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 03

Mg. Ing. Julio Pereyra Rosales

1. Gestión de comunicación y documentación

7. Soporte

7.4 Comunicación

TITULO QUE COMUNICAR	ASUNTO (SUBJECT) QUE COMUNICAR	DIRIGIDO POR QUIEN DEBE COMUNICAR	DIRIGIDO A / O (ROLES) A QUIEN COMUNICAR	FECHA DE INICIO CUANDO COMUNICAR	USO DEL CANAL CANAL DE COMUNICACIÓN	SETIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMRE			
						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

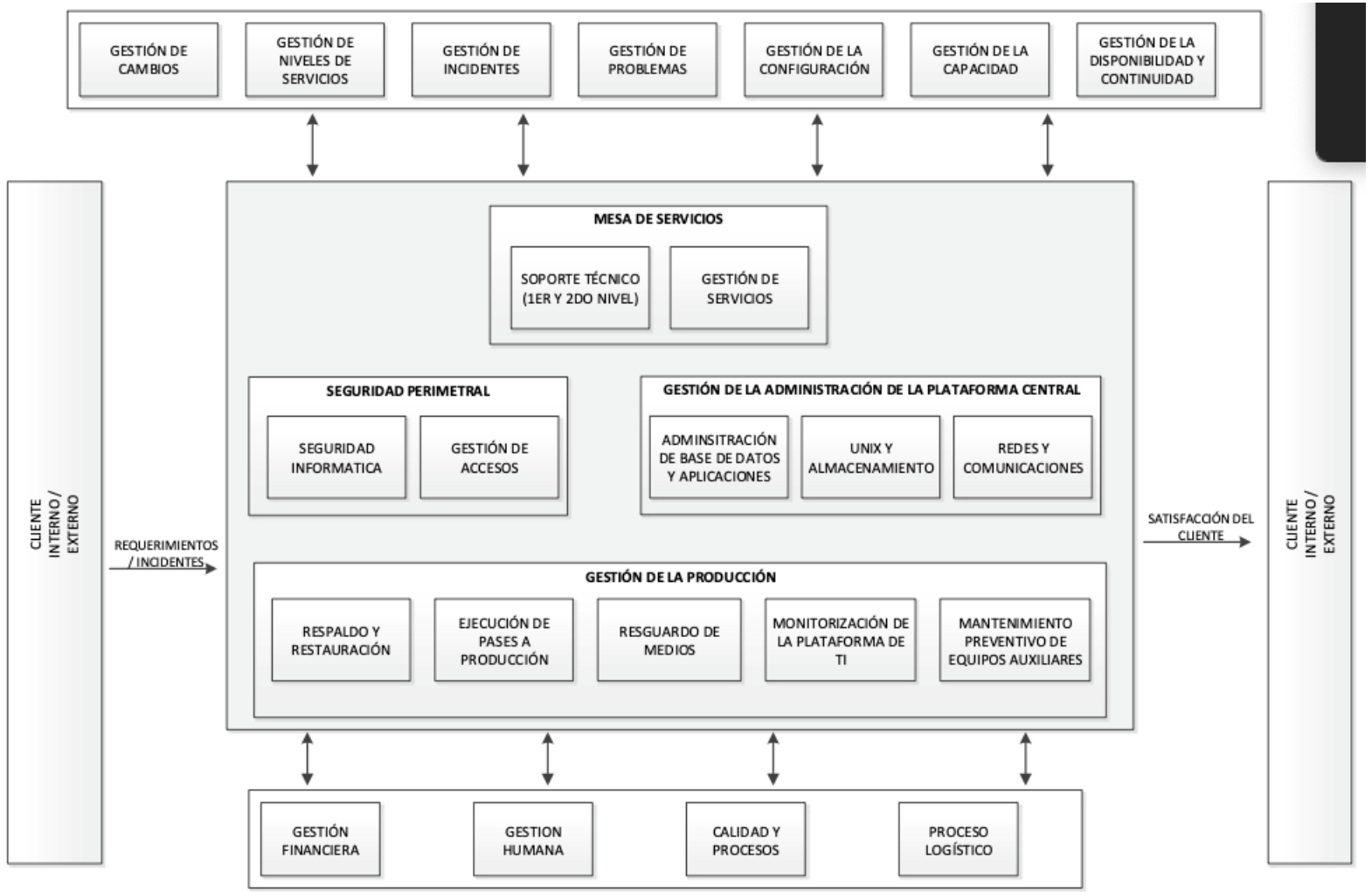
FORMATOS
FOR.GER.001 Compromiso de confidencialidad
FOR.GER.002 Declaración Jurada
FOR.GER.003 Lista de personal
FOR.GER.004 Entrega de cargo
FOR.GER.005 Plan de capacitación del personal
FOR.GER.006 Plan de Contingencia
FOR.GER.007 Lista de asistencia
FOR.GER.008 Lista maestra de documentos
FOR.GER.009 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

2. Gestión de Operaciones

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

Core Business Corp	PROCEDIMIENTO	Código: PRO.009	
	GESTIÓN DE R.R.H.H	Fecha: 24/11/2021	Versión: 4
		Página 1 de 5	

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	
Core Business	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 auditoria, 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	
Core Business	INFRAESTRUCTURA TECNOLOGICA	Fecha: 08/03/2021	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, backup 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 backup de correos desde Webmail, según instructivo INS.004 – Backup 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	
Core Business Corp	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

8.1 Planificación y control operacional

A5 Controles Organizacionales

Objetivo: Lograr que la actitud integral de la organización hacia la protección de datos sea una amplia gama de políticas, reglas, procesos, procedimientos, estructuras organizacionales y comportamientos individuales.

- 5.1 Políticas de seguridad de la información.
- 5.5.2 Funciones y responsabilidades de seguridad de la información.
- 5.3 Segregación de funciones.
- 5.4 Responsabilidades de la gerencia.
- 5.5 Contacto con autoridades.
- 5.6 Contacto con grupos de interés especial.
- 5.7 Inteligencia sobre amenazas.
- 5.8 Seguridad de la información en la gestión de proyectos.
- 5.9 Inventario de información y otros activos asociados.
- 5.10 Uso aceptable de la información y otros activos asociados.
- 5.11 Devolución de activos.
- 5.12 Clasificación de la información.
- 5.13 Etiquetado de Información.
- 5.14 Transferencia de información.
- 5.15 Control de acceso.
- 5.16 Gestión de identidad.
- 5.17 Información de autenticación.
- 5.18 Derechos de acceso.
- 5.19 Seguridad de la información en las relaciones con proveedores.
- 5.20 Abordar la seguridad de la información en los acuerdos con proveedores.
- 5.21 Gestión de la seguridad de la información en la cadena de suministro de TIC.
- 5.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores.
- 5.23 Seguridad de la información para el uso de servicios en la nube.
- 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.
- 5.25 Evaluación y decisión sobre eventos de seguridad de la información.
- 5.26 Respuesta a Incidentes de seguridad de la información.
- 5.27 Aprender de los incidentes de seguridad de la información.
- 5.28 Recolección de evidencia.
- 5.29 Seguridad de la información durante una interrupción.
- 5.30 Preparación de las TIC para la continuidad del negocio.
- 5.31 Requisitos legales, estatutarios, reglamentarios y contractuales.
- 5.32 Derechos de propiedad intelectual.
- 5.33 Protección de registros.
- 5.34 Privacidad y protección de la PII.
- 5.35 Revisión independiente de la seguridad de la información.
- 5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la Información.
- 5.37 Procedimientos operativos documentados.

8. Operación

8.1 Planificación y control operacional

A6 Controles Orientados a las Personas

Objetivo: Definir cómo los empleados interactúan con los datos y entre sí, la empresa puede regular el componente humano de su programa de seguridad de la información. En este conjunto de controles se incluyen la seguridad del personal, la gestión del capital humano y la formación y sensibilización.

- 6.1 Detección.
- 6.2 Términos y condiciones de empleo.
- 6.3 Concientización, educación y capacitación sobre seguridad de la información.
- 6.4 Proceso disciplinario.
- 6.5 Responsabilidades después de la terminación o cambio de empleo.
- 6.6 Acuerdos de confidencialidad o no divulgación.
- 6.7 Trabajo remoto.
- 6.8 Informes de eventos de seguridad de la información.

A7 Controles Físicos

Objetivo: Garantizar la seguridad de los activos tangibles, como sistemas de entrada, procesos de disposición de activos y políticas claras de escritorio. Estos son esenciales para la preservación de la confidencialidad.

- 7.1 Perímetros de seguridad física.
- 7.2 Entrada física.
- 7.3 Protección de oficinas, habitaciones e instalaciones.
- 7.4 Monitoreo de seguridad física.
- 7.5 Protección contra amenazas físicas y ambientales.
- 7.6 Trabajar en áreas seguras.
- 7.7 Limpiar escritorio y limpiar pantalla.
- 7.8 Ubicación y protección del equipo.
- 7.9 Seguridad de los activos fuera de las instalaciones.
- 7.10 Medios de almacenamiento.
- 7.11 Utilidades de soporte.
- 7.12 Seguridad del cableado.
- 7.13 Mantenimiento del equipo.
- 7.14 Eliminación segura o reutilización del equipo.

8. Operación

8.1 Planificación y control operacional

A8 Controles Tecnológicos

Objetivo: Garantizar que las regulaciones y procedimientos digitales de la empresa cumplan con criterios de configuración, administración y acceso para que la tecnología no presente huecos de seguridad ya sea por acceso no autorizados, fallas de funcionamientos o por mala administración.

- 8.1 Dispositivos terminales de usuario.
- 8.2 Derechos de acceso privilegiado.
- 8.3 Restricción de acceso a la información.
- 8.4 Acceso al código fuente.
- 8.5 Autenticación segura.
- 8.6 Gestión de capacidad.
- 8.7 Protección contra *malware*.
- 8.8 Gestión de vulnerabilidades técnicas.
- 8.9 Gestión de configuración.
- 8.10 Eliminación de información.
- 8.11 Enmascaramiento de datos.
- 8.12 Prevención de fuga de datos.
- 8.13 Copia de seguridad de la información.
- 8.14 Redundancia de las instalaciones de procesamiento de información.
- 8.15 Registro.
- 8.16 Actividades de seguimiento.
- 8.17 Sincronización de reloj.
- 8.18 Uso de programas de utilidad privilegiados.
- 8.19 Instalación de software en sistemas operativos.
- 8.20 Seguridad de redes.
- 8.21 Seguridad de los servicios de red.
- 8.22 Segregación de redes.
- 8.23 Filtrado web.
- 8.24 Uso de criptografía.
- 8.25 Ciclo de vida de desarrollo seguro.
- 8.26 Requisitos de seguridad de la aplicación.
- 8.27 Principios de ingeniería y arquitectura de sistemas seguros.
- 8.28 Codificación segura.
- 8.29 Pruebas de seguridad en desarrollo y aceptación.
- 8.30 Desarrollo subcontratado.
- 8.31 Separación de los entornos de desarrollo, prueba y producción.
- 8.32 Gestión de cambios.
- 8.33 Información de prueba.
- 8.34 Protección de los sistemas de información durante las pruebas de auditoría.

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón