicitan la planificación de la gestión de riesgos, y la respectiva documentación de esa actividad.

Objetivos de Seguridad de la Información

Los objetivos que aquí deben documentarse, de conformidad con lo solicitado en la cláusula 6.2, son los específicos de la gestión que, a su vez, estarán vinculados a los controles respectivos del anexo A.

Informes de evaluación y de gestión de riesgos

Las conclusiones y resultados que arrojan las tareas de evaluación y gestión de riesgos deben documentarse según lo solicitado en las cláusulas 8.2 y 8.3.

Inventario de activos

No todos los requisitos de documentación en ISO 27001:2022 parten de una solicitud en una cláusula. **Este, y los subsiguientes en esta guía, son ejemplo de ello**. El inventario de activos, en particular, es requisito para la implementación del Control A.5.9. Por supuesto, en este y en los casos que siguen, se considerarán documentos obligatorios solo en el evento de que el control sea obligatorio para la organización.

Uso aceptable de los activos

Este documento se solicita en el Control A.5.10. También se podría denominar Política de Seguridad Informática, y está vinculado con los activos que se han inventariado en el documento anterior.

https://www.escuelaeuropeaexcelencia.com/2023/01/documentacion-en-iso-270012022-lista-actualizada-de-los-documentos-obligatorios-en-la-ultima-revision/

Información documentada mínima en el SGSI

Procedimiento de respuesta a incidentes

Control que lo solicita: A.5.26. El objetivo es documentar las acciones que prevé la organización ante la ocurrencia de un incidente o una infracción.

Requisitos reglamentarios, contractuales y legales

Un inventario de las leyes, normas, acuerdos o regulaciones a los que está obligada la organización, en materia de Seguridad de la Información o Protección de Datos, es lo que solicita documentar el control A.531.

Procedimientos Operativos de Seguridad para la Gestión de TI

El control A.5.37 es muy específico. Solicita documentar todos los procedimientos prácticos que se ponen en marcha para garantizar la Seguridad de la Gestión de TI.

Definición de roles y responsabilidades de seguridad de la información

Aunque la información que debe documentarse según los controles A.6.2 y A.6.6 **puede incluirse en la política o en la declaración de objetivos**, es bueno también crear un documento exclusivo, para satisfacer el requerimiento.

Definición de configuraciones de seguridad

Se refiere a procedimientos y configuraciones de seguridad en el área de TI, y se solicita en el Control A.8.9.

Principios de ingeniería de sistemas seguros

Finalmente, el control A.8.27 requiere una política de desarrollo seguro de sistemas de información.

https://www.escuelaeuropeaexcelencia.com/2023/01/documentacion-en-iso-270012022-lista-actualizada-de-los-documentos-obligatorios-en-la-ultima-revision/

Registros mínimos en el SGSI

- **Registros sobre capacitaciones, experiencia, calificaciones y habilidades**, que usualmente son certificados de programas de formación, CVs o evaluaciones de resultados de las capacitaciones impartidas.
- **Reportes, seguimiento y mediciones** de la efectividad de los controles o de la eficiencia de alguna acción correctiva.
- **Resultados de la auditoría interna** o del programa de auditorías.
- **Resultados de las inspecciones o revisiones** de la Alta Dirección.
- **Resultados de la implementación de acciones correctivas** u otro tipo de medidas tomadas para prevenir riesgos.
- **Actividades de usuarios** y otros registros automáticos en los diferentes sistemas de información.

https://www.escuelaeuropeaexcelencia.com/2023/01/documentacion-en-iso-270012022-lista-actualizada-de-los-documentos-obligatorios-en-la-ultima-revision/

4. Contexto de la organización

4.1 Comprensión de la organización y su contexto

Análisis DOFA SITECH	Oportunidades	Amenazas
	1. Crecimiento del mercado en torno a la tecnología. 2. Estilos de vida tecnológicos. 3. Oportunidades en el sector educativo.	1. Patrones y cambios en el mercado. 2. Tasa de cambio de moneda extranjera fluctuante. 3. Competencia desleal.
Fortalezas	**Estrategias FO**	**Estrategias FA**
1. Habilidad para responder a la tecnología Cambiante. 2. Agresividad para enfrentar la competencia. 3. Nivel tecnológico de la empresa. 4. Estabilidad laboral y nivel de pertenencia de la fuerza de trabajo. 5. Lealtad y satisfacción del cliente. 6. Facilidad de créditos y acuerdos de pago con proveedores.	1. Implementar estrategias de negocio para nichos de mercado en crecimiento. 2. Aprovechar la lealtad de los clientes para generar estabilidad y dedicar esfuerzo en incursionar en el sector educativo. 3. Generar un acercamiento a los prospectos de clientes mediante el uso de tecnología aprovechando el uso masivo de las redes sociales.	1. Generar planes de acción mediante el uso delos créditos y acuerdos de pagos a proveedores para superar la fluctuación de la moneda extranjera. 2. Fortalecer y socializar la ética en los empleados y clientes evitando los impactos de la competencia desleal. 3. Generar estrategias tecnológicas de cambio para responder oportunamente a las variaciones y requerimientos del mercado.
Debilidades	**Estrategias DO**	**Estrategias DA**
1. Falta de sistemas de control. 2. Alta Rotación de personal. 3. Falta de inversión de I&D de nuevos servicios. 4. Estabilidad de los costos.	1. Realizar pruebas piloto de tecnología con el personal internos, para motivarlos a conocer la línea de negocio, aprovechando el auge de la tecnología en los estilos de vida actuales. 2. Implementar las soluciones del sector educativo internamente para incentivar la I&D de nuevos servicios y capacitar al personal en general en el uso de las mismas. 3. Generar estrategias generales para estabilizar los costos de operación al contemplar el crecimiento de la organización junto con el del mercado.	1. Generar sistemas de control y verificación de procesos 2. Definir procesos documentados que le permita al personal generar estándares en busca de costos mínimos de reprocesos. 3. Implementar planes de incentivos para evitar la alta rotación de personal y la migración a la competencia.

FORTALEZAS	DEBILIDADES
Políticas de Seguridad Efectivas	Falta de Recursos
Tecnología Avanzada	Sistemas Desactualizados
Personal Capacitado	Capacitación Inadecuada
Cultura de Seguridad	Políticas Inconsistentes
OPORTUNIDADES	**AMENAZAS**
Avances Tecnológicos	Amenazas Avanzadas y Persistentes (APT)
Conciencia Creciente	Ransomware
Colaboración y Alianzas	Fugas de Información
Regulaciones y Normativas	Evolución de las Amenazas

4. Contexto de la organización

4.2 Comprensión de las necesidades y expectativas de partes interesadas

PARTES INTERESADAS		REQUISITOS DEL SGSI
INTERNAS	ACCIONISTAS	Maximizar la rentabilidad del negocio.
	GERENTES	Maximizar la rentabilidad del negocio. Garantizar la disponibilidad de los servicios entregados al cliente.
	COLABORADORES	Laborar en una empresa sólida y de prestigio. Proteger su información personal.
EXTERNAS	CLIENTE	Asegurar la confidencialidad, integridad y disponibilidad de su información
	PROVEEDORES	Alianzas estratégicas Proteger la continuidad de las operaciones Cumplimiento de los compromisos pactados
	GOBIERNO	Cumplir con las leyes Responsabilidad Social

4. Contexto de la organización

4.3 Determinar el alcance del SGSI.

MAPFRE

ALCANCE

Luego de analizar los aspectos internos y externos, las necesidades y expectativas de las partes interesas y las interfaces y dependencias internas y externas de la empresa detallas en el documento SGSI.DC.01 Conocimiento de la organización y las partes interesadas, se determina el siguiente alcance para el SGSI:

"*Sistema de Gestión de Seguridad de la Información para el servicio de Facturación Electrónica, incluyendo PSE (Proveedor de Servicios Electrónicos) soportado por los procesos de Implantación, Soporte y Desarrollo de Software, de acuerdo con la declaración de aplicabilidad vigente*"

4. Contexto de la organización

4.3 Determinar el alcance del SGSI.

Certificado ES23/00001295

El sistema de gestión de

LEADER NETWORK MARKETING, S.L

Dirección Fiscal: C/ San Vicente Mártir, 160, pta 2, 46007 Valencia

ha sido evaluado y certificado que cumple con los requisitos de

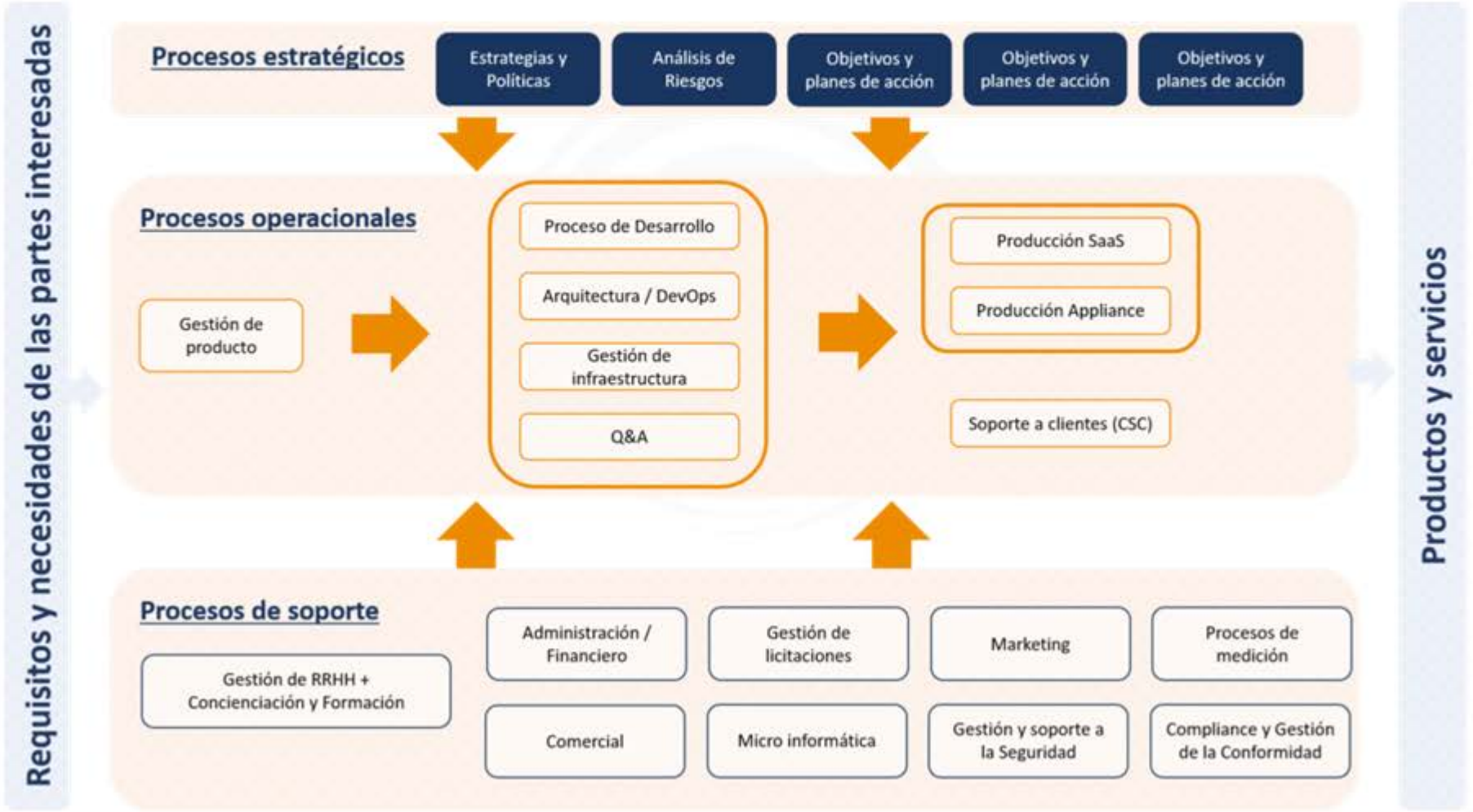
ISO/IEC 27001:2022

Para las siguientes actividades

Los sistemas de información que dan soporte a la implantación y asistencia técnica de soluciones de telecomunicaciones y seguridad; diseño,
programación y gestión de plataformas documentales de coordinación y control de accesos.
Según declaración de aplicabilidad Rev.2

4. Contexto de la organización

4.4 Sistema de gestión de seguridad de la información



5. Liderazgo

5.1 Liderazgo y compromiso

La Alta Dirección debe:

Establecer la política y objetivos del SGSI y que sean compatibles con la dirección estratégica.

Integración del SGSI en los procesos del negocio.

Apoyar a otros roles de la dirección para la eficacia del SGSI.

Asegurarse que los recursos necesarios del SGSI estén disponibles.

5. Liderazgo

5.1 Liderazgo y compromiso

La Alta Dirección debe:

- Comunicación de la importancia del SGSI.
- Asegurarse que el SGSI cumpla lo planificado.
- Comprometerse, dirigir y apoyar a las personas para contribuir a la eficacia de SGSI.
- Promover la mejora continua.

5. Liderazgo

5.2 Política

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La dirección de OBSS INGENIERÍA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para OBSS INGENIERÍA la protección de la información es fundamental y busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a OBSS INGENIERÍA según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de OBSS INGENIERÍA.
- Garantizar la continuidad del negocio frente a incidentes.

OBSS INGENIERÍA ha decidido junto con su equipo directivo apoyarse en en una consultoría para el diseño la definición y posterior implementación y operación de un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva. Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc.

Para abordar este punto es necesario remitirse a la "Guía de políticas específicas de seguridad y privacidad de la información" y mencionar aquellas que OBSS INGENIERÍA haya establecido como necesarias y primordiales.

5. Liderazgo

5.3 Roles, responsabilidades y autoridad

	PROCEDIMIENTO	Código: PRO-028
	GESTIÓN DE ACTIVOS	Fecha: 09/03/2021 | Versión: 1
		Página 1 de 5

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para establecer, mantener y asegurar un nivel de protección adecuado para los activos de información de Core Business Corporation.

2. **ALCANCE**

Aplica a todo el personal de CORE BUSINESS CORPORATION.

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. **DEFINICIONES**

- **Activo de información:** Es todo aquello que representa valor para la CBC desde software, hardware, información, servicios y colaboradores.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad**: Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad:** Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Propietario del activo**: Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Usuario:** Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Propietario del riesgo:** Es el responsable de la realización y ejecución de los controles.

5. RESPONSABILIDADES

5.1. **Oficial de Seguridad de la Información**
- Informar al Socio principal sobre el desempeño del SGSI.
- Dar seguimiento a los registros de SGSI.
- Organizar la realización de las auditorías internas y externas del SGSI.
- Promover la capacitación y concientización de los colaboradores acerca de la gestión de la seguridad de la información.
- Liderar los proyectos de mejora del SGSI.

5.2. **Propietario del Activo de Información**
- Controlar el uso y seguridad de los activos que le son asignados para la creación, procesamiento, transmisión y almacenamiento de información relacionadas al proceso o área que le compete.
- Entender y abordar los riesgos relacionados a la seguridad de la información de los activos del proceso o área de su responsabilidad.
- Asegurar que el activo de información se utiliza únicamente para los propósitos de la organización.

5.3. **Usuario del Activo de Información**
- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos para el uso aceptable de los activos de información que le compete.
- Comunicar al propietario del activo de información las amenazas y vulnerabilidades que identifique durante el desarrollo de sus actividades.

	PROCEDIMIENTO	Código: PRO-023
	GESTIÓN DE RIESGOS OPERACIONALES	Fecha: 5/10/21 | Versión: 1
		Página 1 de 5

1. **OBJETIVO**

Establecer el proceso para la identificación, análisis, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información; asimismo, definir los controles que permitan mitigar o disminuir el riesgo identificados.

2. **ALCANCE**

Aplica a todos los procesos relacionados con el SIG.

Se considera los riesgos y oportunidades hacia los procesos que afecten a los activos de información.

3. **REFERENCIAS:**

- ISO 27001:2013. Requisitos de un Sistema de Seguridad de la Información.
- ISO 27002. Técnicas de seguridad Código de prácticas para los controles de seguridad de la información.
- ISO 3100. Gestión de Riesgos

4. **DEFINICIONES**

- **Activo de información:** Es todo aquello que representa valor para la Entidad desde software, hardware, información, servicios y personas.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad**: Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad:** Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Riesgo aceptable:** es el riesgo que se ha conseguido reducir o mitigar de tal forma que pueda ser tolerado por la organización. Nivel de riesgo medio o bajo.
- **Riesgo residual:** riesgo restante después del tratamiento del riesgo.
- **Probabilidad:** Posibilidad de que el evento riesgoso ocurra de acuerdo con situaciones ya presentadas basadas en registros reales, datos, hechos o información conocida.
- **Amenaza:** Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática.
- **Impacto:** Consecuencia que pueda ocasionar en la empresa la materialización del riesgo.
- **Propietario:** Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Custodio:** Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Vulnerabilidad:** Debilidad de los sistemas, ya sean equipos de cómputo, servidores, tanto hardware como software, sistema operativo, sistemas de información, aplicaciones, redes, etc. que puede ser utilizados o aprovechados por delincuentes informáticos, con el fin de ocasionar daño o extraer información confidencial y datos personales.
- **Consecuencia:** el resultado de un evento (amenaza) que afecta a los objetivos.
- **Propietario del riesgo:** Es el responsable de la realización y ejecución de los controles.

5. Liderazgo

5.3 Roles, responsabilidades y autoridad

1

Líder de Seguridad

Define la estrategia y supervisa el programa de seguridad, asegurando la alineación con objetivos y reportando KPIs.

2

Administrador de Riesgos de Seguridad

Preside el Consejo de Riesgos de la Información y con el grupo gestiona riesgos, supervisa, define procesos y asegura la aplicación de políticas.

3

Auditor Interno de Seguridad

Realiza auditorías, mantiene independencia, crea y ejecuta planes anuales, informa resultados a la dirección general.

4

Propietarios de Control

Desarrollan entornos seguros, gestionan operaciones de seguridad, realizan evaluaciones de configuración y aseguran disponibilidad de sistemas.

5. Liderazgo

5.3 Roles, responsabilidades y autoridad

Todo el personal

Recibe capacitación básica de seguridad, formación específica según funciones y entrenamiento normativo o contractual.

5

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

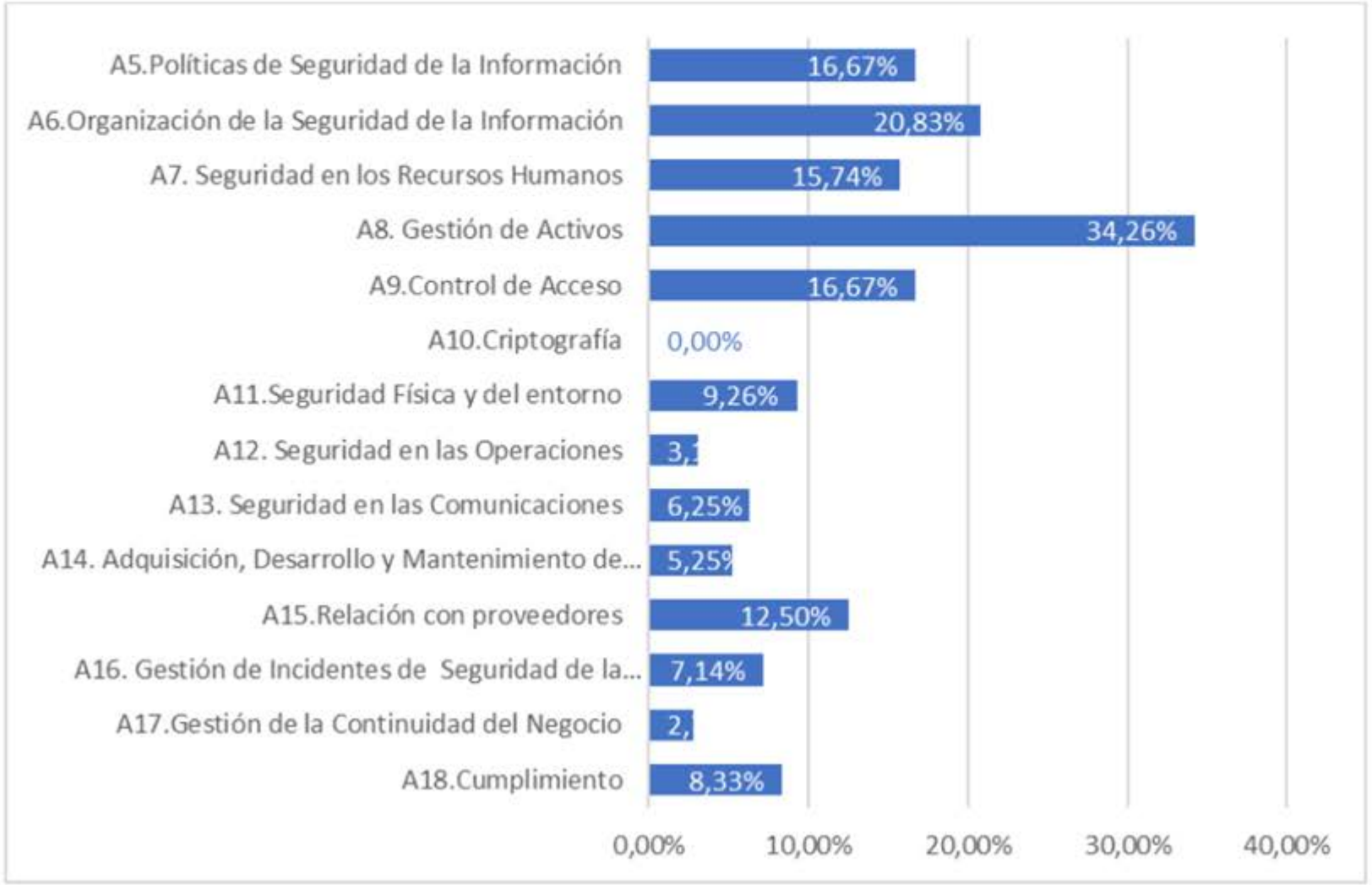
6. Planificación

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 susceptibilidad a divulgación o a modificación no autorizada.

6. Planificación

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



6. Planificación

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

Dependencia	Nombre de la tarea	Política de Gestión y Desempeño	Objetivo SGSI (*)	Responsable	Fecha Inicio	Fecha Fin	Fuente de Financiación
				Proveedor de Seguridad			
Dirección de Tecnología	Mitigación de vulnerabilidad de la prueba anual del Q1-2024	Seguridad Digital	OBJ 8	Dirección de Tecnología	1/04/2024	30/06/2024	Findeter $0
Vicepresidencia de Riesgos	Ejecución análisis de vulnerabilidades primera prueba anual Q2-2024	Seguridad Digital	OBJ 8	Oficial de Seguridad de la Información Proveedor de Seguridad	1/07/2024	30/08/2024	Findeter $38,901.500
Dirección de Tecnología	Mitigación de vulnerabilidad de la prueba anual del Q2-2024	Seguridad Digital	OBJ 8	Dirección de Tecnología	1/09/2024	31/12/2024	Findeter $0
Vicepresidencia de Riesgos	Ejecución Prueba de Hacking ético	Seguridad Digital	OBJ 8	Oficial de Seguridad de la Información Proveedor de Seguridad	1/07/2024	31/12/2024	Findeter $16,566,514
Vicepresidencia de Riesgos	Ejecución Prueba de Ingeniería Social	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información Proveedor de Seguridad	1/07/2024	31/12/2024	Findeter $14,081,537
Vicepresidencia de Riesgos	Actualizar la gestión de riesgos de proveedores en el sistema WRM	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información Unidad Riesgos Operativos	1/01/2024	07/30/2024	Findeter $0

(*) Objetivos del SGSI incluidos dentro del SGI

OBJ 6: Optimizar el nivel de efectividad de los controles de la Entidad.
OBJ 7: Incrementar el nivel de conciencia de los trabajadores en seguridad de la información para promover el uso adecuado de los activos de información.
OBJ 8: Fortalecer la seguridad de la información a través de la gestión oportuna de los incidentes y vulnerabilidades.

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				

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.

7. Soporte

7.4 Comunicación

TITULO	ASUNTO (SUBJECT)	DIRIGIDO POR	DIRIGIDO A / O (ROLES)	FECHA DE INICIO	USO DEL CANAL	SETIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMRE			
QUE COMUNICAR	QUE COMUNICAR	QUIEN DEBE COMUNICAR	A QUIEN COMUNICAR	CUANDO COMUNICAR	CANAL DE COMUNICACIÓN	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
5.2 Política 6.2 Objetivos de seguridad de la información	Política y Objetivos del SGSI	Gerente del Servicio	Personal (Servicio)	Anual	email																
5.2 Política 6.2 Objetivos de seguridad de la información	Política de gestión del servicio y la importancia de su cumplimiento.	Oficial de Seguridad de la Información (Servicio)	Personal (Servicio)	Por Evento	Charla de inducción / File Server																
5.3 Roles organizacionales, responsabilidades y autoridades	Funciones y responsabilidades	Coordinador del área (Servicio)	Personal nuevo (Servicio)	Al inicio de la relación laboral y/o cuando se actualice la descripción de puestos.	Documento																

7. Soporte

7.4 Comunicación

TITULO	ASUNTO (SUBJECT)	DIRIGIDO POR	DIRIGIDO A / O (ROLES)	FECHA DE INICIO	USO DEL CANAL	SETIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMRE			
QUE COMUNICAR	QUE COMUNICAR	QUIEN DEBE COMUNICAR	A QUIEN COMUNICAR	CUANDO COMUNICAR	CANAL DE COMUNICACIÓN	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
A.16 Gestión de Incidentes de seguridad de la información	Eventos o incidentes de seguridad de la información	Personal ONP / Personal del Servicio / Proveedores / Visitas	Mesa de Administración de Servicios	Por Evento	Informe																
9.1 Monitoreo, medición, análisis y evaluación	Servicio de Monitoreo	Responsable del Proceso (GMD)	Responsable del Proceso (ONP)	Mensual	Informe																
6.1 Acciones para abordar los riesgos y oportunidades	Resultados del análisis y evaluación de riesgos / Plan de tratamiento de riesgos	Oficial de Seguridad de la Información (Servicio)	Gestor de Seguridad de la Información (ONP)	Anual	Informe																
9.2 Auditoría Interna	Resultados de informes de auditoría	Oficial de Seguridad de la Información (Servicio)	Gestor de Seguridad de la Información (ONP)	Anual	Informe																
9.3 Revisión de gestión	Resultados de la revisión por la Dirección	Oficial de Seguridad de la Información (Servicio)	Comité del SGSI	Mensual	Acta de reunión																
10.1 No Conformidades y acciones correctivas	Resultado de las acciones correctivas y preventivas	Oficial de Seguridad de la Información (Servicio)	Gestor de Seguridad de la Información (ONP)	Permanente	Informe																
A.12.6.1 Gestión de las vulnerabilidades técnicas	Resultados del análisis de vulnerabilidades técnicas	Jefe de Producción	Supervisor de Administración de Plataformas y Redes	Anual	Informe																

7. Soporte

7.5 Información documentada

CLASIFICACIÓN	DEFINICIÓN	EJEMPLOS
CONFIDENCIAL	Es la información que debe mantenerse en la más estricta reserva. Está sujeta al cumplimiento de requisitos legales y/o contractuales. Tiene mucho valor para su propietario, es crítica para el desarrollo estratégico del negocio y su divulgación no autorizada podría ocasionar impactos severos a la organización en términos económicos y de prestigio, principalmente. Su divulgación a terceros podría darse sólo bajo la autorización formal del representante legal, mediante la firma de un acuerdo de confidencialidad.	Información de Clientes, Información Comercial, Información del personal, Información Económica-financiera, etc.
RESTRINGIDO	Es aquella información inherente a las operaciones de un proceso o área de negocio específica. Podría estar sujeto a cumplimiento legal y/o contractual, es crítica para las operaciones del proceso o área de negocio, su pérdida o divulgación no autorizada podría ocasionar perjuicios a la organización en términos económicos, de servicio al cliente y ventaja competitiva. Su divulgación a terceros podría darse sólo bajo la autorización formal de su propietario mediante la firma de un acuerdo de confidencialidad.	Procesos operativos, Políticas específicas, Procedimientos, Instructivos, Manuales técnicos y de usuario, Formatos y Registros, y otros similares
PÚBLICO	Información destinada al conocimiento de la comunidad.	Publicaciones en Página Web

DOCUMENTOS DE LA ORGANIZACIÓN	DOCUMENTO		
	Elaboración o Modificación	Revisión	Publicado y Distribuido por
Documentos del Sistema de Gestión: Política y Objetivos	Oficial de Seguridad de la Información	Gerente del Proyecto	Gerente del Proyecto
Documentos del Sistema de Gestión: Manual, procedimientos, formatos, etc.	Oficial de Seguridad de la Información	Gerente del Proyecto	Oficial de Seguridad de la Información
Documentos de Operación	Personal dentro del alcance del SGSI	Dueño del proceso o área	Dueño del proceso o área

7. Soporte

7.5 Información documentada

DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
POLITICAS
POL.GER.001 Política de Seguridad de la Información
POL.GER.002 Política de Escritorio y Pantalla Limpios
POL.GER.003 Política de Gestión de Accesos
POL.GER.004 Política de Gestión de activos
POL.GER.005 Política de Administración de Software
MANUALES
MAN.GER.001 Manual de Organización y Funciones del SGSI
MAN.GER.002 Manual de Manual SGSI
MAN.GER.003 Manual de Gestión de Riesgos
MAN.GER.005 Manual de Alcance del SGSI
PROCEDIMIENTOS
PRO.GER.001 Ingreso de Personal
PRO.GER.002 Proceso Disciplinario

DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
PRO.GER.003 Terminación de Relación Laboral
PRO.GER.004 Control de Documentos
PRO.GER.005 Control de Registros
PRO.GER.006 Auditoria Interna SGSI
PRO.GER.007 Acciones Correctivas y Preventivas
PRO.GER.008 Gestión de Incidentes de Seguridad
PRO.GER.009 Medición efectividad de controles
PRO.GER.010 Comunicaciones del SGSI
PRO.GER.011 Cumplimiento y requisitos legales
PRO.GER.012 Gestión de activos de información
PRO.GER.013 Compresion y Encriptacion de Archivos con el Winzip
PRO.GER.014 Seguridad Física y del ambiente
PRO.GER.015 Relaciones con el proveedor
PRO.GER.016 Gestión de la continuidad
PRO.SIN.001 Control de Accesos
PRO.MAS.025 Gestión de Incidencias
PRO.MAS.053 Gestión de Cambios

7. Soporte

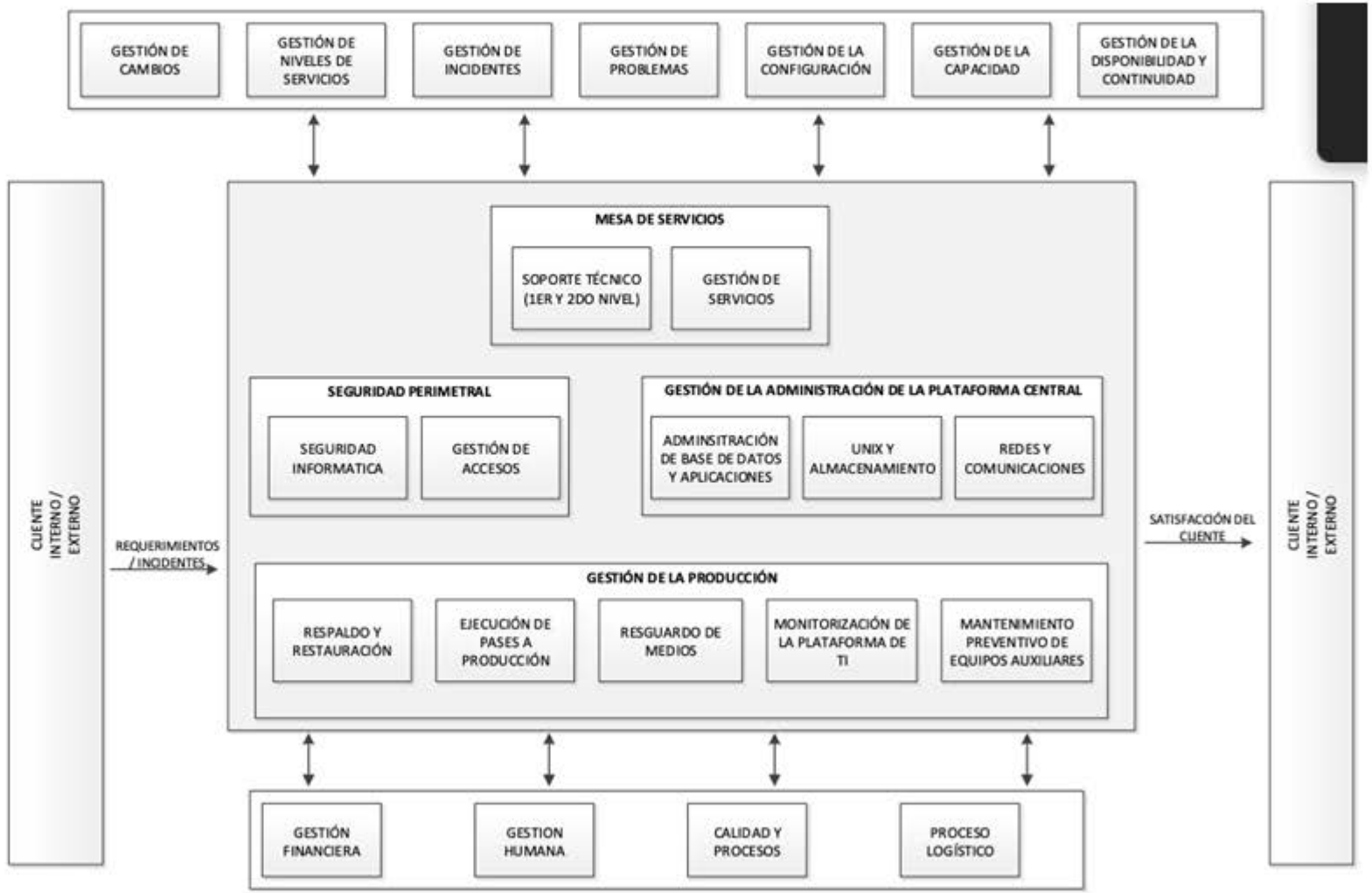
7.5 Información documentada

FORMATOS
FOR.GER.001 Compromiso de confidencialidad
FOR.GER.002 Declaración Jurada
FOR.GER.003 Lista de personal
FOR.GER.004 Entrega de cargo
FOR.GER.005 Plan de capacitación del personal
FOR.GER.006 Plan de Contingencia
FOR.GER.007 Lista de asistencia
FOR.GER.008 Lista maestra de documentos
FOR.GER.009 Lista maestra de registros
FOR.GER.010 Solicitud de cambio
FOR.GER.011 Revisión post implementación
FOR.GER.012 Lista de Contactos
FOR.GER.013 Identificación de Partes Interesadas del SGSI
FOR.GER.014 Declaración de Responsabilidad de Uso de Cuentas Privilegiadas
FOR.GER.015 Examen
FOR.GER.016 Inventario de Activos

DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
FOR.GER.017 Gestión de riesgos y oportunidades
FOR.GER.018 Enunciado de Aplicabilidad
FOR.GER.019 Plan De Tratamiento de Riesgos
FOR.GER.020 Programa Anual de Auditoria
FOR.GER.021 Plan de Auditoria Interna
FOR.GER.022 SAC
FOR.GER.023 Medición de Procesos y Controles del SGSI
FOR.GER.024 Identificación de Requisitos de Seguridad de la Información
FOR.GER.025 Objetivos del SGSI

8. Operación

8.1 Planificación y control operacional



8. Operación

8.1 Planificación y control operacional

	PROCEDIMIENTO	Código: PRO.025
	GESTIÓN DE ACTIVOS	Fecha: 08/03/2021 | Versión: 1
		Página 1 de 5

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para establecer, mantener y asegurar un nivel de protección adecuado para los activos de información de Core Business Corporation.

2. **ALCANCE**

Aplica a todo el personal de CORE BUSINESS CORPORATION.

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. **DEFINICIONES**

- **Activo de información:** Es todo aquello que representa valor para la CBC desde software, hardware, información, servicios y colaboradores.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad**: Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad**: Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Propietario del activo**: Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Usuario**: Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Propietario del riesgo**: Es el responsable de la realización y ejecución de los controles.

5. **RESPONSABILIDADES**

5.1. **Oficial de Seguridad de la Información**

- Informar al Socio principal sobre el desempeño del SGSI.
- Dar seguimiento a los registros de SGSI.
- Organizar la realización de las auditorías internas y externas del SGSI.
- Promover la capacitación y concientización de los colaboradores acerca de la gestión de la seguridad de la información.
- Liderar los proyectos de mejora del SGSI.

5.2. **Propietario del Activo de Información**

- Controlar el uso y seguridad de los activos que le son asignados para la creación, procesamiento, transmisión y almacenamiento de información relacionadas al proceso o área que le compete.
- Entender y abordar los riesgos relacionados a la seguridad de la información de los activos del proceso o área de su responsabilidad.
- Asegurar que el activo de información se utiliza únicamente para los propósitos de la organización.

5.3. **Usuario del Activo de Información**

- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos para el uso aceptable de los activos de información que le compete.
- Comunicar al propietario del activo de información las amenazas y vulnerabilidades que identifique durante el desarrollo de sus actividades.

	PROCEDIMIENTO	Código: PRO.025
	GESTIÓN DE RIESGOS OPERACIONALES	Fecha: 5/10/21 | Versión: 1
		Página 1 de 5

1. **OBJETIVO**

Establecer el proceso para la identificación, análisis, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información, asimismo, definir los controles que permitan mitigar o disminuir el riesgo identificados.

2. **ALCANCE**

Aplica a todos los procesos relacionados con el SIG.

Se considera los riesgos y oportunidades hacia los procesos que afecten a los activos de información.

3. **REFERENCIAS:**

- ISO 27001:2013. Requisitos de un Sistema de Seguridad de la Información.
- ISO 27002. Técnicas de seguridad Código de prácticas para los controles de seguridad de la información.
- ISO 3100. Gestión de Riesgos

4. **DEFINICIONES**

- **Activo de información:** Es todo aquello que representa valor para la Entidad desde software, hardware, información, servicios y personas.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad**: Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad:** Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Riesgo aceptable:** es el riesgo que se ha conseguido reducir o mitigar de tal forma que pueda ser tolerado por la organización. Nivel de riesgo medio o bajo.
- **Riesgo residual:** riesgo restante después del tratamiento del riesgo.
- **Probabilidad:** Posibilidad de que el evento riesgoso ocurra de acuerdo con situaciones ya presentadas basadas en registros reales, datos, hechos o información conocida.
- **Amenaza:** Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática.
- **Impacto:** Consecuencia que pueda ocasionar en la empresa la materialización del riesgo.
- **Propietario:** Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Custodio:** Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Vulnerabilidad:** Debilidad de los sistemas, ya sean equipos de cómputo, servidores, tanto hardware como software, sistema operativo, sistemas de información, aplicaciones, redes, etc. que puede ser utilizados o aprovechados por delincuentes informáticos, con el fin de ocasionar daño o extraer información confidencial y datos personales.
- **Consecuencia:** el resultado de un evento (amenaza) que afecta a los objetivos.
- **Propietario del riesgo:** Es el responsable de la realización y ejecución de los controles.

8. Operación

8.1 Planificación y control operacional

	PROCEDIMIENTO	Código: PRO.009	
Core Business Corp	GESTIÓN DE R.R.H.H	Fecha: 24/11/2021	Versión: 4
		Página 1 de 3	

1. **OBJETIVO**

   Establecer los lineamientos para gestión de los recursos humanos de Core Business Corp. (CBC), desde el ingreso de los nuevos colaboradores, los procesos de formación, conocimientos de la empresa; la observación, medición y análisis del desempeño laboral y la desvinculación de los colaboradores de CBC.

   Reconocer al colaborador que mediante el despliegue de sus conocimientos, habilidades y actitudes alcanza un extraordinario desempeño organizacional

2. **ALCANCE**

   Este procedimiento es de alcance a todos los trabajadores de Core Business Corp (CBC).

3. **REFERENCIAS**

   - ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
   - ISO 45001: 2018: Sistema de Seguridad y Salud en el Trabajo.
   - ISO/IEC 27001: 2013 Gestión de seguridad de la información

4. **DEFINICIONES**

   - **Competencia:** capacidad con la que se aplican los conocimientos y las habilidades con el fin de conseguir los resultados previstos.
   - **Retroalimentación o Feedback:** Proceso de retroalimentación en el cuál intervienen un colaborador y su jefe con la finalidad de establecer un plan de mejora que impacte positivamente en los factores que afectan el desempeño.
   - **Formación:** Es un proceso de mejora continua en el que se busca mejorar las habilidades personales y laborales, así como aumentar la productividad de los colaboradores. Asimismo, permite la reducción de accidentes de trabajo debido a la implementación de conocimientos y la satisfacción laboral.
   - **Capacitación:** Es el proceso destinado a promover, facilitar, fomentar y desarrollar las aptitudes, habilidades o grados de conocimiento de los trabajadores, con el fin de permitirles mejores oportunidades, condiciones de vida y de trabajo, y de incrementar la productividad procurando la necesaria adaptación de los trabajadores a los procesos tecnológicos y a las modificaciones estructurales de la economía.

5. **DESARROLLO**

   5.1 **Reclutamiento y selección**

   El proceso de reclutamiento y selección es realizado por el Practicante de Psicología laboral, bajo la supervisión del Jefe de Administración y Finanzas.

   Las actividades de reclutamiento y selección consideran el perfil de puesto descrito en el Manual de Organización y funciones de la Organización.

   La actividad de reclutamiento se realiza a través de la publicación en bolsa de trabajo y solicitud, mediante correo electrónico, de recomendaciones al personal de CBC.

   La selección del nuevo trabajador se realiza en las siguientes etapas:

   - Evaluación preliminar de la hoja de vida de los postulantes; debe cumplir con lo establecido en el perfil de puesto.
   - Confirmación de las referencias y veracidad del Currículo de los postulantes.
   - Entrevista personal o virtual, a cargo del Practicante de Psicología Organizacional, Jefe del Área y Socio Principal.
   - Evaluación de capacidades, se envía una actividad relacionada al puesto de trabajo para que sea desarrollada por el postulante, de acuerdo con el resultado de esta actividad se define al postulante seleccionado.
   - Solicitud y revisión de antecedentes policiales, judiciales y penales del candidato seleccionado
   - Comunicación a los postulantes, seleccionados y no seleccionados el fin del proceso.

   Todos los postulantes pasan por todas las etapas de selección hasta llegar a la evaluación final, si el postulante no cumple los requerimientos de una etapa, se descalifica.

8. Operación

8.1 Planificación y control operacional

	PROCEDIMIENTO	Código: PRO.004	
	GESTIÓN DEL CAMBIO	Fecha: 14/05/2021	Versión: 2
		Página 1 de 2	

1. **OBJETIVO**

El presente documento establece los lineamientos para gestionar los cambios, procesos de negocio, instalaciones de procedimiento de la información y sistemas, y las modificaciones que impactan al Sistema Integrado de Gestión.

2. **ALCANCE**

Aplica a todos los cambios mayores relacionados con el Sistema Integrado de Gestión.

3. **REFERENCIAS:**

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018. Requisitos de un Sistema de gestión de seguridad y salud en el trabajo.
- ISO 27001:2013. Requisitos de un Sistema de Gestión de Seguridad de la Información.

4. **DEFINICIONES**

- **SIG:** Sistema Integrado de Gestión.
- **Cambio mayor:** Cambio que involucra la intervención de la gerencia, tal y como lo muestra la tabla 1.
- **Cambio menor:** Cambios que pueden ser gestionados por acciones correctivas y no implica la necesidad gestionar un proyecto detallado, por ejemplo: control de cambios en la información documentada, cambios de fecha, auditor, lugar de ejecución, etc., de los servicios coordinados con el cliente.

5. **DESARROLLO**

5.1. Identificación de necesidad de cambio

Todo colaborador de CBC puede identificar y generar una solicitud de cambio. Dicha solicitud será considerada siempre y cuando se exponga un cambio que afecte al SIG, como lo expone la tabla 1.

Tabla 1. Listado de cambios aplicables

Estratégico	• Cambio de planificación estratégica (análisis de contexto). • Aspectos legales.
Financieros	• Asignación o reasignación de presupuesto a alguna área específica o por algún requerimiento específico. • Compra de servicios o bienes mayores a 15000 soles.
Recurso Humano	• Asignación o reasignación de responsabilidades. • Creación de nuevos puestos de trabajo.
Procesos Operativos	• Cambio de metodología de auditoría, inspección, asesoría, capacitación. • Adición de nuevos servicios.
Procesos de Apoyo	• Cambio de infraestructura tecnológica a nivel corporativo. • Cambio de ambiente de trabajo.

Tras la identificación, el colaborador debe comunicarlo enviando un correo al responsable de Desarrollo de Procesos y Socio Principal para su respectiva evaluación.

	PROCEDIMIENTO	Código: PRO.015	
	INFRAESTRUCTURA TECNOLOGICA	Fecha: 08/05/2021	Versión: 1
		Página 1 de 3	

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para elaborar y controlar los documentos relacionados a los servicios informáticos de Core Business Corporation.

2. **ALCANCE**

Aplica a todos los procedimientos y documentos relacionados con el Sistema Integrado de Gestión de CORE BUSINESS CORPORATION.

3. **REFERENCIAS:**

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018. Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001: Sistema de Gestión de Seguridad de la Información.

4. **DEFINICIONES**

- **CPanel.** Permite administrar una cuenta de alojamiento web con la máxima eficiencia. Ya sea creando nuevos usuarios FTP y direcciones de correo electrónico o monitoreando recursos, creando subdominios e instalando software.
- **Hosting:** Es un servicio de alojamiento para sitios web. El hosting web aloja los contenidos de tu web y tu correo electrónico para que puedan ser visitados en todo momento desde cualquier dispositivo conectado a Internet.
- **Dominio:** Un dominio web es el nombre único que recibe un sitio web en internet. Este nombre identifica a una página web concreta sin que puedan existir dos o más sitios web que compartan el mismo nombre de dominio.
- **Backup de información:** Es una copia de seguridad o el proceso de copia de seguridad. Backup se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- **Antivirus:** Es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora. Una vez instalados, la mayoría del software antivirus se ejecutan automáticamente en segundo plano para brindar protección en tiempo real contra ataques de virus.

5. **DESARROLLO**

5.1. Gestor de Hosting Dominio y Correo Electrónico:

El Coordinador de Hosting, Dominio y Correos realiza el servicio de mantenimiento, monitoreo del hosting y dominio, backups de información en el hosting.

Valida el requerimiento de la solicitud de correo en el **FOR.035 Formato de información de personal nuevo y entrega de equipo.**

Crea nuevo correo en el cpanel según lo detallado en el documento INS.003 – Creación de nuevo correo en CPANEL

Configura correo electrónico en el equipo del usuario.

Configura y archiva de correos, creación de carpeta pst en el equipo del usuario.

Realiza baja de correos, según instructivo INS.008 – Eliminación de Correo

Realiza backups de correos desde Webmail, según instructivo INS.004 – Backups de Correo

Realiza mantenimiento buzón de correos en servidor, según instructivo INS.009 – Mantenimiento de buzón de correos en el servidor.

5.2. Gestor de Soporte Técnico:

El Coordinador de Hosting, Dominio y Correos atiende a las consultas de apoyo de los clientes

Administra software y herramientas de asistencia técnica.

Realiza diagnóstico y solución de problemas de los clientes.

Está pendiente de la actualización de los productos y servicios de la empresa.

Realiza instalación y configuración de equipos de cómputo.

Realiza mantenimiento Preventivo de equipos de cómputo, según instructivo INS.005 – Mantenimiento preventivo de equipo de cómputo.

Registra y Controla Compromisos de Seguridad de la Información a los usuarios, según instructivo FOR.036– Compromiso de seguridad de la información.

8. Operación

8.1 Planificación y control operacional

	PROCEDIMIENTO	Código: PRO.011	
	GESTIÓN DE PROVEEDORES	Fecha: 8/03/2021	Versión: 2
		Página 1 de 3	

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para la selección, evaluación, contratación y re-evaluación de proveedores, contratistas y contratación externa que presten servicios a Core Business Corp (CBC).

2. **ALCANCE**

Aplica a todos los proveedores que presten los servicios de capacitación externa, auditoría, inspecciones, asesorías y procesos internos.

3. **REFERENCIAS**:

- ISO 9001:2015. Requisitos de un Sistema de Gestión de Calidad.
- ISO 45001: 2018: Sistema de Seguridad y Salud en el Trabajo.
- ISO 27001:2013: Sistema de Seguridad de la información.

4. **DEFINICIONES**

- **Proveedor interno**: Persona que presta servicios a los procesos internos de CBC.
- **Proveedor externo**: Persona que brindan servicios a los clientes a nombre de CBC.
- **Servicio interno**: Proyectos o servicio constante que un proveedor realiza a los procesos internos de CBC.

5. **DESARROLLO**

5.1. Análisis de necesidad de servicio

El Business Partner realiza el análisis de necesidad según proceso, actividad, servicio a brindar y nivel de criticidad, estas son:

Procesos Operativos - Actividad	Servicio	Criticidad
Capacitación	Interno, Tercerizado	Alto
Eco-Learning	Tercerizado	Alto
Auditorías	Interno, Tercerizado	Alto
Inspección	Interno, Tercerizado	Alto
Asesoría	Interno, Tercerizado	Alto

Procesos de Apoyo - Actividad	Servicio	Criticidad
Página web	Tercerizado	Medio
Contabilidad	Tercerizado	Medio

5.2. Búsqueda selección de proveedor

El Business Partner realiza la búsqueda de especialistas en el mercado, según perfil, necesidad del cliente y proyecto interno.

Solicita el curriculum documentado y/o declaración jurada. Selecciona a los proveedores de acuerdo con el cumplimiento del perfil de búsqueda.

8. Operación

8.2 Evaluación de los riesgos de seguridad de la información

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
				efectos de la contaminación														
Instalaciones / Data Center	INSTALACIONES	AME028	TERREMOTO (SISMOS)	Sede ubicada en zona sísmica / Fallas estructurales de las instalaciones	2			5	5	10	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	5	7
	INSTALACIONES	AME029	ATAQUE DESTRUCTIVO (VANDALISMO, TERRORISMO, ACCIÓN MILITAR,...)	Inseguridad en el contexto social	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	5	1
	INSTALACIONES	AME030	INCENDIO	No se tienen extintores ni sistema contra incendio / Tomas eléctricas en mal estado	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	4	3
	INSTALACIONES	AME031	INUNDACIÓN	Conexiones de agua dentro del área de procesamiento de datos	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	5	4	12
	INSTALACIONES	AME032	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

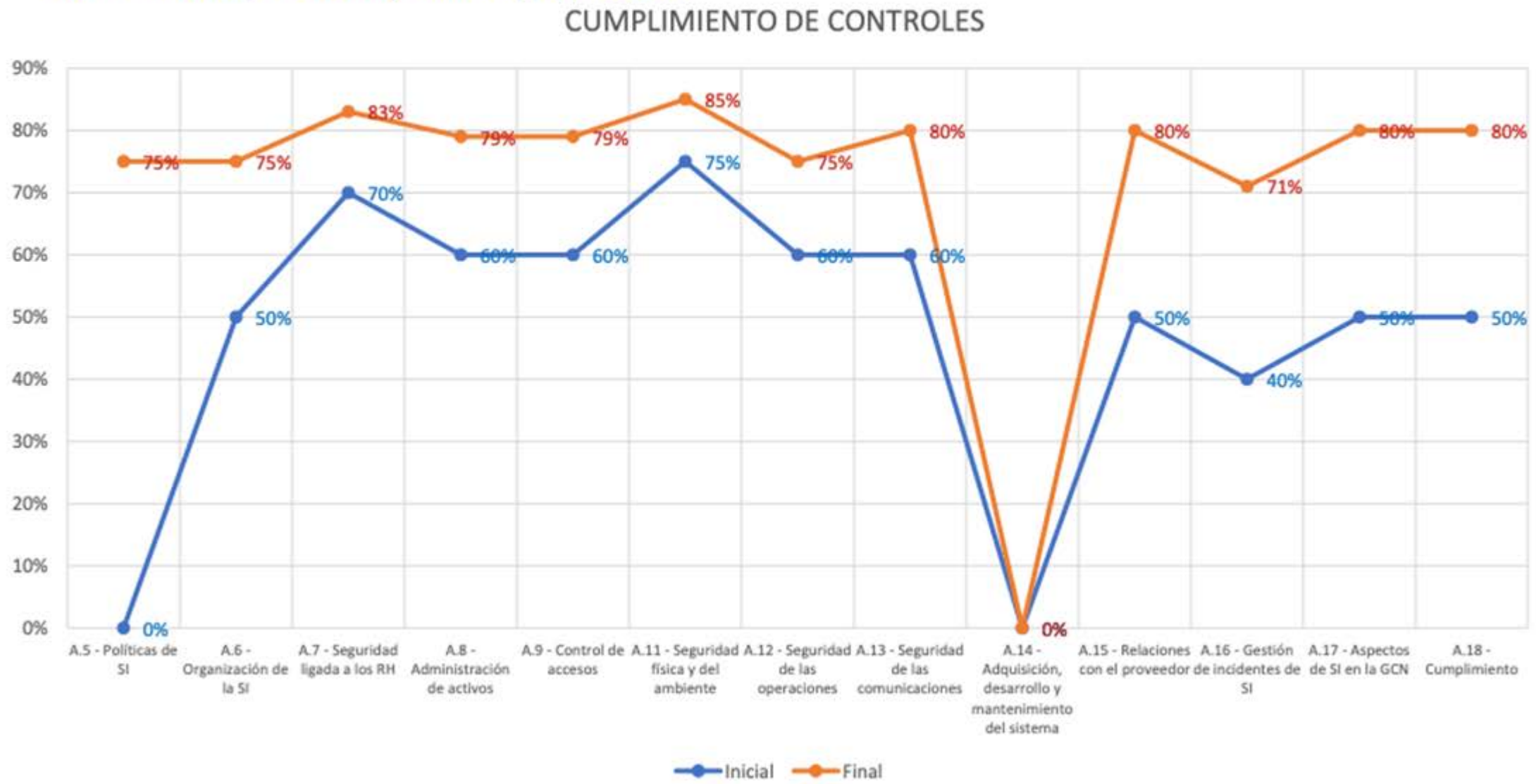
9. Evaluación de desempeño

9.1 Monitoreo, medición, análisis y evaluación

Política	Objetivo	Indicadores	Meta	Formato / Fuente de datos	Frecuencia de medición	Responsable
Preservar la confidencialidad, integridad y disponibilidad de la información de nuestras partes interesadas.	Controlar los riegos de información en los proceso de la empresa	RIESGOS SI. Control operacional: (N° acciones ejecutadas del Control Operacional del RIEGOS SI/ Total de acciones) x 100%	70%	Matriz de RIESGOS SI	Mensual	Procesos SIG/ Business Parte
	Controlar las amenazas en la seguridad de la información	% de ataques informáticos que impidieron la prestación de algún servicio	0	Registros de incidencias	Mensual	Procesos SIG/ Business Parte

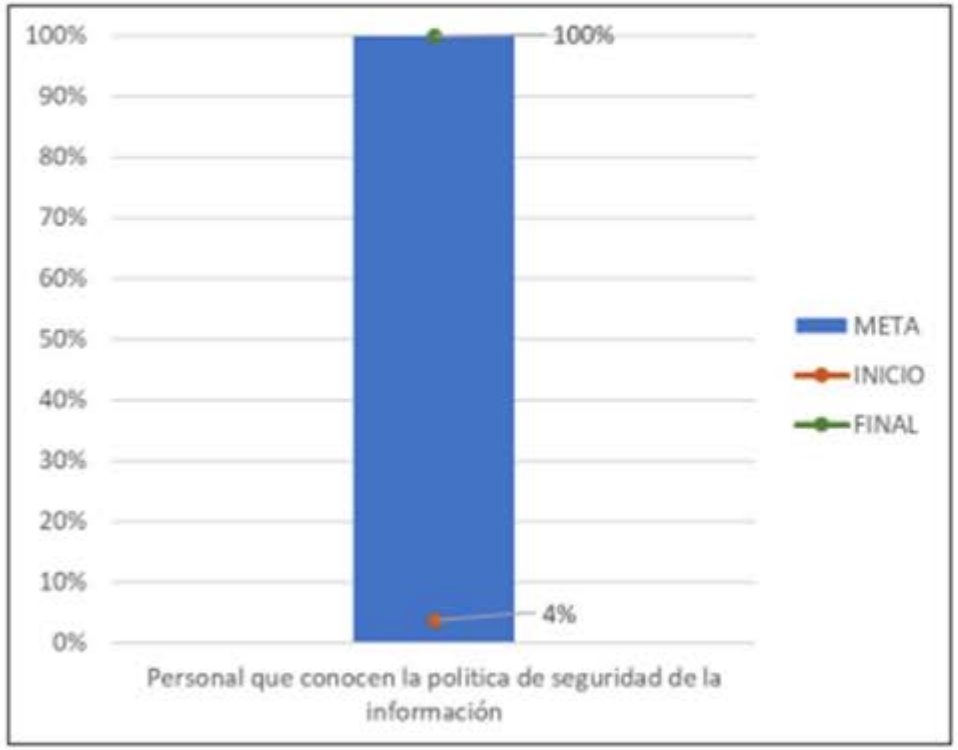
9. Evaluación de desempeño

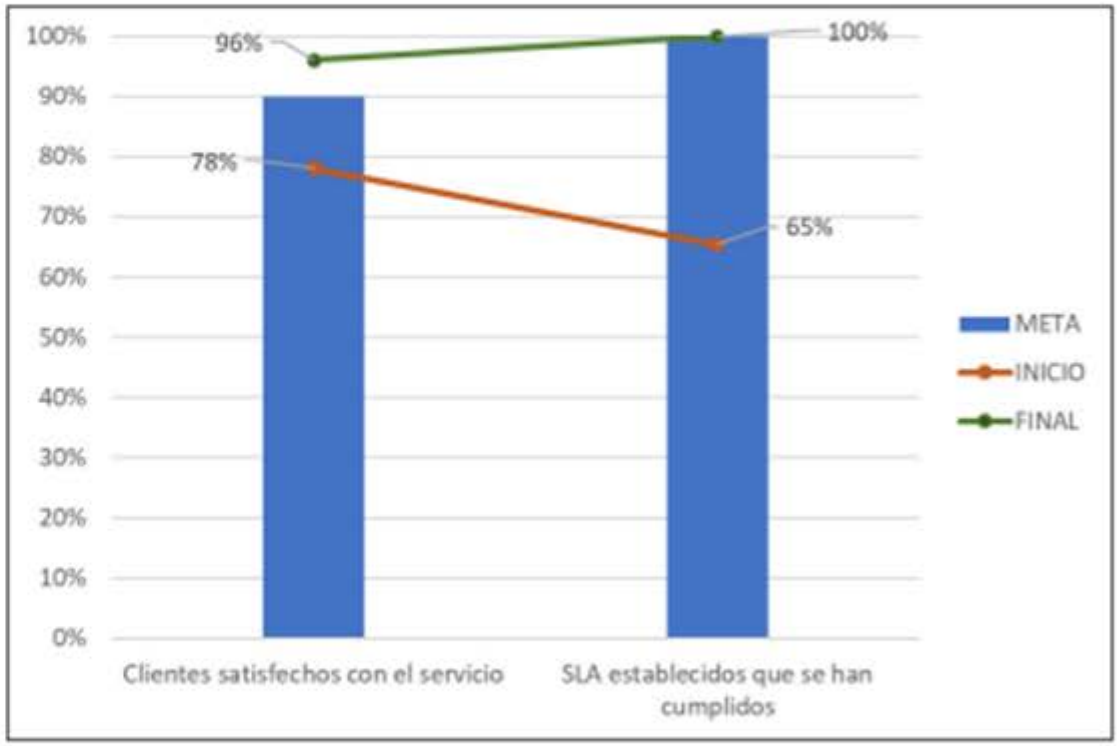
9.1 Monitoreo, medición, análisis y evaluación



9. Evaluación de desempeño

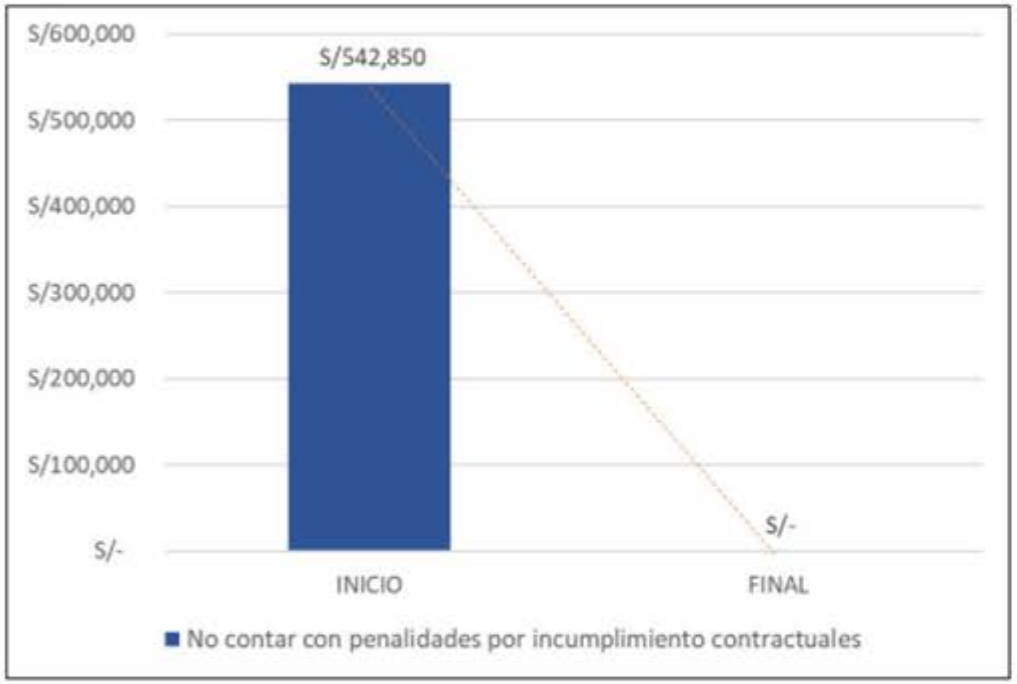
9.1 Monitoreo, medición, análisis y evaluación

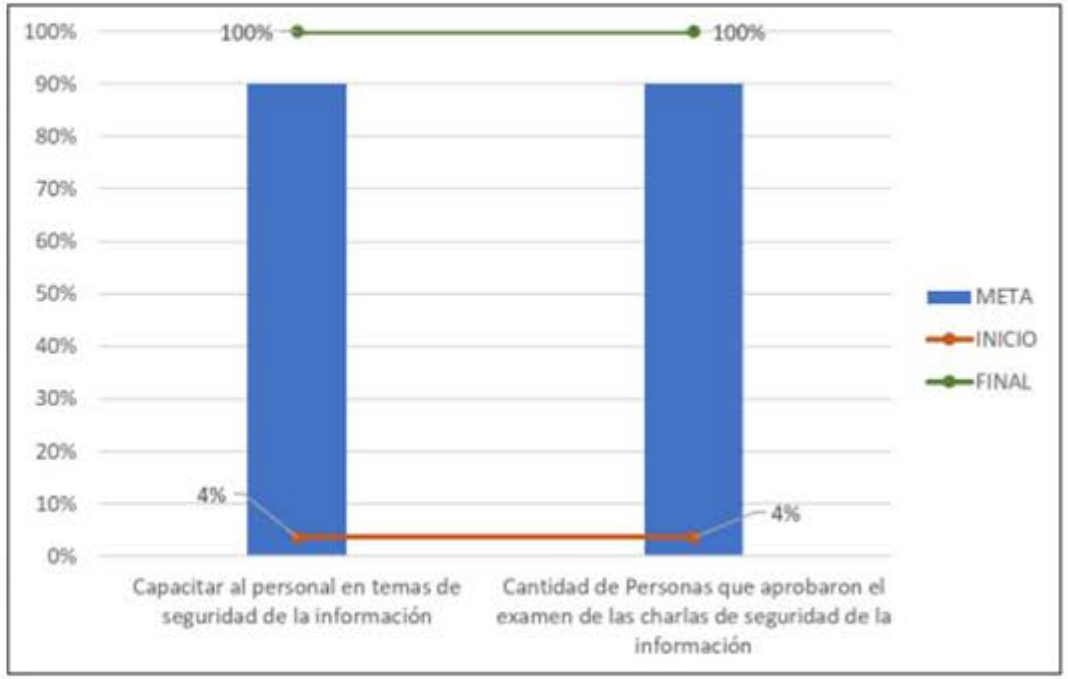




9. Evaluación de desempeño

9.1 Monitoreo, medición, análisis y evaluación





9. Evaluación de Desempeño

9.2 Auditoría Interna

PLAN DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2022	
Auditor Líder: Julio Pereyra **Equipo Auditor**: No aplica **Especialista**: No aplica **Auditor en Entrenamiento**: No aplica	**Fecha de Inicio**: 22.8.2024 **Fecha de Finalización:** 22.8.2024 **Día de Informe**: 26.8.2024 **Norma a auditar**: ISO 27001:2022

Objetivos de la Auditoría: • Verificar el cumplimiento de los requisitos de las Normas ISO 27001:2015 • Verificar el cumplimiento de los requisitos legales • Verificar el cumplimiento de los requisitos inherentes al servicio
Metodología: Entrevista y muestreo
Criterios de auditoría: Documentación del sistema de gestión de seguridad de la información, regulatorio, normativo y propios de la organización; a través de muestreo, observación y entrevista.
Alcance: Consultoría y outsourcing en aplicaciones informáticas empresariales: implementación, desarrollo de software, outsourcing, soporte y mesa de ayuda.

9. Evaluación de Desempeño

9.2 Auditoría Interna

Horario	Proceso/ Área a Auditar	Requisitos de las Normas Aplicables	Responsable del área auditada	Auditor
		ISO 27001:2022		
09:00 a 09:15	Reunión de apertura			Julio Pereyra
09:15 a 10:00	Gestión Estratégica	4.1,4.2,4.3,4.4,5.1,5.2,5.3,6.1,7.1,9.1, 9.3,10.1,10.2	Gerente General	Julio Pereyra
10:00 a 11:00	Sistema de gestión de la seguridad de la información	4.1,4.2,4.3,4.4,5.2,5.3,6.1,6.2,6.3, 7.3, 7.4,7.5,9.1, 9.2,10.1,10.2	Responsables del SIG	Julio Pereyra
11:00 a 12:00				
12:00 a 12:30	Gestión de innovación y marketing	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2,8.3, 9.1,10.1,10.2	Gerente de Innovación y marketing	Julio Pereyra
12:30 a 13:00	Gestión comercial	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2, 8.3,9.1,10.1,10.2	Gerente Comercial	Julio Pereyra
13:00 a 14:00	Almuerzo			
14:00 a 14:30	Gestión de Telecomunicaciones	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2, 9.1,10.1,10.2	Gerente de Consultoría	Julio Pereyra
14:30 a 15:00	Gestion de Eventos y Respaldo	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2,8.3, 9.1,10.1,10.2	Gerente de Desarrollo	Julio Pereyra
15:00 a 15:30	Logística	4.4,5.2,5.3,6.1,6.3, 7.1, 7.3, 7.4,7.5,8.1, 8.2,8.39.1,10.1,10.2	Gerente de Administraciónn y Trasformación Digital	Julio Pereyra
15:30 a 16:00	Gestión de Mesa de Ayuda	4.4,5.2,5.3,6.1,6.3, 7.1, 7.3, 7.4,7.5,8.1,8.2.8.3, 9.1,10.1,10.2		
16:00 a 17:00	Talento Humano	4.4,5.2,5.3,6.1,6.3, 7.1, 7.2,7.3, 7.4,7.5,8.1,8.2,8.3 , 9.1,10.1,10.2	Gerente de Talento Humano	Julio Pereyra
17:00 a 17:15	Consolidación de hallazgos			
17:15 a 17:45	Reunión de cierre			

Auditor Líder

Gerente

9. Evaluación de Desempeño

9.3 Revisión por la dirección

Entradas

a. Estado de las Revisiones por la Dirección previas

b. Cambios en cuestiones internas y externas

c. Cambios en necesidades y expectativas de P.I.

d. Información sobre el comportamiento de la S.I.:

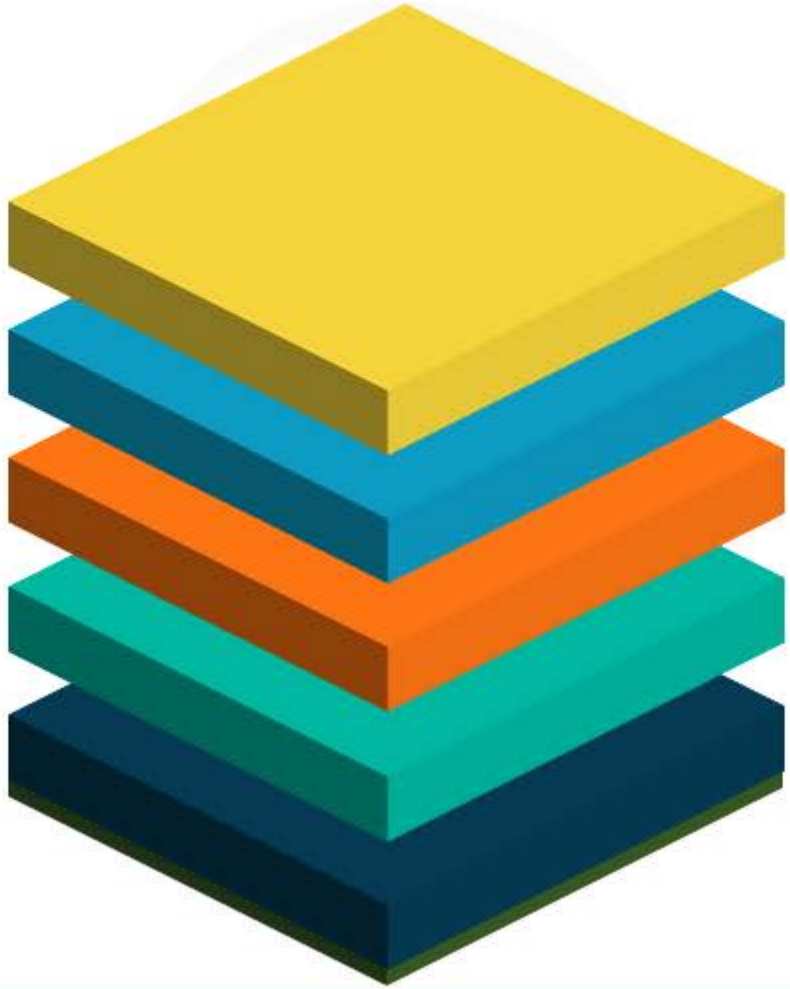
Tendencias:

- No conformidades y acciones correctivas.
- Seguimiento y resultados de la evaluación de la medición.
- Resultado de auditorías
- Cumplimiento de los objetivos de S.I.

e. Comentarios de las partes interesadas

f. Resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.

g. Oportunidades de mejora



Resultados

Oportunidades de mejoramiento continuo

Cualquier necesidad de cambio en el SGSI

9. Evaluación de Desempeño

9.3 Revisión por la dirección

Tabla 1 Incidentes de Seguridad Atendidos Vs Reportados

Tabla2 Histórico de incidentes y peticiones

9. Evaluación de Desempeño

9.3 Revisión por la dirección

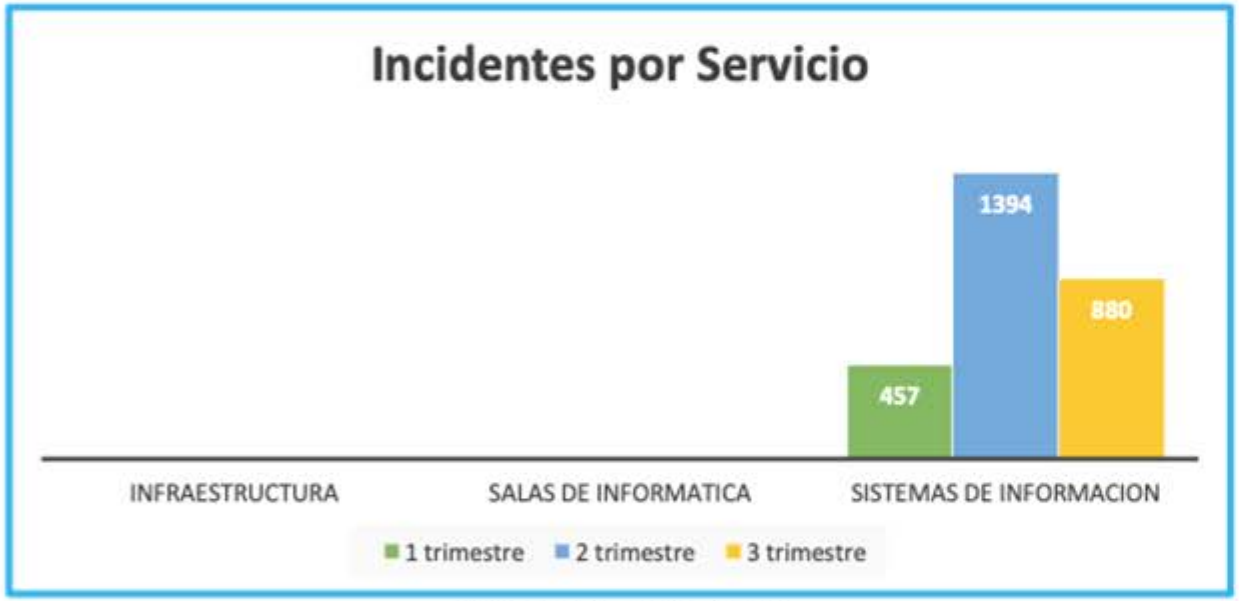


Tabla5 Incidentes por servicio

Tabla7 Histórico Satisfacción de usuarios

9. Evaluación de Desempeño

9.3 Revisión por la dirección

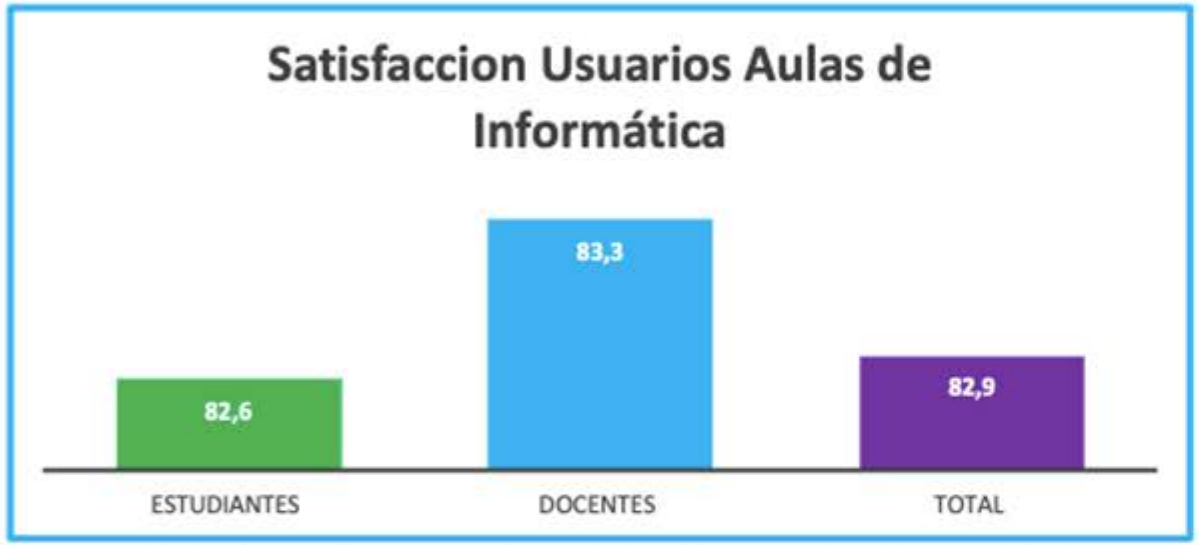


Tabla 8 Satisfacción de usuarios Aulas de Informática (los datos se encuentran en %)

No	Nombre del indicador	Frecuencia	Meta	1º Semestre 2021	2º Semestre 2021	1º Semestre 2022	2º Semestre 2022
1	Cumplimiento de los acuerdos de nivel de servicio	Semestral	80%	100%	100%	100%	
2	Satisfacción de usuarios de los acuerdos informáticos	Semestral	80%	100%	100%	100%	

Tabla 9 Resultados Indicadores

9. Evaluación de Desempeño

9.3 Revisión por la dirección

	# Activos	INACTIVOS	ACTIVOS	OBSOLETOS	CRITICOS
HARDWARE	1557	0	1557	0	1
SOFTWARE	149	5	138	2	8
INFORMACIÓN	3	0	3	0	1
SERVICIOS	33	0	33	0	0
RECURSO HUMANO	47	4	43	0	0
TOTAL ACTIVOS	**1789**	**9**	**1778**	**2**	**10**

9. Evaluación de Desempeño

9.3 Revisión por la dirección

En 2022, A partir de la identificación de activos de información, se trabajó en el análisis e identificación de riesgos de los diez (10) activos de información que fueron valorados como ALTO, siguiendo el procedimiento A-RI-P35, por lo tanto, se realizó Plan de Tratamiento a algunos de estos activos los cuales son:

- Servidor LDAP (2020)
- Servidor SIIUPS (2020)
- A-RI-P35-F01 (2022)
- Mesa de Servicio Institucional (2022)

Respecto a los activos de información aplicativo GOOBI y esquema GOOBI, no se realizó plan de tratamiento, debido a que se determinó que se asume el riesgo de acuerdo al análisis y evaluación de riesgos realizada.

Como resultado, se obtiene un nivel de riesgo Alta y cinco niveles de riesgo Moderada.

Se destaca que los controles implementados a partir de la operación del SGSI, han eliminado el número de riesgos que se tenían en extremo; esto evidencia que los controles han sido efectivos permitiendo disminuir los niveles de los riesgos residuales.

9. Evaluación de Desempeño

9.3 Revisión por la dirección

En cuanto a los cambios que pueden afectar al Sistema de Gestión de Servicios de TI y Sistema de Gestión de Seguridad de la Información se identificaron los siguientes:

- La desvinculación o no continuidad de personal en la Dirección afecta negativamente la prestación de los servicios, generando atrasos o el incumplimiento de los acuerdos de niveles de servicio con los usuarios.

- La vinculación de personal no capacitado o sin experiencia en programación o manejo de herramientas avanzadas como SPRING, ANGULAR u ORACLE, genera demora en el desarrollo de aplicaciones y cumplimiento de condiciones seguras en el desarrollo.

- Por falta de interés por parte de la alta dirección en el cumplimiento de las normas ISO 20000-1 e ISO 27001 se pueden presentar

    - La poca toma de conciencia de la comunidad
    - Desacato a los requisitos de la norma
    - Incumplimiento a los requisitos de la norma
    - Fallas en los procedimientos
    - Afectación en la prestación de los servicios
    - Daño en la infraestructura tecnológica y no contar con el respaldo requerido
    - Perdida de le certificación
    - Detrimento patrimonial por la pérdida de las certificaciones de las nomas internaciones ocasionando una mala imagen a nivel regional y nacional de la universidad

- Por falta de recursos no se pueda dar cumplimiento a la ejecución de los proyectos que se encuentran estipulados en el Plan de Desarrollo Institucional.

- Respaldo de personal indispensable para el desarrollo de procedimientos críticos de la Dirección

10.Mejora

10.1 Mejora Continua

	OPORTUNIDAD DE MEJORA	OBJETIVO	ORIGEN	CONVENIENCIA					¿Es conveniente?	Sede o filiales	Acciones a tomar	RESPONSABLE DE LA OPORTUNIDAD DE MEJORA	¿Es ADECUADA la Oportunidad de Mejora? (avances en campo)	¿Es EFICAZ la Oportunidad de Mejora? (en base al Objetivo)	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
				Objetivos SGSI	Partes Interesad	Impacto en los riesgos	Mejora Continua	Total																	
1	Adecuar la Matriz de Riesgos del SGSI a TODAS las Filiales.	Reducir la detección de no conformidades y riesgos del SGSI en las filiales	Auditoría externa 2023	2	2	2	3	9	Si	Cusco, Arequipa, Lima, Huancayo	1. Actualizar el AMFE 2. Difundir el AMFE actualizado	Coordinador del SGSI	1. Se identificó todos los riesgos por cada sede / filial. 2. Los trabajadores participaron en los cursos de capacitación	A través de una auditoria seguimiento (vía remota), se verificó que todas las sedes y filiales identificaron sus riesgos											
2	Revisar la factibilidad de cambiar las metas, ya que las actules se mantienen en permanente cumplimiento en los últimos 6 meses.	Aumentar el compromiso y la toma de conciencia en el personal, sobre la mejora continua	Auditoría externa 2023	3	1	2	3	9	Si	Cusco, Arequipa, Lima, Huancayo	1. Generar el informe de resultados 2. Realizar la planificación en función a los datos obtenidos	Responsables de procesos y filiales	Se realizaron reuniones de revisión de nueva metas. Para el caso del proceso de gestión de accesos, se ha reducido la meta de indice de eventos de 10 a 5 (medido a nivel mensual)	Se mantienen las nuevas metas cumplidas y en proceso de mejora para el periodo 2024											
3	Integrar / reducir el número de instructivos en la operación, ya que a la fecha existe 134 documentos en calidad de instrucciones / instructivos de trabajo.	Mejorar la trazabilidad de las actividades operativas en el SGSI	Revisión por la Dirección Dic 2023	2	2	1	3	8	Si	Cusco, Arequipa, Lima, Huancayo	Los requisitos documentarios son los mínimos requeridos y se plasma así en el procedimiento.	Responsables de procesos y filiales	De 134 documentos (instructivos) se ha reducido a 77. Los cuales son especificamente operativo y cn su respectiva integración de formatos / registros.	Se ha verificado que se han reducido las no conformidades por causa de poca disponibilidad a los documentos y el personal mantiene conocimiento mas oportuno											
4	Revisar la velocidad y disponibilidad de los sistemas de información, se indicó que en ocasiones el sistema es lento. (Esto podría afectar a la gestión de indicadores , gestión de pedidos de emergencia y el FODA).	Mantener eficaz el desarrollo de la información y registros del SIG.	Sugerencias del personal	1	1	2	3	7	No	No aplica	No aplica	No aplica	No aplica	No aplica											

10. Mejora

10.2 Conformidades y acciones correctivas

Origen de la No Conformidad		Proceso / Lugar en donde se detectó la No Conformidad
Reclamo		Operaciones () Gestión de Activos () Ingeniería ()
Salida No Conforme		
Incumplimiento de Procedimientos Misionales		Gestión de Mesa de Ayuda (x) Gestión de Telecomunicaciones ()
Incumplimiento de Procedimientos del SGSI		
Incumplimiento de Metas de Indicadores		**Persona quien detecta la No Conformidad**
Seguimiento y Evaluación de Proveedores		Coordinador del SGSI
Auditoria Interna	x	
Auditoria Externa		
Otros :		

DECRIPCIÓN DE LA NO CONFORMIDAD

Incumplimiento:

No se almacena la documentación del proceso de gestión de Mesa de Ayuda.

Evidencia:

Se solicitó al responsable del proceso los siguientes registros:

a. REG-SGSI-004 Registro de eventos
b. REG-SGSI-005 Registro de Seguimiento de eventos
c. REG-SGSI-008 Reporte de Evento Mensuales

De acuerdo con el REG-SGSI-002 Lista de Registro se menciona que los respectivos registros (descritos en líneas arriba) se deben almacenar a 12 meses, 18 meses y 6 meses respectivamente. Se solicitó las siguientes evidencias:

a. REG-SGSI-004 Registro de eventos (del periodo: diciembre 2023 y enero 2024). No se presentó evidencias.
b. REG-SGSI-005 Registro de Seguimiento de eventos (del periodo: noviembre 2023 y marzo 2024). No se presentó evidencias.
c. REG-SGSI-008 Reporte de Evento Mensuales (del periodo: enero 2024 y febrero 2024). No se presentó evidencias

REQUISITO: 7.5.3 Control de la información documentada (acápite d)

Generado por : Irwin Damasco Gogin **Responsable de Área :** Aquiles Zine

ACCIÓN (ES) INMEDIATA (S) (acción que elimina la no conformidad)

Búsqueda y almacenamiento de los registros solicitados. Ordenamiento integral del almacenamiento de los registros.

Responsable (s) de Acción (es) Inmediata (s): Aquiles Zapata

EVALUACIÓN DE NECESIDAD DE ACCIÓN CORRECTIVA

¿Es necesaria la implementación de acciones correctivas?

Si (x) No () ¿por qué?

Los registros solicitados son de alto impacto para el seguimiento de los resultados del sistema de gestión de seguridad de la información (gestión de eventos)

Responsable (s) de la Evaluación: Aquiles Zapata

ANÁLISIS DE CAUSAS (describir las principales causas de la no conformidad)

1. **¿Por qué no se ubicaron los registros seleccionados?**

   Respuesta: Se evidencio que no existen criterios de orden para el almacenamiento físico de registros.

2. **¿Por qué no existen criterios de orden para el almacenamiento de registros?**

   Respuesta: No se ha priorizado la identificación de métodos de almacenamientos físicos.

3. **¿Por qué no se ha priorizado la identificación de métodos de almacenamientos físicos?**

   Respuesta: Se desconoce metodología de almacenamiento físico de registros

Responsable (s) del Análisis de Causa (s) : Aquiles Zine / Gonzalo López

ACCIONES CORRECTIVAS

Descripción de Acción Correctiva	Responsable	Plazo	Plazo de Eficacia
1. Implementar la metodología de orden y limpieza en relación a las 5 S.	Karla Mullén	Inmediato	3.5.2024

VERIFICACIÓN DE LA EFICACIA DE ACCIONES CORRECTIVAS (llenado por el Coordinador del SGSI)

Verificación: Al día 3.05.2024, se realizó la revisión de los siguientes registros en el proceso de gestión de Mesa de Ayuda:

a. REG-SGSI-004 Registro de eventos (del periodo: octubre 2023). Se evidencia los registros.
b. REG-SGSI-005 Registro de Seguimiento de eventos (del periodo: febrero 2024). Se evidencia los registros.
c. REG-SGSI-008 Reporte de Evento Mensuales (del periodo: marzo2024). Se evidencia los registros.

La acción correctiva implementada ha sido eficaz.

Fecha: 3.5.2024.

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón