TRABAJO DE GRADO
Opción Práctica y Pasantía.

Auditoría al control interno de los archivos planos de nómina.

Corporación Universitaria Remington.
Facultad ciencias contables.
Contaduría Pública.

Manuela Marín García.
Olga Liliana Londoño Baena.
Validación de Funciones
2023.

Agradecimientos

A Dios, por permitirme desarrollar mis capacidades, ser refugio en cada situación frustrante y ser guía para cada decisión tomada.

A mi Familia, que ejercen de piedra angular, por estar, ofrecerme amor y un apoyo más que incondicional.

A mi Pareja, por ser ejemplo de superación, por enseñarme que la vida es bonita mientras día a día se trabaja desde nuestro ser.

A Docentes e Institución, por brindarme los conocimientos necesarios para lograr con éxito el objetivo de este proyecto.

1. Indice de Contenido

1. Indice de Contenido 3
2. Indice de Tablas 4
3. Indice de Figuras 5
4. Resumen 6
5. Problemática Abordada en la Práctica o Pasantía 8
6. Objetivos 10
6.1. Objetivo General 10
6.2. Objetivos Específicos 10
7. Metodología 11
8. Resultados. 14
8.1. A Quien Pueda Interesar: 14
8.2. Informe de Auditoría Interna 15
8.2.1. Objetivo de la Auditoría 15
8.2.2. Objetivos Específicos de la Auditoría 15
8.2.3. Alcance de la Auditoría 15
8.2.4. Criterios de la Auditoría 16
8.2.5. Metodología de la Auditoría 16
9. Desarrollo de la Auditoría. 17
9.1. Talento Humano Asociado al Proceso: 18
9.2. Descripción del Proceso 22
9.3. Mapa de Calor 28
10. Observaciones y Recomendaciones 31
11. Conclusiones. 32
12. Referencias 33
13. Anexos 34
13.1 Anexo 1 Política de Intercambio de Información 34
13.2. Anexo 2 Política Corporativa de Seguridad de la Información 42
13.3. Anexo 3 Seguridad de la Información 61
13.4. Anexo 4 Manual de Cumplimiento de Políticas de Seguridad de la Información 74

2. Indice de Tablas

Tabla 1 Distribución del Personal por Áreas 12
Tabla 2 Análisis Perfil Profesional. 20
Tabla 3 Matriz de Riesgo y Mapa de Proceso 28

3. Indice de Figuras

Figura 1 Ubicación Sede Principal. Fuente Propia Manuela Marin, 26 de octubre 2023..... 8
Figura 2 Nivel de Educación. Fuente Propia Manuela Marin, 30 de Octubre 2023..... 21
Figura 3 Sección Archivo Plano en Software. Fuente Software Gosem, 01 de Noviembre 2023.22
Figura 4 Archivo Plano (PAB) Cifrado en ZIP. Fuente Propia Manuela Marin, 01 de noviembre 2023..... 23
Figura 5 Aplicativo I Service. Fuente Aplicativo Interno, 01 de noviembre 2023..... 23
Figura 6 Correo a Contabilidad y Tecnología. Fuente Correo Gmail, 01 de Noviembre 2023.... 24
Figura 7 Formato Aceptado por Software ERP. Fuente Propia Manuela Marin, 01 de noviembre 2023..... 25
Figura 8 Software Ofima. Fuente Software Ofimática, 01 de Noviembre 2023. 26
Figura 9 Flujograma Proceso. Fuente Propia Manuela Marin, 06 de Noviembre 2023 27

4. Resumen

Un archivo de texto plano o simple (el nombre se origina por el hecho de ser archivos que carecen de formatos) contiene caracteres alfanuméricos que pueden ser: letras, números y puntuaciones sin ningún tipo de formato, es decir, sin estilo, tipo de letra, tablas entre otros. Son archivos de texto que son utilizados para almacenar información sin límite y no posee una estructura jerárquica, se pueden crear con facilidad en cualquier herramienta de editor de texto o en software y su uso se hace efectivo en cualquier área o campo como, por ejemplo en la informática a través de las configuraciones de sistemas, equipos y programas y en la contabilidad con el objetivo de compartir, almacenar e intercambiar información de manera ágil, sencilla y rápida, logrando reclutar todos los datos y registros en un solo lugar generando facilidad al momento de comprender, evaluar y entender la información.

Estos archivos planos o simples son una herramienta importante y muy útil en el área de la contabilidad porque permiten el intercambio de información financiera y contable entre diferentes programas o sistemas, facilitando registros y controles de las cifras y valores que ingresan y salen de la compañía Y/O empresa; ayudan a promover una correcta y eficiente administración y dominio del negocio apoyando el crecimiento y mejora empresarial.

Existen varios tipos de archivos de texto y entre los más usados o comunes se encuentran:

- TXT: El cual almacena texto sin formato.
- DOC - DOCX: Son archivos de texto del software de textos Microsoft Word.
- ODT: Documento del procesador de texto llamado OpenOffice Writer.
- RTF: Archivo de texto enriquecido.

La facilidad de estos archivos se da cuando permiten que la interacción sea completa, es decir, muchos de los archivos mencionados anteriormente tienen funciones y características adicionales que hacen de su uso una herramienta facilitadora; estos archivos pueden viajar o compartirse sin inconvenientes a través de internet, son archivos en los cuales varias personas pueden trabajar y adicionar información como una base compartida en un mismo archivo como también permiten ser evaluados para detectar errores, ortografía y gramática antes de realizar el cargue final a los sistemas contables o informáticos.

Palabras Claves

Herramienta, funcionabilidad, contabilidad, informática, intercambio.

5. Problemática Abordada en la Práctica o Pasantía

La empresa Contento BPS S.A ubicada en la ciudad de Medellín, es una empresa que cuenta con un aproximadamente de 1.500 empleados distribuidos en 4 sedes, Itagüí siendo la sede principal, la sede de naranjal ubicado en el centro de la ciudad de Medellín, 1 sede en Bogotá y 1 sede en la ciudad de Cali.

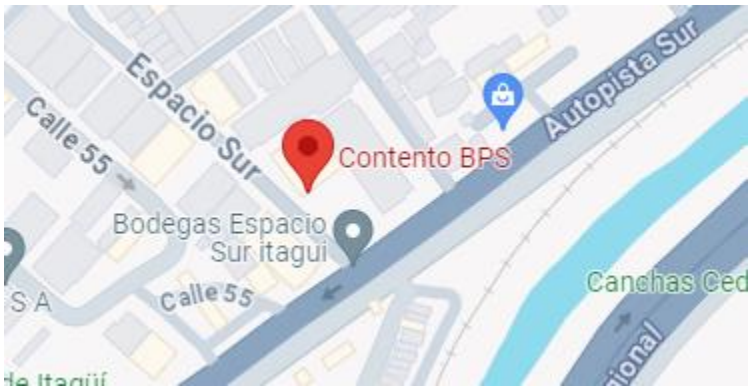

Figura 1 Ubicación Sede Principal. Fuente Propia Manuela Marin, 26 de octubre 2023.

Es una empresa donde su área administrativa, financiera y contable se establece en la cuidad de Itagüí, desde donde se realiza todas las funciones para sus 4 sedes; de forma mensual la compañía Contento BPS S.A cumple con sus obligaciones de pago de nómina con su respectiva contabilización y para cumplir con esto hace uso de herramientas tecnológicas.

Luego de realizar un diagnóstico a este proceso se logra identificar que este desarrollo presenta factores que dentro de la compañía se pueden convertir en un riesgo,

tanto operativo, psicosocial, perdidas de datos y fraude.

Para lograr que el área de la contabilidad y el área de nómina se encuentren relacionados y con la información actualizada, el personal de nómina en su proceso de cierre de mes envía a contabilidad una serie de archivos de texto planos que se genera desde su sistema o software y se importa al sistema de contabilidad.

Este proceso se debe realizar así debido a que el área de nómina y el área de contabilidad no cuentan con un mismo sistema o software, por lo tanto, se genera una posibilidad de riesgo, pues la misma información no se encuentra unificada en un solo sistema y para hacerla compartida se debe generar archivos de texto plano exportados de un sistema hacia otro.

Para realizar estos procesos se debe de tener mucha precaución al momento de generar la información pues es una herramienta que, así como la tecnología tiene puntos positivos, pero también contiene riesgos y puntos a mejorar.

6. Objetivos

6.1. Objetivo General

Evaluar y controlar la correcta aplicación de los procedimientos y lineamientos internos de la exportación e importación de archivos de texto plano realizados por medio de la gestión de nómina hacia el área de contabilidad.

6.2. Objetivos Específicos

- Identificar los riesgos que se generan al exportar e importar archivos de texto plano con información contable y financiera.

- Evaluar el proceso de exportación e importación de información contable y financiera a través de archivos de texto plano.

- Verificar el cumplimiento de la normativa interna de seguridad de la información para la generación y cargue de archivos de texto plano.

7. Metodología

Este proyecto de plan de empresa está desarrollado a través de una investigación descriptiva, que se convierte en una problemática que surge de analizar diversos factores dando paso a la generación de una pregunta de investigación acerca de la medición y evaluación de los riesgos y el control interno del uso de archivos planos en el área de nómina.

Cuenta con un diseño de investigación de tipo documental y de campo, usando el análisis de documentos, datos entre otros registros en un espacio real y tomado directamente del objeto de estudio; es un proyecto con un enfoque cualitativo con la finalidad de analizar, diagnosticar y recoger información sobre las probabilidades de riesgo, métodos y proceso aplicados con el objetivo de minimizar y evidenciar la eficiencia Y/O ineficiencia del proceso y del correcto uso de los sistemas internos de seguridad de la información para dar un resultado de análisis entrelazado con las normativas y políticas internas correspondientes.

Este proyecto es una investigación retrospectiva, ya que; se realiza una evaluación y un análisis a un hecho que ya se viene presentando en la empresa Contento BPS, pues es de conocimiento que el uso de archivos planos es una herramienta habitual para la compañía y que se hace uso de este cada mes al realizar los cierres de la gestión de nómina hacia el área contable, se aplica un método de investigación explicativo por tanto expone los posibles opciones y tipos de riesgos que se pueden generar al hacer uso de los archivos planos pero también cuenta con un enfoque hacia el método de

investigación descriptivo pues se realiza un análisis de los procesos y procedimientos utilizados para la generación, modificación u envió de los archivos planos por medio de una Auditoría al proceso interno; en la investigación, se hace uso de un muestreo discrecional centrada en el área contable y de nómina de la empresa Contento BPS S.A, áreas las cuales nos permiten ejecutar la auditoría al control interno a los archivos planos de nómina midiendo su eficacia y riesgos.

Tabla 1 Distribución del Personal por Áreas

	Área			
	Nómina	**Contabilidad**	**Tecnología**	**TOTAL**
Cantidad de integrantes	**6**	**4**	**1**	**11**

El desarrollo de los objetivos de este trabajo de grado se realizó a través de los métodos y técnicas de recogida de la información de observación y revisión de registros, los cuales nos permiten obtener un seguimiento tal cual ocurre en su cotidianidad o habitualidad mientras se está ejecutan el normal desarrollo del proceso, no se obtienen opiniones o comentarios de terceros pues al estar involucrado en la gestión el método la observación se convierte en una vivencia y una técnica más precisa; por otro lado, tenemos el método de la revisión de registros que nos permite examinar e investigar los documentos que se manejan o usan en el proceso y contienen toda la información de los cierres de nómina mensuales.

Para el análisis de la información este proyecto usa la técnica de la visualización de datos que nos permite por medio de un flujograma, graficas e imágenes, entrevistas y reuniones para darle claridad al caso de investigación; este proyecto también hace uso de mapa de calor que permite identificar y diagnosticar los niveles de riesgos que presenta el proceso de los archivos planos y este resultado se obtiene de la realización de la Auditoría a los procesos internos.

El proyecto hizo uso de herramientas de análisis de datos como el Microsoft Office Excel que apoyó el desarrollo de tablas y gráficos para el correcto avance del procesamiento de los datos y también se hace uso de herramientas que permiten crean flujogramas que detallan el proceso de los archivos planos.

8. Resultados.

Itagüí, 30 noviembre 2023.

Señores

CONTENTO BPS S.A

8.1. A Quien Pueda Interesar:

De manera cordial remito a ustedes el informe final de Auditoría al control interno en los archivos planos de nómina.

La finalidad de este análisis es brindarle al coordinador del proceso un plan de mejoramiento y demás acciones correspondientes.

Durante el desarrollo de esta Auditoría no se presentaron limitaciones y se facilitó el acceso a documentación física, digital, políticas, procedimientos, sistemas y áreas; a la fecha no tenemos registros de suceso o hechos que afecten de forma directa Y/O indirecta el proceso y su correcto funcionamiento, teniendo en cuenta no solo la ejecución si no también la seguridad de la información.

Cordialmente,

Manuela Marín García
Corporación Universitaria Remington

<table>
<tr><td rowspan="2">  </td><td rowspan="2">INFORME DE
AUDITORÍA INTERNA</td><td colspan="6">Código: BPS-01</td></tr>
<tr><td colspan="6">Versión: 01</td></tr>
<tr><td colspan="2">Fecha: 23/07/2014</td><td colspan="6"></td></tr>
<tr><td colspan="2">FECHA DE EMISIÓN DEL INFORME FINAL</td><td>Día:</td><td>30</td><td>Mes:</td><td>11</td><td>Año:</td><td>2023</td></tr>
</table>

8.2. Informe de Auditoría Interna

8.2.1. Objetivo de la Auditoría

Evaluar la gestión del proceso interno de archivos planos de nómina de la empresa CONTENTO BPS S.A.

8.2.2. Objetivos Específicos de la Auditoría

1. Verificar el cumplimiento de los lineamientos, normas y la seguridad para el intercambio de información, conservación y uso, de acuerdo con lo establecido en las políticas internas.
2. Revisar el cumplimiento y aplicación de los requisitos de control y seguridad plasmados para garantizar el correcto funcionamiento del proceso.

8.2.3. Alcance de la Auditoría

Realizar verificación, evaluación y diagnóstico del proceso de archivos planos del área de nómina, a través de los cumplimientos de requisitos normativos y políticas internas.

8.2.4. Criterios de la Auditoría.

1. Política de Intercambio de información (PL-SI-09) V04 202308 (Ver Anexo 1)
2. Política Corporativa de Seguridad de la Información (PL-SI-03) v17 202308 (Ver Anexo 2)
3. Seguridad de la Información (PR-SI-01) V10 202308 (Ver Anexo 3)
4. Manual de Cumplimiento de Políticas de Seguridad de la Información (M-SI-01) V08 202301 sección 6.1 – 6.8 – 6.15 – 9 – 9.1 – 9.2 – 9.3. (Ver Anexo 4)

8.2.5. Metodología de la Auditoría

1. Revisión de la ejecución del proceso vs normativa interna (PL-SI-09) V04 202308, (PL-SI-03) v17 202308 entre otras políticas de la empresa Contento BPS S.A.
2. Análisis de la entrega de información frente la normativa de seguridad dándole cumplimiento a ISO/IEC 27000, procedimientos y normatividad interna.
3. Solicitud de explicaciones, entrevistas, aclaraciones y justificaciones sobre el desarrollo y entrega final del proceso de archivo plano.

9. Desarrollo de la Auditoría.

De acuerdo con el diagnóstico realizado a la ejecución y uso de los archivos planos en el área de nómina de la empresa CONTENTO BPS S.A llevado a cabo a través de la medición de procedimientos, actividades y seguridad de la información se logra determinar la efectividad del proceso y el mejoramiento continuo de la empresa, desarrollando competencias que ayuden a cumplir los objetivos empresariales que fija la entidad.

La metodología planteada para el desarrollo de esta auditoría logro evidenciar falencias y acciones a mejorar en la seguridad de la información dentro del proceso, se hizo uso de la observación descriptiva como herramienta principal para obtener y evaluar la información suministrada, la entrevista se utilizó para examinar detalladamente el proceso desde una percepción completa y así lograr entender el proceso.

La evaluación se lleva a cabo de acuerdo con las normas de auditoría, políticas y normativa interna establecidas en fechas anteriores, los resultados de esta auditoria presentan una base confiable y verídica dado que su origen se fundamenta en una correcta planeación y efectiva ejecución del trabajo.

Inicialmente se hace notificación de la realización de la auditoria entre el periodo del 12 de octubre 2023 al 29 de noviembre 2023 haciendo entrega del resultado el día 30 de noviembre 2023, se pactaron visitas y encuentros con el área de contabilidad, tecnología y entrevistas con el área de nómina para obtener información y así reunir y centralizar cada dato.

Al desarrollar la auditoria resalto aspectos positivos como:

- Excelente disposición del personal encargado de cada área (contabilidad, tecnología y nómina) para el proceso de auditoría.
- Correcta gestión y trabajo de los integrantes directamente relacionados con el proceso de generación, cargue y procesamiento de los archivos planos.

9.1. Talento Humano Asociado al Proceso:

El uso, generación, desarrollo y procesamiento de archivos planos lo realizan el personal de las áreas de nómina, contabilidad y tecnología:

- Cuatro profesionales universitarios en planta 6 del edificio donde se establece el área contable.
- Un profesional universitario en planta 6 del edificio establecido en el área de tecnología.
- Un profesional especialista en planta 1 del edificio establecidos en el área de nómina.
- Un profesional universitario en planta 1 del edificio establecidos en el área de nómina.
- Cuatro tecnólogos en planta 1 del edificio establecido en el área de nómina.

Se realiza un análisis de los perfiles de los integrantes del área de nómina quienes son los directamente responsables del proceso de generación y los responsables de la información donde se observa lo siguiente:

- Coordinador del área: Contrato a término indefinido, cumple con requisito para la contratación teniendo un nivel alto en experiencia y preparación.
- Analista del área: Contrato a término indefinido, con nivel medio de preparación y alto nivel de experiencia.
- Auxiliares de nómina: Contrato a término indefinido, se encuentran en una escala entre básica y media en nivel de preparación y experiencia.

Tabla 2 Análisis Perfil Profesional.

Cargo	Área	Subproceso	Tiempo en la empresa	Perfil Profesional	Cumplimiento
Coordinador	Nómina	Generación y procesamiento nómina	9 años	Tecnólogo, Contador público, especialista tributario con 9 años de experiencia en campos contables y administrativos	✓
Analista		Liquidación reporte seguridad social	6 años	Tecnólogo, Contador público, con 7 años de experiencia en campos contables y administrativos	✓
Auxiliar 1		Liquidaciones definitivas	4 años	Tecnólogo, en proceso del título de contador público, con 4 años de experiencia en campos contables y administrativos	✓
Auxiliar 2		Sustituciones patronales	15 meses	Tecnólogo, en proceso del título de contador público, con 4 años de experiencia en campos contables y administrativos	✓
Auxiliar 3		Ausentismos-Vacaciones	10 meses	Tecnólogo con 10 meses de experiencia en campos contables y administrativos	−
Auxiliar 4		Payflow-Estudios crédito	4 meses	Tecnólogo con 4 meses de experiencia en campos contables y administrativos	−
Coordinador	Contabilidad	Generación y procesamiento contabilidad	14 años	Tecnólogo, Contador público, especialista en proceso de titulación para especialista con 20 años de experiencia en campos contables.	✓
Analista		Liquidación impuestos	5 años	Tecnólogo, Contador público, con 7 años de experiencia en campos contables.	✓
Auxiliar 1		Contabilización sustituciones patronales	Años	Tecnólogo, Contador público, con años de experiencia en campos contables.	✓
Auxiliar 2		Facturación	Años	Tecnólogo, en proceso de titulación de contador público, con años de experiencia en campos contables.	✓
Coordinador	TIC	Conversión de archivo plano	10 años	Tecnólogo, Científico-Analista de datos, especialista en Big Dara con 15 años de experiencia en campos tecnológicos.	✓

Nota: la evaluación del seguimiento se fundamenta en el nivel de experiencia y estudios; la mayoría de los integrantes cumplen con los requisitos en un alto nivel. Los integrantes que se encuentran en nivel medio son integrantes que en el momento tienen poca participación del proceso de archivos planos.

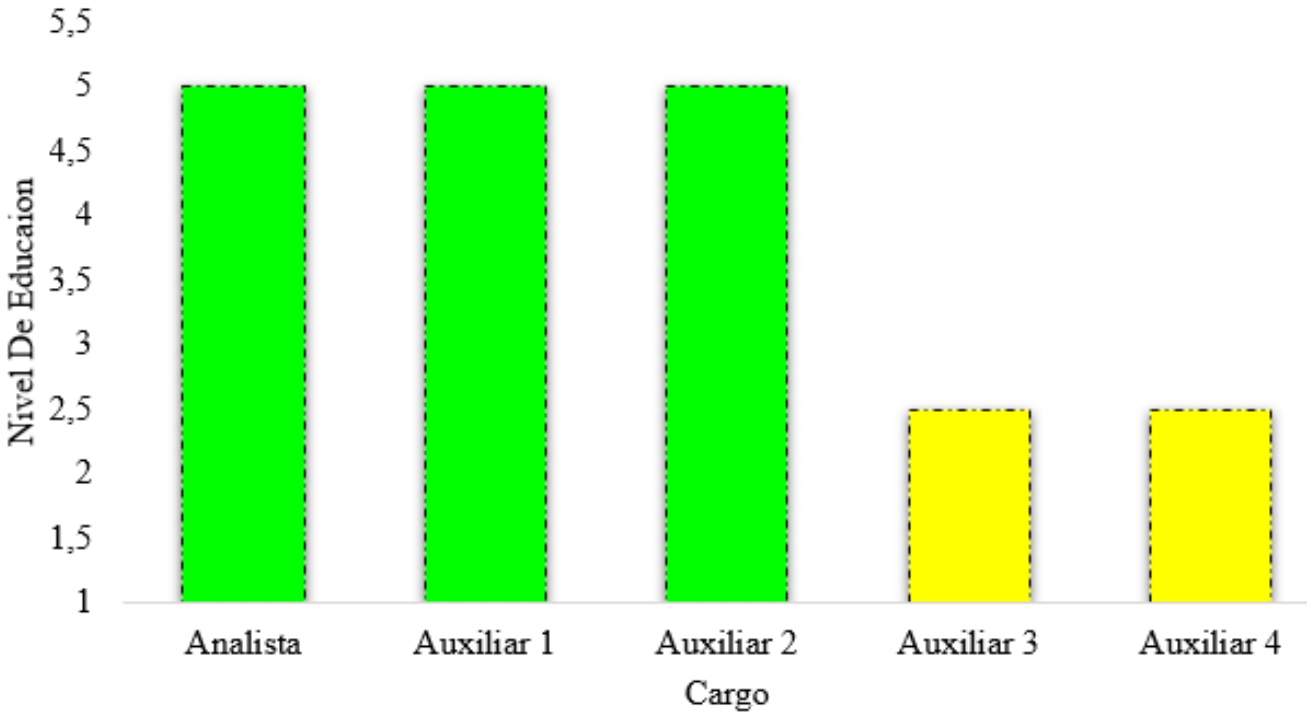

Figura 2 Nivel de Educación. Fuente Propia Manuela Marin, 30 de Octubre 2023.

El personal involucrado en el proceso de archivo plano es un personal con niveles educativos altos, no certifica que por esta razón los niveles de riesgo del proceso no existan, pero si se logra identificar una mitigación y un nivel bajo de ´probabilidad de riesgo.

9.2. Descripción del Proceso

A través del método de entrevista y observación se logra desarrollar un flujograma donde se permite evidenciar el completo desarrollo del proceso, desde su origen hasta su final; el área de nómina es el encargado de la generación de este archivo, se descarga la información desde su sistema o software generando un archivo de tipo TXT (Texto sin formato) se valida esta información vs la información almacenada en el sistema realizando una comparación de datos y cifras, previamente esta información se encuentra validada exportando datos del software a un formato de Excel para realizar cruces y validaciones dado que la información que se envía por medio de los archivos planos no cuentan con cifras adicionales, colores etc.… debe ser un archivo limpio con la información precisa y concreta.

Luego de realizar esta validación y cerciorarse de que los datos almacenados en el sistema se encuentren correctos y no requerían correcciones se procese a exportar el archivo plano así:

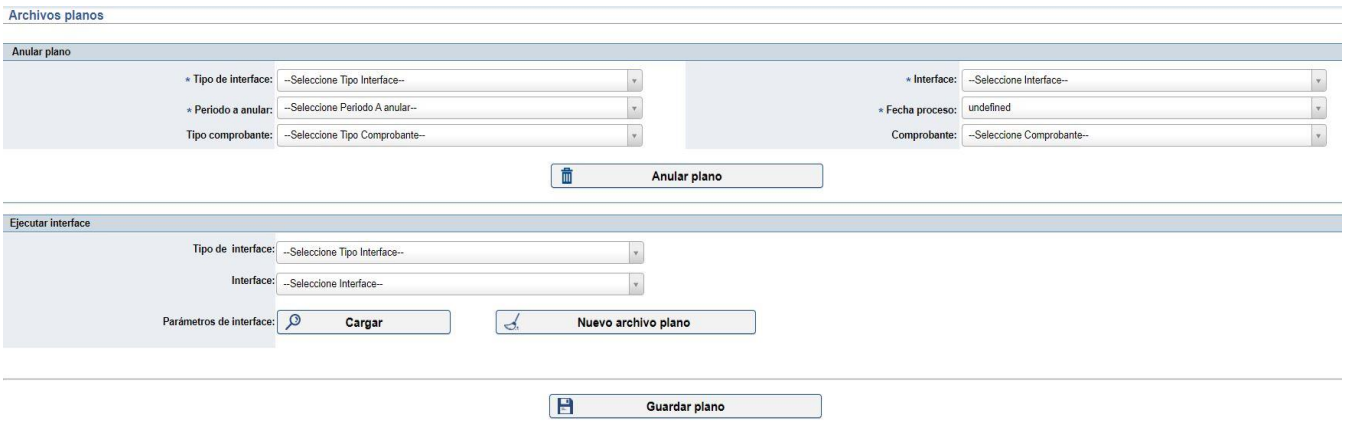

Figura 3 Sección Archivo Plano en Software. Fuente Software Gosem, 01 de Noviembre 2023.

Al obtener el archivo plano revisado, el integrante responsable del proceso debe cifrar este archivo con contraseña en un archivo ZIP así:

Figura 4 Archivo Plano (PAB) Cifrado en ZIP. Fuente Propia Manuela Marin, 01 de noviembre 2023.

Cuando el archivo plano se encuentre cifrado se procede a enviar esta información bajo una solicitud de I service, que es un aplicativo donde se realizan solicitudes internas en la compañía donde se especifica el área al que se le hace entrega, en este caso tecnología, adjuntando el archivo ZIP, este sistema genera un numero de Ticket Único:

Detalle

Id	100453	Fecha de Creación	2023-11-03 12:29:12	Creador	
Nombre Area	TIC	Proceso	Desarrollo	Sede	1
Centro de Costos	DIRECCION GESTION HUMANA-10900201	Archivo Requerimiento	Ver archivo	Tipo Requerimiento	Solicitud reporte-BD
Fecha Respuesta	2023-11-03 16:26:08	Archivo Respuesta		Fecha Vencimiento	2023-11-09 18:00:00
Responsable		Estado	Cerrado		
Comentario	Buen día Don Fabio, envío comprobante contable NIIF correspondiente al mes de octubre 2023 para ser cargado a contabilidad, muchas gracias				

Figura 5 Aplicativo I Service. Fuente Aplicativo Interno, 01 de noviembre 2023.

Como control adicional, por medio de correo electrónico, se hace entrega al área contable, de gerencia y nuevamente al coordinador del área de tecnología el número del ticket del aplicativo de I Service + el archivo adjunto cifrado:

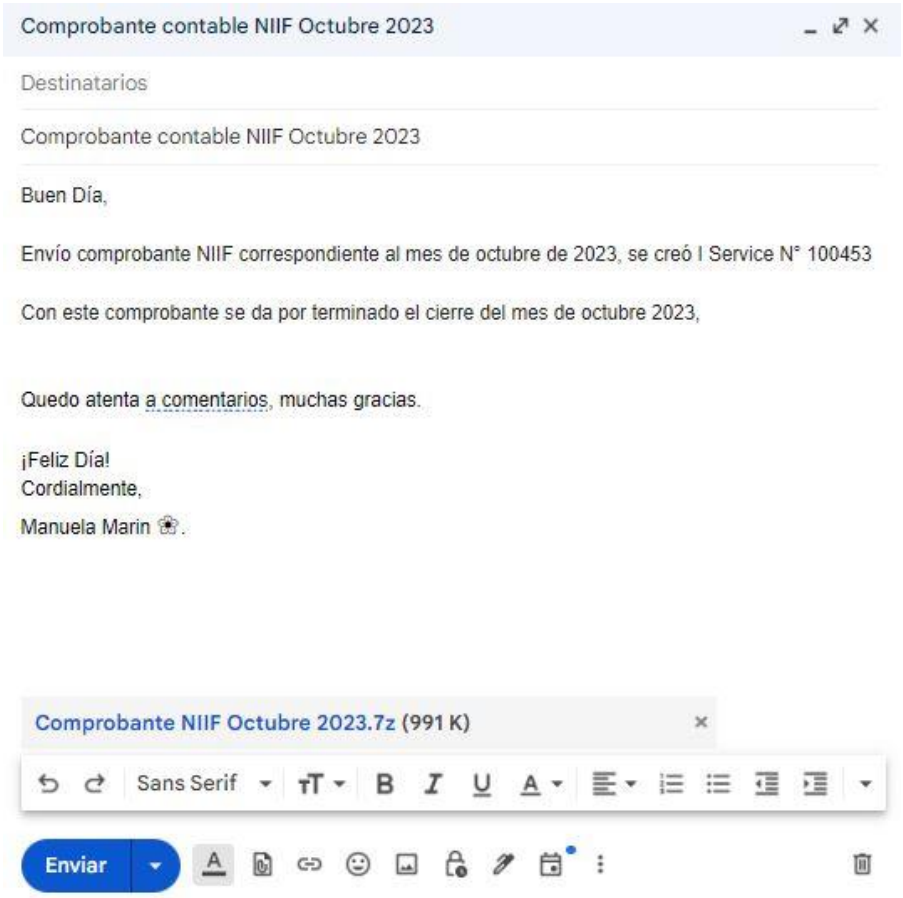

Figura 6 Correo a Contabilidad y Tecnología. Fuente Correo Gmail, 01 de Noviembre 2023.

El área de tecnología recibe la solicitud con el ticket único junto con el archivo adjunto en el correo electrónico, realiza una validación y comparación de estos archivos para posteriormente procesar la información del archivo TXT a un formato que el sistema contable, en este caso el software ERP (Ofimática S.A), permita:

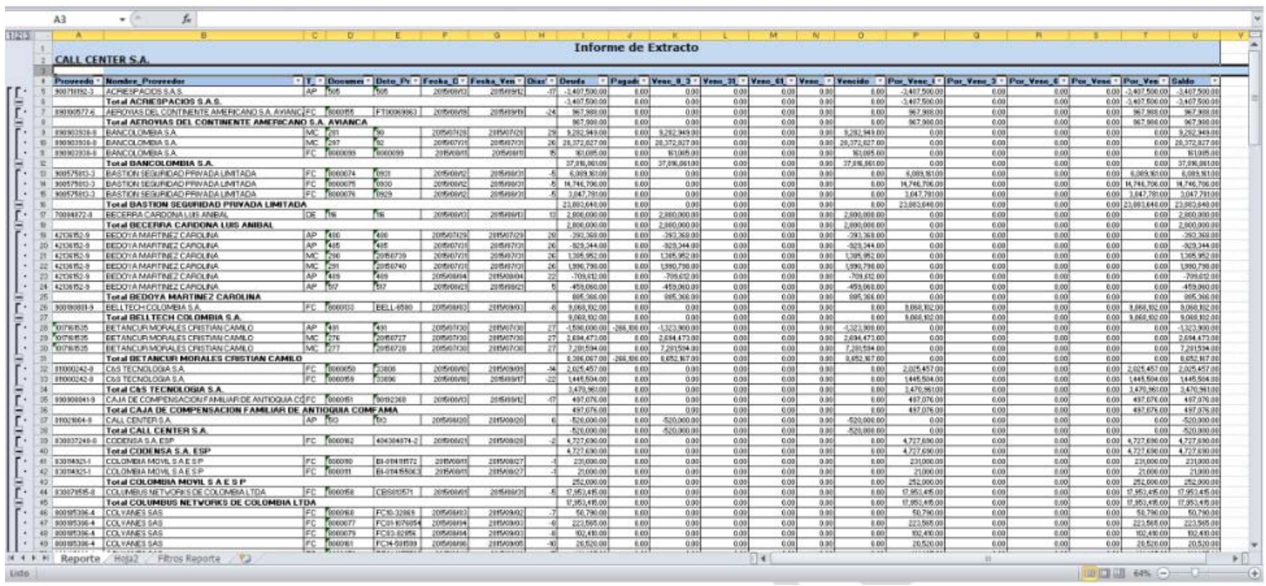

Figura 7 Formato Aceptado por Software ERP. Fuente Propia Manuela Marin, 01 de noviembre 2023.

Con información procesada y convertida el coordinador del área de tecnología, hace entrega al área contable el archivo final listo para ser importado al sistema, el área contable realiza validación de datos y cruces para cerciorarse que no haya perdidas de datos y procede a cargar esta información al software:

Figura 8 Software Ofima. Fuente Software Ofimática, 01 de Noviembre 2023.

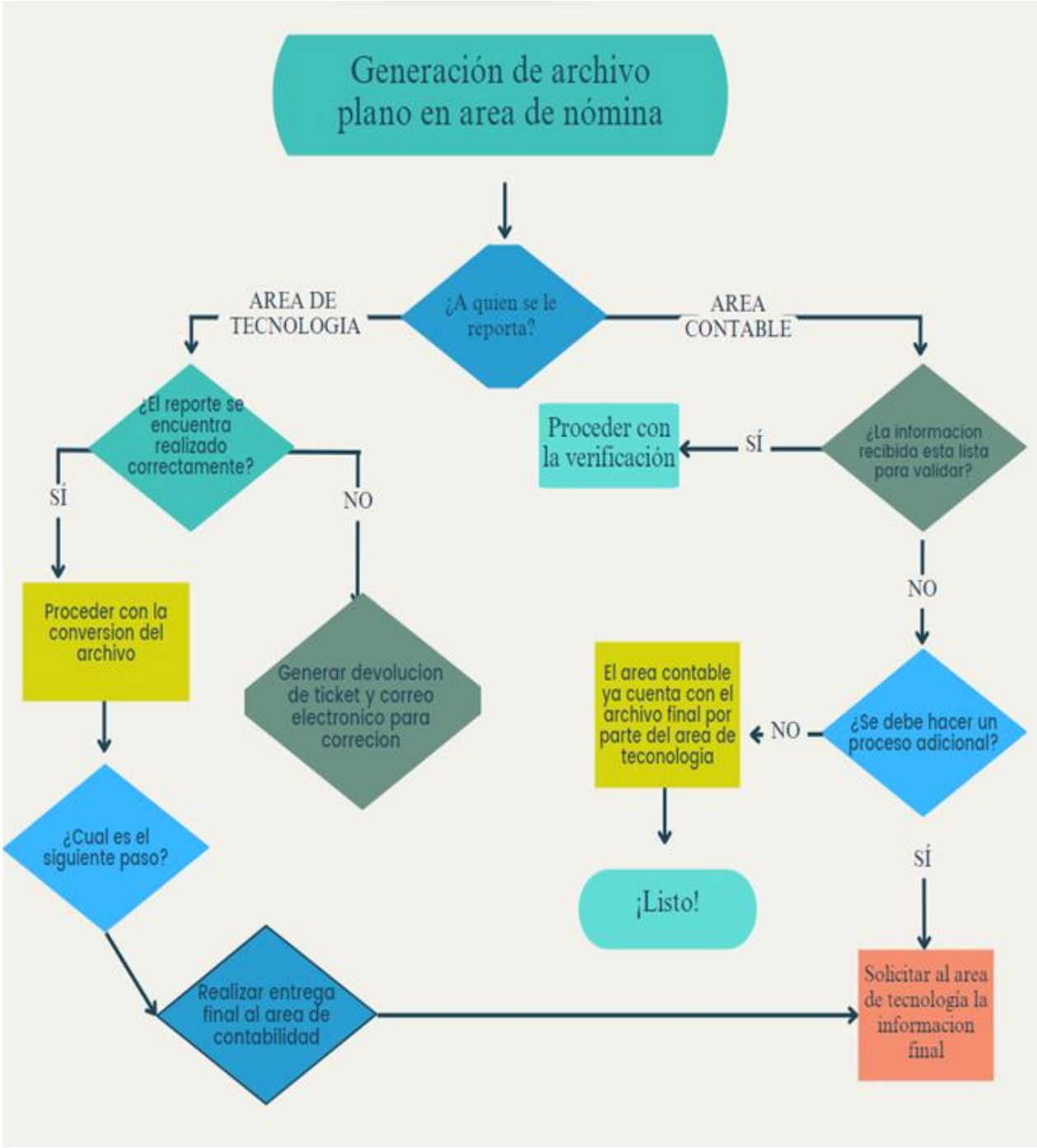

Figura 9 Flujograma Proceso. Fuente Propia Manuela Marin, 06 de Noviembre 2023

9.3. Mapa de Calor

Tabla 3 Matriz de Riesgo y Mapa de Proceso

Fases 1	**Identificar el evento**	Creación, desarrollo, validación y seguridad de los archivos planos.	**Convenciones**		
Fases 2	**Determinar la probabilidad**	Relacionado con las estadísticas de los eventos identificados, son datos que reposen en la empresa	**A: Alta**	**M: Media**	**B: Baja**
Fases 3	**Determinar el impacto**	Relacionado con la materialidad en los estados financieros	**A: Alta**	**M: Media**	**B: Baja**
Fases 4	**Matriz de riesgos y Mapa de calor**				

	Eventos	**P: Estadísticos**	**I: Impacto**
1	Creación de archivos planos	**B**	**B**
2	Desarrollo del archivo plano	**M**	**M**
3	Validación de los datos del archivo plano	**B**	**A**
4	Seguridad de información del uso de archivo plano.	**A**	**A**

MATRIZ DE RIESGO VS CONTROL						Auditoría y/o REVISORÍA FISCAL				
LE CORRESPONDE A LA EMPRESA						Evalúa los controles existentes				
ITEMS	EVENTO	MAPA DE RIESGO			CONTROL EXISTENTE	A	R	D	PRUEBAS DE CONTROL	
		A	M	B		Adecuado	Razonable	Deficiente	Sustantiva	Cumplimiento
1	**Creación de archivos planos**			X	Información extraída directamente del software	X				X
2	**Desarrollo del archivo plano**		X		Revisar formato e información contenida		X		X	
3	**Validación de los datos del archivo plano**			X	Validación de la información del software vs cálculos manuales	X			X	
4	**Seguridad de información del uso de archivo plano.**	X			Cifrar archivo con contraseña ZIP		X			X

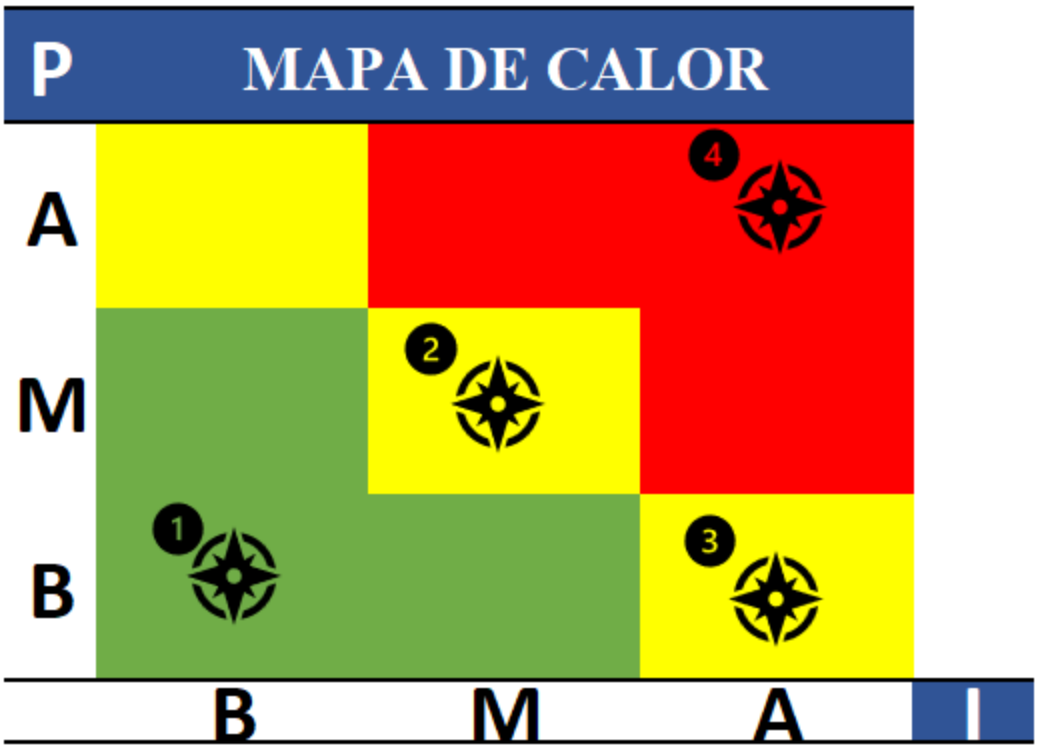

Figura 10 Resultado Mapa de Calor. Fuente Propia Manuela Marin, 20 de Noviembre 2023.

10. Observaciones y Recomendaciones

- Se recomienda implementar niveles de seguridad más completos, al realizar el mapa de calor y la matriz de riesgo se logra evidenciar que el proceso que requiere atención inmediata corresponde al proceso 4 “Seguridad de información del uso de archivo plano”.

  Si bien se logra evidenciar un control existente y en funcionamiento se requiere de un control más fuerte, que asegure que la información recibido o exportada no será asequible para cualquier integrante de la empresa CONTENTO BPS S.A y solo será procesada y revisada por los integrantes directamente relacionados con el proceso.

- Se recomienda explotar y hacer uso del aplicativo I Service con el que la empresa cuenta, se considera luego de analizar el programa que es un sistema que permite definir un remitente exacto y no es un aplicativo manipulable, haciendo que, el nivel de seguridad sea alto.

- Se recomienda continuar con la gestión y el compromiso con el cual los integrantes relacionados al proceso realizan sus labores correspondientes, buscando en toda ocasión mitigar riesgos y logrando el crecimiento empresarial.

Se firma constancia en Itagüí, Antioquia, a los 30 días del mes noviembre de 2023.

Manuela Marín García
Corporación Universitaria Remington.

11. Conclusiones.

La realización de la auditoria al control interno de los archivos planos de nómina permitió a la empresa CONTENTO BPS S.A certificar que los procesos se encuentran al día de hoy funcionando correctamente, cumplimiento con las normativas fijadas y que como toda empresa presenta puntos a mejorar, que, aunque requieren de atención inmediata no son falencias o cuellos de botella que generen retrocesos a la empresa.

Por medio de la auditoría realizada se logra evidenciar que el ítem que presenta un riesgo alto es la seguridad de la información, pero debemos dejar en claro y estipulado que aun cuando hay falencia y hay que mejorar no significa que sea un proceso que afecte el resultado final, es un ítem que se debe de solucionar inmediatamente por el nivel de riesgo que constituye a nivel de política de seguridad, pero no a nivel de funcionamiento o desarrollo del proceso.

El desarrollo de la auditoria permitió conocer por completo el proceso directamente relacionado con el archivo plano, dejando en evidencia que el personal se encuentra capacitado y cuenta con valores profesionales y corporativos que hacen del proceso un procedimiento confiable, efectivo y útil.

12. Referencias

- Software ERP. (2023, 12 de septiembre). Ofima S.A.S. Sitio web: https://ofima.com/software-erp/
- GOSEM GH. (s.f). Sitio Web: https://sighsas.com/V4/gosem-gh/
- Equipo editorial, Etecé (2023,06 de marzo). Marco metodológico, Sitio web: https://concepto.de/marco-metodologico/
- Texto plano. (2014, enero 23). EcuRed, Sitio web: https://www.ecured.cu/index.php?title=Texto_plano&oldid=2145037.
- Chaupi, A. J. H. (2010). Algoritmo de encriptación de archivo de texto plano. Ciencia y Desarrollo, 11, 55-58.
- Barahona Barahona, G. F. (2016). Sistema de contabilidad gubernamental generador de archivos planos para la carga de información financiera AlE-SIGEF del GADP de San Vicente de Pusir, Bolívar Carchi (Bachelor's thesis).
- Sánchez Tobón, J. (2020). Creación de macro para la realización de archivo plano de la empresa. Tecnológico de Antioquia Institución Universitaria.

13. Anexos

13.1 Anexo 1 Política de Intercambio de Información

(PL-SI-09) V04 202308

Documentación Interna

Objetivo

"Establecer y mantener esquemas de seguridad para el intercambio de la información entre los procesos de la organización y cualquier entidad externa (Aliado estratégico, proveedor, ente de control, etc.) en línea con los acuerdos definidos e involucrados con la prestación de servicios."

Alcance

Esta política aplica para toda la información digital y/o física intercambiada entre los sistemas de información de Contento BPS y que requiera ser entregada a entidades externas bajo acuerdo de intercambios de información por traspaso vía correo electrónico, internet, Nube, Login en sistemas, y/o a través de cualquier medio magnético o de almacenamiento, papel u otro medio disponible. También se incluyen los procesos internos en relación con la carga/descarga de información en los equipos locales.

Introducción

El intercambio de información es una práctica utilizada entre entidades que requieren compartir información en forma oportuna o en tiempo real con el fin de obtener alta capacidad de desempeño de sus procesos.

Esta práctica es constantemente amenazada por agentes internos y externos que no permiten un flujo adecuado para lograr su fin. Es por esto por lo que los activos de información logran ser vulnerados y, por ende, genera la materialización de riesgos inherentes al proceso.

Esta política busca proteger la información de posibles amenazas y brinda oportunidades de disminución de las vulnerabilidades asociadas.

Definiciones

Login: Usuario de autenticación en sistemas de información.

SFTP: Protocolo seguro de transferencia de información.

Cifrado: El cifrado en ciberseguridad es la conversión de datos de un formato legible a unformato codificado. [Fuente: Kaspersky]

Contraseña: Código secreto para controlar el acceso hacia un recurso.

Transferencia: Mover información desde usuario fuente, hacia un usuario destino, por un canal establecido.

Propósito

Definir las directrices para proteger el intercambio de información de manera interna yexternas ya sea digital o física, a través de sistemas de información o de forma presencial.

Marcos de referencia

Los contenidos de esta política de intercambio de información se han estructurado paraproporcionar las características de confidencialidad e integridad de la información Corporativa de los procesos que requieran este tipo de control, según lo previsto en:

Norma internacional ISO/IEC 27002:2015 A.13.2 Transferencia de Información

Ley 1581 de 2012 Protección de Datos Personales.

Compromisos de la Empresa

Contento BPS entendiendo la importancia de la seguridad de la información y de la efectiva comunicación entre sus partes interesadas internas y externas, teniendo como base las medidas de seguridad adecuadas, emplea técnicas idóneas de transferencia de información.

La compañía como responsable de procesos, procedimientos o actividades que impliquen transferencia de información empleando medios digitales y físicos, se establecen mecanismos de protección de la confidencialidad e integridad para la entrega o recepción de estos.

Marco Sancionatorio

El uso indebido o incumplimiento de lo establecido en la presente política, dará lugar a la intervención del área jurídica, gestión del talento organizacional, y/o la alta dirección para dar aplicación a las medidas administrativas disciplinarias o legales a que hubiere lugar.

Factores Críticos de Éxito

Ausencia de recursos

Desconocimiento del procedimiento y la política a quienes están dirigidos.

Incumplimiento de la presente política

Utilización de las herramientas sin homologar por la empresa.

Desconocimiento por parte de terceros, de los procedimientos y mecanismos de control establecidos por CONTENTO BPS.

Declaración de la Política

Esta Política sobre intercambio de información se integrará a la normativa básica de la empresa, incluyendo su difusión, y las sanciones correspondientes por incumplimiento de esta.

Es Política de Contento BPS S.A.:

La herramienta aprobada y homologada para las actividades de transferencia de información es el SFTP. Se puede transferir información por el medio que determine el aliado estratégico o entes de control, por ejemplo, por medio de correo electrónico siempre y cuando se cumpla con las políticas de cifrado ocriptografías establecidas por la organización.

Definir las condiciones de uso de las infraestructuras y mecanismos utilizados para el intercambio de comunicación (incluyendo conexiones inalámbricas).

Todas las definiciones de uso de técnicas se deben basar en buenas prácticas como el uso de herramientas de cifrado, llaves criptográficas, etc. para proteger la confidencialidad y autenticidad de la información.

Proteger la información intercambiada de la intercepción, interrupción, fabricación/modificación de los datos intercambiados.

Proteger contra código malicioso que podría ser transmitido a través de la infraestructura de comunicaciones establecida entre la compañía y el cliente.

Establecer directrices de uso, retención y eliminación de los datos intercambiados, en concordancia con la legislación aplicable a la compañía de orden nacional einternacional.

Establecer canales de comunicación entre la compañía y el cliente a fin de concientizar y sensibilizar permanentemente al personal en el uso de la información y los riesgos inherentes a los procesos.

Proteger las bases de datos e información de datos personales que pueda verse vulnerada en virtud de tal transferencia de información con las medidas de seguridad necesarias para el caso y en cumplimiento de la Ley 1581 de 2012, paraevitar un uso o divulgación no autorizada.

Ningún empleado está autorizado a desarrollar actividades de carga y/o descarga de información por un medio distinto al autorizado SFTP el cual está aprobado solo para intercambio de información.

Los activos de información físicos que requieran ser compartidos a partes externas, deberán enviarse por medio de una empresa de correo certificado, la cual cuente con los controles necesarios para garantizar la confidencialidad e integridad de la información. Ver procedimiento "*Correspondencia interadministrativa*"

Los activos de información físicos donde CONTENTO BPS es el receptor serán recibidos en primera instancia por la persona del área de recepción, quien será la encargada de hacer entrega directa a la persona quien va dirigida el activo, firmando el recibido a satisfacción

La transferencia a nivel interno, de información física clasificada como confidencial, se debe realizar directamente por los implicados (fuente- receptor)sin intermediarios, con el fin de garantizar la confidencialidad e integridad de esta.

Vigencia.

Esta política rige a partir de la fecha y ha sido establecida comunicada y aprobada por laalta dirección.

Dado en la ciudad de Medellín a los 15 días del mes de agosto de 2023 se aprueba por el Representante Legal.

DAVID RODRIGUEZ **DORALBA SIERRA**

Representante Legal Líder de Seguridad de la Información

APROBACION Y OFICIALIZACION

FASES	**CARGO RESPONSABLE**	**NOMBRE**	**MEDIO POR EL CUAL SE APROBÓ**
Elaboración	Líder de Seguridad de la Información	Doralba Sierra	Correo electrónico
Revisión			
Aprobación	Representante Legal	David Rodríguez	

MODIFICACIONES / ACTUALIZACIONES

VERSIÓN	**FECHA (año-mes)**	**DESCRIPCIÓN RESUMIDA DE LA MODIFICACIÓN / ACTUALIZACIÓN / ANULACIÓN**
OO	2018-02	Creación
01	2018-09	Actualización de contenido

02	2021-01	Actualización de contenido
03	2022-06	Actualización de contenido
04	2023-08	No se realiza ningún cambio

13.2. Anexo 2 Política Corporativa de Seguridad de la Información

(PL-SI-03) v17 202308

Documento interno

Objetivo

Establecer el liderazgo y compromiso de la Alta Dirección frente al Sistema de Gestión de Seguridadde la Información – SGSI de CONTENTO BPS S.A, mediante el establecimiento de la Política Corporativa de Seguridad de la Información, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

Alcance

La presente política aplica a todos los empleados, aliados y partes interesadas (internas y externas),que gestionan datos o hacen uso de los activos de información de CONTENTO BPS S.A.

Definiciones

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elementorelacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. [Fuente: ISO/IEC 27000:2012].

Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [Fuente: ISO/IEC 27000:2018].

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. [Fuente: ISO/IEC 27000:2018].

Gestión de Riesgos: Proceso efectuado por la alta dirección de la entidad y por todo el personal paraproporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].

Impacto: Las consecuencias que puede ocasionar a la organización la materialización del riesgo. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de lainformación inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [Fuente: ISO/IEC 27000:2018].

Integridad: Propiedad de la exactitud y la integridad. [Fuente: ISO/IEC 27000:2018].

Parte Interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a símisma como afectada por una decisión o actividad. [Fuente: ISO/IEC 27000:2018].

Plan de Continuidad del Negocio: Información documentada que guía a una organización pararesponder a una interrupción y reanudar, recuperar y restaurar la entrega de productos y servicios según sus objetivos de continuidad del negocio. [FUENTE: ISO 22300: 2018].

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. [Fuente: Manual Metodología de Riesgos: Función Pública:2022].

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Seguridad de la Información: Preservar la confidencialidad, integridad y disponibilidad de la información. [Fuente: ISO/IEC 27000:2018].

Sistema de Gestión de la Seguridad de la Información - SGSI: parte del sistema de gestión general, basado en un enfoque de riesgo empresarial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Nota: El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos. [Fuente: ISO/IEC 27000:2012].

Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información. [Fuente: ISO/IEC 27000:2018].

Sistema de Gestión: Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos. [Fuente: ISO/IEC 27000:2018].

Propósito

Definir una directriz de alto nivel, que enmarque las pautas relacionadas con el diseño,implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI para CONTENTO BPS, y que, a su vez, sirva como un marco de referencia parael uso adecuado de los activos de información y la gestión de riesgos que se deriven de la utilización los mismos.

Marco de referencia

Esta política está sustentada en lo establecido en la Norma ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información, en el requisito 5.2 POLÍTICA, la cual debe ser adecuado alpropósito de la compañía, objetivos estratégicos e incluir el compromiso de la alta dirección frentea su cumplimiento y mejora continua.

Compromiso de la dirección

La Alta Dirección de Contento BPS S.A. está comprometida con el desarrollo y la implementacióndel Sistema de Gestión de Seguridad de la Información, así como el mantenimiento y mejora continua del mismo.

Como muestra de este compromiso ha autorizado el diseño e implementación del SGSI basado en la norma ISO 27001:2013, y aprobado la presente política.

Importancia de la seguridad de la información

La implementación del SGSI permite la protección de los activos de información de la compañía y sus partes interesadas, mediante la gestión de riesgos y la adopción de una cultura de seguridad,garantizando la continuidad del negocio, la disminución de materialización de riesgos e incidentes y la optimización del retorno de inversiones y mayores oportunidades de negocio.

La seguridad de la información se enfoca en la preservación de las siguientes características:

Confidencialidad: Garantizar que la información sea accesible sólo a aquellas personasautorizadas dado su rol y privilegios asociados.

Integridad: salvaguardar la exactitud y completitud de la información y los métodos deprocesamiento.

Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a la información y alos recursos relacionados con la esta, siempre que lo requieran.

Entendiendo que la información puede existir en diversas formas (física y digital) y puede estar contenida o trasmitirse por cualquier medio (papel, USB, correo

electrónico, video, dispositivos móviles, conversación, entre otros), independientemente de esto, siempre debe contar con los controles necesarios para su adecuada protección de acuerdo con su clasificación.

Marco Sancionatorio

El incumplimiento de la presente política dará lugar a la aplicación de las medidas disciplinarias o legales vigentes en la organización, con la intervención del área Jurídica, Gestión del Talento y/o la Alta Dirección; de acuerdo con los procedimientos internos, el impacto que esto tenga para la empresa y demás lineamientos aplicables a la compañía.

Factores Críticos de Éxito

Falencias en los planes de sensibilización a todas las partes interesadas identificadas.

Falta de apoyo, liderazgo o compromiso por parte de la Alta Dirección.

Incumplimiento de la presente política por desconocimiento.

Declaración de la Política de Seguridad de la Información

CONTENTO BPS consiente de la importancia de la seguridad de la información y la protección de sus activos para el cumplimiento de su misión, visión y objetivos estratégicos, ha adquirido el compromiso de proteger la integridad, disponibilidad y confidencialidad de la información mediante el diseño, implementación,

mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información – SGSI, a través de la gestión de activos, incidentes y riesgos de seguridad de la información.

CONTENTO BPS se compromete a dar cumplimiento de los requisitos legales aplicables, además de promover una estrategia de seguridad de la información basada en las mejores prácticas y adopción de los controles descritos en la norma ISO 27001:2013. De igual forma, establece lasmedidas requeridas para la formación de su personal y la toma de conciencia de todas las partesinteresadas frente al SGSI.

La implementación de nuevos proyectos que puedan representar riesgos de seguridad de la información debe contar con actividades de planeación, seguimiento y cierre que incluyan la seguridad de la información durante todo su ciclo de vida. Adicionalmente, como parte de las actividades del proceso de Seguridad de la Información, está el de garantizar el acompañamientoen el diseño, implementación, ejecución de pruebas y actualización del Plan de Continuidad deNegocio acorde a las necesidades de la Compañía y a los riesgos que puedan afectar el desempeño, respuesta u operación de Contento BPS frente a eventos que puedan interrumpir el normal desarrollo de los servicios prestados.

A continuación, se relacionan controles aplicables para todos los integrantes de la compañía.

Portar el Carné siempre que vaya a ingresar al edificio, en un lugar visible, que lo identifique como empleado de Contento BPS S.A., en caso de ser colaborador de alianzas, mostrar su respectivo carné de la empresa para la cual labora y respetar el debido proceso de registro en la recepción.

Antes de ingresar a su área de trabajo correspondiente, debe de guardar sus pertenencias en el locker asignado, en caso de no tener locker, debe reportarlo con su jefe inmediato paraque éste, lo manifieste ante la Líder de seguridad física y se le asigne uno. En caso de quese utilice un locker sin haberse notificado y autorizado, se procederá a romper el candado y al correspondiente desalojo, estos artículos que sean desalojados se deben reclamar al Líder de Seguridad física.

No se permite el ingreso de dispositivos móviles y de almacenamiento a la operación a todo el personal, con excepción de Gerentes y Ejecutivos de cuenta y personal autorizado por el Área de Seguridad de la Información, de igual forma se ratifica que las acciones dentro dela operación para temas personales con líneas no corporativas no serán permitidas, para loscasos donde sea necesario chat web o algún tipo de herramienta de comunicación se debengestionar una licencia corporativa.

Estos dispositivos incluyen

Celulares

Tablet

Computadores

Cámaras fotográficas

USB

Discos extraíbles

Al igual que el ingreso y uso de

Cuadernos

Revistas

Hojas

Apuntes físicos

Lápices, lapiceros, marcadores

Objetos cortopunzantes.

Para el personal de las Áreas de Apoyo (Compras, Gestión del Talento Organizacional, Gestión Documental, Gestión Financiera, Gestión Jurídica, Mantenimiento, Seguridad de la Información, Tecnología y Comunicaciones, BI, Formación, Unidad de Valoración de Experiencias, Calidad ydemás administrativos), se autoriza el uso del celular siempre y cuando no intervenga por ningúnmotivo en los ambientes de Operación.

Guardar absoluta reserva de la información que se gestiona en la compañía en concordancia al acuerdo de confidencialidad que se firma cuando se ingresa a la organización

Para garantizar que sus contraseñas no sean conocidos por nadie debes utilizar la aplicación de gestión de contraseñas que te permitirá almacenarlas de forma segura, estas son personales e intransferibles

Solo el personal de Tecnología y comunicaciones está autorizado para cambiar configuraciones a los PC asignados y/o movilizarlos (Pc, mouse, teclado, diademas) en sitios internos o externos dependiendo de las directrices recibidas. Los daños físicos malintencionados a estos componentes será incumplimiento a la política de dispositivos móviles y conexión remota.

No está permitido a ningún proceso comprometer la integridad de la información por mediode programas, solicitudes de edición de audios, o cualquier otra actividad que modifique,altere, adicione o suprima toda o parte de los datos, contenidos en CDR, grabaciones, reportes, indicadores, bases de datos o cualquier tipo de documentación de propiedad de la empresa o terceras partes.

Todo visitante debe registrarse en la recepción, si llega en vehículo, debe parquear en el sitioasignado y desplazarse a la recepción para realizar dicho registro y

si llega con acompañantes, los mismos deben de bajar del vehículo en la portería para registrarse.

El personal externo a la compañía debe de ser acompañado por un empleado durante todo el tiempo que permanezca en las instalaciones.

Todo el personal debe informar a su jefe inmediato y éste al Líder de Seguridad de la Información, los eventos o incidentes detectados y que impliquen riesgo de incumplimientoa las normas de Seguridad de la Información.

No está permitido el ingreso a otras áreas diferentes a las estipuladas en el contrato con lacompañía, únicamente tendrán el acceso configurado por la Líder de Seguridad Física.

No está permitido el ingreso de alimentos y bebidas a las estaciones de trabajo ya que pueden poner en riesgo los equipos y causar daño o deterioro. Únicamente se permite elingreso de un termo con tapa segura y debe ser ubicado en un lugar retirado del equipo.

No se deben dejar documentos físicos en las impresoras o escáner; además no se pueden dejar archivos digitales en los computadores ni servidores con acceso público después deimprimir o escanear alguna información.

No se permite solicitar ni entregar firmas en documentos en blanco ni conservar firmas digitales de otros integrantes.

Objetivos de Seguridad de la Información

Garantizar la integridad, confidencialidad y disponibilidad de la información, mediante la adecuada gestión de los activos de información propios y de las partes interesadas internas y externas, estableciendo una metodología de clasificación, etiquetado, transferencia, almacenamiento y uso, que permita minimizar el riesgo existente frente a estos.

Minimizar la materialización de riesgos de seguridad de la información, continuidad del negocio y privacidad y protección de datos personales, mediante su gestión adecuada yoportuna, tomando como marco de referencia la norma ISO 31000 y 27005.

Mejorar continuamente la conveniencia, adecuación y eficacia del Sistema de Gestión deSeguridad de la Información de Contento BPS, mediante la implementación de accionescorrectivas eficaces, auditorías internas y externas objetivas, participación de las partes interesadas internas y externas y revisiones a intervalos planificados del proceso de seguridad de la información.

Capacitar y sensibilizar a los integrantes, aliados, proveedores y demás personas vinculadas a la compañía, logrando la aPropiación de una cultura de seguridad de información, reflejada en el nivel de cumplimiento de políticas, procedimientos y resultados de las evaluacionesdel conocimiento adquirido en los ejercicios de formación.

Gestionar de manera oportuna los incidentes, eventos y vulnerabilidades de seguridad de la información, adoptando procedimientos claros para el reporte, atención, tratamiento, seguimiento y aplicación de las lecciones aprendidas, con el fin de reducir la probabilidad e impacto de incidentes futuros.

Disponer de los recursos financieros, humanos y de infraestructura necesarios para mantener el adecuado desempeño del Sistema de Gestión de Seguridad de la Información de Contento BPS, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información Propia y de sus partes interesadas internas y externas.

Comunicación

La Política Corporativa de Seguridad de Información se dará a conocer a todas las partes interesadas identificadas en el contexto organizacional, por medio de los canales dispuestos por la compañía y definidos en el procedimiento de comunicación interna y externa. La presente políticaestará disponible como información documentada.

Revisión, Actualización y Seguimiento

Esta política será revisada anualmente o actualizarse en el momento en que existan modificaciones en el propósito, misión, visión, objetivos estratégicos o el contexto de la compañía; en el alcancedel Sistema de Gestión de Seguridad de la Información - SGSI o cuando existan cambios legales, estatutarios o reglamentarios.

Se deberá hacer seguimiento periódico al cumplimiento de las disposiciones aquí contenidas, porlo menos una vez al año.

Cumplimiento

Todos los integrantes, aliados, proveedores y demás partes interesadas, deberán dar cumplimiento al 100% de la política.

Dado en la ciudad de Medellín a los 08 días del mes de agosto del 2023 se aprueba por el Representante Legal.

DAVID RODRÍGUEZ DORALBA SIERRA

Representante Legal Líder de Seguridad de la Información

APROBACION Y OFICIALIZACION

FASES	**CARGO RESPONSABLE**	**NOMBRE**	**MEDIO POR EL CUAL SE APROBÓ**
Elaboración	Coordinadora de Seguridad de la Información	Doralba Sierra	Correo electrónico
Revisión			
Aprobación	Representante Legal	David Rodríguez	

MODIFICACIONES /ACTUALIZACIONES

VERSIÓN	**FECHA (año-mes)**	**DESCRIPCIÓN RESUMIDA DE LA MODIFICACIÓN / ACTUALIZACIÓN /ANULACIÓN**
00	2011-05	Creación
01	2013-	Actualización de Políticas por revisión anual

	05	
02	2015-03	Actualización de Políticas por revisión anual

03	2016-04	Actualización de Políticas por revisión anual
04	2016-12	Actualización de imagen corporativa
05	2018-01	Actualización de contenido
06	2018-09	Actualización de contenido
07	2018-12	Actualización de contenido
08	2019-04	Actualización de contenido
09	2019-05	Actualización de contenido
10	2020-09	Inclusión de disposiciones en cuanto a; Trabajo en casa, Teletrabajo, inclusión de Seguridad de la Información en todas las etapas de los proyectos emprendidos, y prohibiciones de uso de dispositivos personales para

		temas Corporativos
11	2021-09	Actualización de contenido
12	2022-02	Actualización de contenido
13	2022-04	Estructura del documento y actualización de contenido
14	2022-09	Actualización de contenido
15	2023-05	Actualización de objetivos, definiciones y redacción de la declaración de la política.
16	2023-06	Inclusión de controles para los integrantes de contento
17	2023-08	Inclusión de aplicativo de gestión de contraseñas

13.3. Anexo 3 Seguridad de la Información

(PR-SI-01) V10 202308
Documento interno

Objeto

Establecer medidas de Seguridad y Protección de la Información, realizando seguimientos y acciones de monitoreo y control, procediendo con los correctivos pertinentes por el Área Jurídica y GTO según los hallazgos obtenidos, así mismo establecer y coordinar la ejecución de las actividades que permitan que la Compañía se prepare para enfrentar un evento que afecte la continuidad del Negocio, bajo unos tiempos mínimos de recuperación.

Alcance

Inicia con el análisis de la normativa que aplica para la Compañía en cuanto a la Seguridad de la Información, pasando por la validación del cumplimiento en la infraestructura física y tecnológica, realizando seguimientos programados a los procesos procurando implementar controles en donde se pueden presentar riesgos en la confidencialidad, integridad y disponibilidad de la información.

Definiciones

Ciberseguridad: Es la práctica de proteger la información, los dispositivos móviles, lossistemas electrónicos, las redes y los datos de ataques maliciosos. También

se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

Información Confidencial: Es la información cuya divulgación no está autorizada paradarse a conocer a terceros o que puede ser manipulada con fines de daño o perjuicio parasu dueño o propietario.

Información Reservada: Es la que puede compartirse a nivel de empresa para realizar lagestión Propia del proceso, en este caso el Aliado Estratégico contractualmente permitesu uso.

Información General: Es aquella que esta publicada para todos.

Integridad de la Información: Esta determinada dentro de la organización como la maneraen que la información es controlada, para evitar cambios, que es coherente y completadesde su creación o recibo hasta la destrucción.

Disponibilidad de la información: Son los niveles de acceso de la información definido por la compañía siguiendo las obligaciones contractuales con el Aliado Estratégico.

Plan de Continuidad: plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro deun tiempo predeterminado después de una interrupción no deseada o desastre. En él se identifican las vulnerabilidades, detallan las medidas necesarias para evitar prolongados cortes de servicios, y se definen los pasos que se deben realizar para restablecerlo o activar la contingencia.

BIA: Análisis de Impacto del Negocio, cuenta con los siguientes componentes: Personalrequerido, Áreas de trabajo, Backups de información, Aplicativos críticos, Dependencias de otras áreas, Dependencias de terceras partes, Criticidad de los recursos de información, Participación del personal de seguridad informática y los usuarios finales,Análisis de todos los tipos de recursos de información.

Tratamiento de los riesgos: Prevenir, reducir, evitar o transferir, buscando eliminar la amenaza completamente, minimizar la probabilidad de que ocurra y/o minimizar su efecto.

Información: constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje.

Aliado Estratégico: Entidad a la que se le presta un servicio.

Contrato: Acuerdo de voluntades, verbal o escrito para formalizar la prestación de unservicio, estableciendo condiciones relativas especialmente al valor, tiempo y requisitospara la ejecución.

Condiciones Generales

Responsabilidades

Las responsabilidades generales y específicas de cada proceso están descritas en eldocumento Roles y Responsabilidades en SI (LI-SI-03)

Pasos Secuenciales

Cuando se presenta un cambio normativo que aplique a Seguridad de la Información

El proceso inicia con la recepción del cambio de normativa por entidades gubernamentales como la Superintendencia financiera, por las necesidades explicitas dadas en los pliegos de peticiones de las licitaciones.

La empresa CONTENTO BPS S.A, evalúa los cambios normativos, en cada uno de los ítems que afecten la seguridad de la información tanto física, locativa, procedimental y la manera en que se realizara la difusión de dichos cambios y adecuaciones al interiorde la empresa.

En la evaluación del cambio normativo se contemplará la afectación tanto de la Política de Seguridad de la Información como del Plan de Continuidad y Contingencia, determinando su actualización de ser necesaria.

De la evaluación a la normativa o licitación se contemplan los cambios físicos, procedimentales y/o tecnológicos requeridos.

De necesitarse estos cambios, se procede a planear y ejecutar, teniendo en cuenta los procesos de apoyo del sistema de gestión de calidad aplicando en cada proceso las actividades necesarias para su realización.

Una vez implementados los cambios se validarán si cumplen con lo definido por lanueva directriz y se continuará con el seguimiento.

Seguimientos periódicos al cumplimiento de las políticas de Seguridad de la Información

Realizar verificaciones periódicas a los equipos de cómputo para evaluar el cumplimiento de las políticas de seguridad de la información. Verificación de Condiciones Seguras (FO-SI-05)

Informar al líder de proceso respectivo los hallazgos detectados para su revisión ycorrección, cuando se trate de incumplimientos recurrentes se hará el registro del

Problema en el Formato de Reporte de Incidentes de S.I, y se tomaran los correctivos pertinentes para evitar la ocurrencia en los mismos (Procesos Disciplinarios).

Realizar verificaciones periódicas para el cumplimiento de la política trabajo en casa,teletrabajo o trabajo remoto

Realizar auditorías periódicas de cada área para evaluar el cumplimiento de las políticas de seguridad de la información.

Plan de Capacitación al Personal de la Compañía en Seguridad de la Información

el proceso de Gestión del Talento Organizacional notifica al Líder de Seguridad sobreel personal nuevo en la compañía.

El Líder de Seguridad diseñará y ejecutará la capacitación respectiva, haciendo una evaluación de conocimiento al finalizar ésta.

Si el empleado obtiene una nota inferior a tres puntos cinco (3.5) deberá recibir nuevamente la Inducción Corporativa y ser reevaluado

Cumplimiento de Política de Seguridad de la Información

El área de seguridad de la información notificara a la gerencia encargada de las anomalías que se detecten en la revisión de condiciones seguras, así como las recomendaciones de mejora para la toma de decisiones.

Acompañamiento en Licitaciones e Inicio de Nuevas Operaciones

Responder las licitaciones en las que se presente la Compañía en cuanto a los aspectos que tienen que ver con la Seguridad de la información y la continuidad del negocio, garantizando que se pueda cumplir con lo solicitado.

Hacer las validaciones de seguridad en cuanto a los aspectos operativos, técnicos y tecnológicos que pudieren afectar la Seguridad de la Información cuando defina el inicio de una operación.

Validar la aplicación de los controles que se definieron en la matriz de riesgos deSeguridad de la Información garantizando la mitigación de estos.

Reportar los hallazgos encontrados en la validación para que sean subsanados antes del inicio de la operación.

Construcción de Plan de Continuidad del Negocio

Acompañar el diligenciamiento de la Encuesta de BIA con cada uno de los procesosde la compañía que permite identificar los recursos que se requieren para el normal funcionamiento de la Empresa consolidándolos en el Análisis de Impacto en el Negocio

Acompañar en la construcción de la matriz de riesgos de la compañía en lo que se refiere a Seguridad de la información y a la continuidad del negocio y seleccionar las estrategias para el tratamiento que se le dará a cada uno de ellos.

Elaborar y socializar el Plan de Continuidad y contingencia.

Realizar anualmente el Plan Anual de pruebas Continuidad (PL-SI-03) con las áreascorrespondientes, el área encargada entregará un informe de su ejecución en el formato Informe pruebas de continuidad (FO-SI-04)

Revisar anualmente el plan de continuidad para hacer los ajustes respectivos garantizando que se encuentre siempre actualizado.

Manejo de atención de incidentes. Seguir las indicaciones Política de Gestión de incidentes

Control de activos de información. Según las indicaciones de la Política de Gestión de la Información.

Validar la disposición final de la información cuando pierde su vigencia. Según lasindicaciones del instructivo Destrucción y Borrado seguro

Registros

Política de seguridad de la información Manual de cumplimiento de Políticas de SIManejo de incidencias

Cifrado de la información

Política de Gestión de la InformaciónDestrucción y Borrado seguro Encuesta del BIA

Informe de pruebas plan de continuidad

Verificación de condiciones seguras en equipos de cómputo y terminales Inventario de activos de información

Plan de Continuidad y contingencia del Negocio.

BIA El Análisis de Impacto en el Negocio. Plan Anual de Pruebas de Continuidad

Reporte de Eventos e Incidentes de Seguridad de la InformaciónAcuerdo de confidencialidad

CONTROL DE RIESGOS

RIESGOS IDENTIFICADOS	**ACCIONES PARA PREVENIR**	**MECANISMOS DE CONTROL**
Incumplimiento de las normas legales vigentes regulan a Contento BPS por manejar información del sector financiero.	Consultar con el área jurídica el alcance de lasnormas, y mantenerse actualizado en el tema.	Consultar las entidades encargadas de generar las normas que aplican en materia de seguridad de la información.
Incumplimiento de los seguimientos internos programadas para garantizarla seguridad en la información.	Construir un documento para establecer las fechasy frecuencias de las auditorías.	Verificar la programación de auditorías internas establecida ygarantizar su cumplimiento.

DOCUMENTOS DE REFERENCIA

TIPO DE DOCUMENTO	Nº Y FECHA DE TIPO DE DOCUMENTO	NOMBRE
Norma Técnica	ISO 9001:2008	
Norma Técnica	ISO 19011:2011	Auditoría interna sistemas de Gestión
Manual	Noviembre 2016	Manual de calidad
Circular	042 de 2013	Circular de Seguridad de la Información
Ley	1581 de 2012	Protección de Datos

ANEXOSN/A

APROBACION Y OFICIALIZACION

FASES	CARGO RESPONSABLE	NOMBRE	MEDIO POR EL CUAL SE APROBÓ
Elaboración	Coordinadora de Seguridad de la Información	Doralba Sierra	N/A
Revisión			
Aprobación			

MODIFICACIONES /ACTUALIZACIONES

VERSIÓN	FECHA (año - mes)	DESCRIPCIÓN RESUMIDA DE LA MODIFICACIÓN / ACTUALIZACIÓN / ANULACIÓN
10	2023-08	Ajuste en contenido de los pasos secuenciales

09	2022-09	Actualización de contenido en responsabilidades
08	2020-11	Aclaraciones para trabajadores en casa y/o Teletrabajadores
07	2018-12	Actualización de información
06	2016-12	Actualización imagen
05	2016-08	Actualización objetivo
04	2016-06	Actualización de perfiles
03	2015-07	Actualización de contenido
02	2015-03	Actualización de logotipo corporativo
01	2014-11	Actualización de contenido y acople a procesos internos, actualización a manual de imagen
00	2013-09	Creación

13.4. Anexo 4 Manual de Cumplimiento de Políticas de Seguridad de la Información

(M-SI-01) V08 202301

Documento interno

Objetivo

Definir el propósito general de cada una de las políticas de seguridad de la informaciónestablecidas y aprobadas por Contento BPS, con el fin de proteger los Activos de Información, la tecnología utilizada para su Gestión y la Imagen de la compañía frente amenazas internas y externas, de manera que se dé cumplimiento a las propiedades de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la Información de la Organización.

Marco Sancionatorio

El incumplimiento de las disposiciones establecidas en las Políticas de Seguridad de laInformación de Contento BPS, tendrá como resultado la aplicación de procedimientos disciplinarios conforme al impacto de la falta, las obligaciones contractuales y el Reglamento Interno de Trabajo de Contento BPS S.A.

Introducción

La información es considerada como un recurso que como el resto de los activos de la Organización debe ser protegida en base al cumplimiento de los requisitos aplicables, con el objetivo de mantener los pilares de Integridad, Confidencialidad y Disponibilidad,

minimizando los riesgos de modificación, pérdida o daño; y contribuyendo de esta manera, tanto a una mejor gestión, como a dar cumplimiento a las obligaciones contractuales con los Aliados y terceras partes y a cumplir con la regulación del Estado para nuestro tipo de negocio.

Para que dicha contribución sea efectiva, es necesaria la implementación de una Política Corporativa de Seguridad de la Información que forme parte de la cultura Organizacional de Contento BPS, para lo cual debe contarse con el compromiso de todos los integrantes de la Compañía, para que en conjunto apoyen la difusión y cumplimiento de estas.

Con el propósito de que la implementación de la Cultura Organizacional de la Seguridad de la Información pueda realizarse en forma oportuna, la compañía define como responsable al Líder de Seguridad de la Información para la validación, coordinación y socialización de las Normas y Políticas para que Contento BPS pueda cumplir con los requisitos y condiciones aquí relacionadas.

Definiciones

Líder de Seguridad de la Información: Es la persona que cumple la función de supervisarel cumplimiento de la presente Política y todas las propuestas por la Organización en materia de Seguridad de la Información, y de capacitar a los integrantes de los cargos administrativos y que el área de GTO informe que lo requieran. (Fuente: Adaptado por Contento BPS:2022).

Propietario de la Información: Es la persona a quien la Compañía asigna como responsable del tratamiento de la información de cada uno de los Aliados según la obligación contractual adquirida. (Fuente: Adaptado por Contento BPS:2022).

Política: Intenciones y dirección de una organización, según lo expresado formalmentepor su alta dirección. (Fuente: ISO/IEC 21007: 2012).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar hasta qué punto se cumplen los criterios de auditoría. (Fuente: ISO/IEC 21007: 2012).

Ataque: "Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo". (Fuente: ISO/IEC 21007: 2012).

Autenticación: "Garantía de que una característica reivindicada de una entidad es correcta". (Fuente: ISO/IEC 21007: 2012).

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. (Fuente: ISO/IEC 21007: 2012).

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. (Fuente: ISO/IEC 21007: 2012).

Mejora continua: Actividad recurrente para mejorar el rendimiento. (Fuente: ISO/IEC 21007: 2012).

Control: Medida que modifica un riesgo. (Fuente: ISO/IEC 21007: 2012).

Información Documentada: Se refiere a la información necesaria que una organización debe controlar y mantener actualizada tomando en cuenta y el soporte en que se encuentra. La información documentada puede estar en cualquier formato (audio, video, ficheros de texto etc.) así como en cualquier tipo de soporte o medio independientemente de la fuente de dicha información. (Fuente: ISO/IEC 21007: 2012).

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias. (Fuente: ISO/IEC 21007: 2012).

Seguridad de Información: Preservación de la confidencialidad, integridad y disponibilidadde la información. (Fuente: ISO/IEC 21007: 2012).

Incidente de Seguridad de la Información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativade comprometer las operaciones comerciales y amenazar la seguridad de la información. (Fuente: ISO/IEC 21007: 2012).

Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información. (Fuente: ISO/IEC 21007: 2012).

Integridad: Propiedad de la exactitud y la integridad. (Fuente: ISO/IEC 21007: 2012).

Objetivo: Un objetivo se define como un resultado a lograr. Un objetivo puede ser estratégico, táctico u operacional. (Fuente: ISO/IEC 21007: 2012).

Proceso: Conjunto de actividades interrelacionadas o interactivas que transforman entradas en salidas. (Fuente: ISO/IEC 21007: 2012).

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado - positivo o negativo. (Fuente: ISO/IEC 21007: 2012).

Amenaza: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización. (Fuente: ISO/IEC 21007: 2012).

Alta Dirección: Persona o grupo de personas que dirige y controla una organización alnivel más alto. (Fuente: ISO/IEC 21007: 2012).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas. (Fuente: ISO/IEC 21007: 2012).

Sistema de Gestión de Seguridad de la Información

Objetivos

Administrar la seguridad de la información dentro de la compañía y establecer un marcogerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos autorizados a partes interesadas externas a la información de la Compañía.

Comité de Seguridad de la Información

Los integrantes que conforman este grupo han sido definidos por representantes de todas las áreas de la Compañía, garantizando el apoyo a las Políticas y actividades de Seguridad de la Información estipuladas por Contento BPS.

Secretaria General (Jurídico)

Líder de Seguridad de la Información

Vicepresidente Financiero

Líder Sistema de Gestión

Gerente de TIC

Líder de Mantenimiento y Seguridad Física

Líder de Gestión Documental

Vicepresidente de Operaciones

Gerente de Gestión de Talento Organizacional

Responsabilidades del Comité de Seguridad de la Información

Conocer y apoyar, cuando sea necesario, la gestión de los incidentes relativos a la Seguridad de la Información que se reporten en la Compañía.

Aprobar las propuestas para mantener y mejorar la Seguridad de la Información,de acuerdo con las competencias y responsabilidades asignadas a cada proceso, así como acordar y aprobar las metodologías y procesos pertinentes para su cumplimiento.

Promover la difusión y apoyo a la Seguridad de la Información dentro de la Compañía, así como, coordinar el proceso de administración de la continuidad de las actividades.

Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro y fuera de Contento BPS.

Responsabilidades en Materia de Seguridad de la Información

La Dirección General de Contento BPS asigna las funciones relativas a la Seguridad de laInformación de la Compañía al Líder de Seguridad de la Información, lo cual incluye lasupervisión de todos los aspectos inherentes a las políticas establecidas.

La definición de los campos de aplicación de la Seguridad de la Información se detalla acontinuación:

Seguridad de la Información por parte del Personal

Seguridad de la Información Física

Seguridad de la Información Digital

Seguridad de la Información en las Comunicaciones y las Operaciones

Seguridad de la Información en el Control de Acceso Físico

Seguridad de la Información en el Control de Acceso Lógico

Seguridad de la Información en el Desarrollo y Mantenimiento de Sistemas

Seguridad de la Información en la Planificación de la Continuidad del Negocio

Gestión de los Riesgos de seguridad de la Información

Gestión de Activos de Información

Si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, seguirán conservando la responsabilidad total del cumplimiento deestas.

6. Políticas de Seguridad de la Información

Contento BPS implementa una serie de Políticas de Seguridad de la Información consideradas como elementos imprescindibles para la oportuna y adecuada gestión dela Seguridad de la Información de la compañía. A su vez, los lineamientos descritos encada una de la Políticas de Seguridad de la Información son la evidencia principal pararespaldar el Sistema de Gestión de Seguridad de la Información (SGSI)**,** es decir, todas aquellas responsabilidades y buenas prácticas que ejercen todas las partes interesadas internas y externas en cuanto a la protección de la información.

Los beneficios de aplicar de manera efectiva las Políticas de Seguridad de la Información son de gran utilidad para el cumplimiento de los objetivos estratégicos de seguridad establecidos en la compañía.

La implementación de estos controles trae consigo los beneficios descritos a continuación:

Protección de los Activos de Información: Todos los activos de información definidos por la compañía (Información física y digital, hardware o infraestructura, conocimiento o intangibles, servicios y software).

Protección del Negocio y de sus Procesos: lo que se conoce como alineación estratégica.

Adoptar y adaptarse: a las necesidades Propias y exigidas para las mejores prácticas en materia de seguridad.

Definición de lineamientos: para determinar la conducta de los integrantes de la compañía a través de la definición de funciones y responsabilidades.

Marco normativo: Que determina la postura de la organización hacia la protección de sus activos por medio de la declaración de las actividades permitidas y aquellasque se prohíben.

Crear conciencia: entre el personal sobre la importancia de la información a la cual tiene acceso y los riesgos asociados a estos que pueden afectarlos e identificar la mejor estrategia para minimizar sus consecuencias o la frecuencia con la que se presentan.

Cumplimiento: Las políticas deben establecer lo necesario para estar alineadascon las leyes aplicables de acuerdo con la naturaleza del negocio, así como conlas regulaciones y obligaciones contractuales directamente relacionadas con seguridad de la información.

Las Políticas de Seguridad de la Información contienen las directrices necesarias parasalvaguardar la información Propia y de las demás partes interesadas externas para el cumplimiento contractual con Aliados Estratégicos, las cuales se describen a continuación y están detalladas en la ruta:

\Calidad\Seguridad de la Información

\Calidad\Tecnología y Comunicaciones

\Calidad\Desarrollo del talento e Innovación

\Calidad\Infraestructura física

\Calidad\Compras

1. Política Corporativa de Seguridad de la Información
2. Política Uso de Dispositivos Móviles y Conexión Remota
3. Política Escritorio físico y digital limpio
4. Política de Uso de Correo Electrónico y Redes Sociales

5. Política de Tratamiento de Datos Personales
6. Política de Respaldo de Información
7. Política de Relación con Proveedores
8. Política de Intercambio de Información
9. Política de Gestión Para Ciberataque
10. Política de Gestión de Incidentes
11. Política de Gestión de Activos
12. Política de Desarrollo Seguro
13. Política de Controles Criptográficos
14. Política de Continuidad del Negocio
15. Política de Ciberseguridad
16. Política Control de Acceso Lógico
17. Política Control de Acceso Físico
18. Política de Detección de Software Malicioso
19. Política de Directorio Activo
20. Política de Seguridad en la Red
21. Política de Seguridad de los Recursos Humanos
22. Política Cero Tolerancia al Fraude
23. Política de Seguridad de la información para Teletrabajo, Trabajo en Casa y TrabajoRemoto
24. Política de Gestión de Vulnerabilidades de SI
25. Política de Administración de Parches

El área de Seguridad de la Información realizará revisiones periódicas sobre la vigencia e implementación de las Políticas, a efectos de verificar el cumplimiento de los controles ylas buenas prácticas establecidas.

Contento BPS establece las medidas requeridas para la formación y toma de conciencia de su personal y partes interesadas en todos los aspectos relacionados con la seguridad de la información. A su vez, cuando los integrantes y/o las terceras partes interesadasincumplan alguna de las políticas de seguridad de la información, la Compañía se reserva el derecho de aplicar las medidas disciplinarias vigentes en la Empresa dentro del marco legal aplicable, y dimensionadas al impacto que tengan sobre la misma.

6.1 Política Corporativa de Seguridad de la Información

Esta Política está sustentada en lo establecido en las circulares de la Superintendencia financiera 052 y 022 que aplican para servicios tercerizados en todo lo relacionado conla seguridad de la información

La presente política se establece como cumplimiento al requisito 5.2 Política, de la norma ISO 27001:2022.

Contento BPS brinda orientación y apoyo a la Organización por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos de negocio de la compañía,y para generar capacidad de cumplimiento con las leyes y reglamentos pertinentes a losobjetivos del Sistema de Gestión de Seguridad de la Información.

Además de contener el compromiso de la alta dirección en la protección de la confidencialidad, integridad y disponibilidad de la información, también incluye su compromiso en el cumplimiento de requisitos legales aplicables de acuerdo a la naturaleza del negocio, así como también, en la mejora continua del Sistema de Gestión de Seguridad de la Información.

Por último, se encuentra definidos los 6 objetivos del Sistema de Gestión de Seguridad de la Información, los cuales delimitan los logros que la compañía desea alcanzar en términos de seguridad de la información.

6.8 Política de Intercambio de Información

El intercambio de información es una práctica utilizada entre entidades que requieren compartir información en forma oportuna o en tiempo real con el fin de obtener alta capacidad de desempeño de sus procesos. Esta práctica es constantemente amenazada por agentes internos y externos que no permiten un flujo adecuado para lograr su fin. Espor esto que los activos de información logran ser vulnerados y, por ende, se ve reflejado en la materialización de riesgos inherentes al proceso.

Dado lo anterior, esta política busca proteger la información de amenazas y brinda oportunidades de disminución de las vulnerabilidades asociadas.

Contento BPS establece y mantiene esquemas de seguridad para el intercambio de la información entre los procesos de la compañía y cualquier entidad externa (Aliado estratégico, ente regulador, proveedor, entre otros.) en línea con los acuerdos definidos e involucrados con la prestación de servicios; mediante la definición de canales de comunicación y de transferencia de información seguros desde el inicio de la relación contractual, de manera que permita garantizar la confidencialidad, integridad y disponibilidad de la información de ambas partes.

6.15 Política de Ciberseguridad

El uso de las tecnologías de la información y las comunicaciones trae consigo amenazas permanentes, ya que el avance de estas tecnologías ha incrementado el uso de estasherramientas con fines delictivos. Por tal motivo, Contento BPS implementa controles de Ciberseguridad para generar mecanismos que permitan garantizar la seguridad de la información de la compañía estableciendo además directrices y buenas prácticas (alineadas con las normas internacionales NIST y la norma ISO/IEC 27001:2022) relacionadas con Ciberseguridad para proteger los activos estratégicos de la Organización que dependen o usan las tecnologías de la información y las comunicaciones, generando cultura y compromiso en todos los procesos y operaciones de la compañía y garantizando la confiabilidad, imagen y credibilidad de Contento BPS y sus integrantes.

9 Consideraciones de Auditorías de Sistemas

9.1 Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas,se tomarán medidas en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

9.2 Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protege el acceso a los elementos utilizados en las auditorías de sistemas, es decir, archivos de datos o software, a fin de evitar el mal uso o el compromiso de la información y de los mismos.

9.3 Sanciones por Incumplimiento

Cualquier incumplimiento de lo dispuesto en las Políticas de Seguridad de la Información de la compañía, se sancionará conforme a lo dispuesto en los contratos y el Reglamento Interno de Trabajo.

DOCUMENTOS DE REFERENCIA

TIPO DE DOCUMENTO	Nº Y FECHA DE TIPO DEDOCUMENTO	NOMBRE
Circular	042 de 2012	Circular de Seguridad de la información
Ley	1581 de 2012	Protección de datos personales
Norma Técnica	ISO/IEC 27001:2022	Sistemas de Gestión de Seguridad de laInformación

APROBACION Y OFICIALIZACION

FASES	CARGO RESPONSABLE	NOMBRE	MEDIO POR EL CUAL SE APROBÓ
Elaboración	Coordinadora de Seguridad de la Información	Doralba Sierra	Correo electrónico
Revisión			
Aprobación			

CONTROL DE CAMBIOS

Versión	**Fecha (año mes)**	**Descripción resumida de la modificación / actualización / anulación**
00	2016-05	Creación
01	2016-12	Actualización de imagen y perfiles
02	2017-02	Actualización de información
03	2017-10	Actualización de información
04	2019-05	Actualización del Manual
05	2021-01	Actualización del Manual
06	2022-09	Adición de Políticas: Política de Gestión de Vulnerabilidades de SIPolítica de Administración de Parches

07	2022-12	Adiciones de política de control de acceso físico, eliminación de política de gestión de la información y ajuste en la redacción de políticas en general
08	2023-01	Actualización y ajustes en la redacción del contenido