RESOLUCIÓN No. 0085 DE 2021
(ABRIL 13)

"Por medio del cual se adopta un manual y unos formatos del Sistema de Gestión de Calidad de Bomberos de Bucaramanga"

LA DIRECCIÓN GENERAL DE BOMBEROS DE BUCARAMANGA

En uso de sus facultades Constitucionales, legales y en especial las conferidas en el Acuerdo No. 058 de 1987 del Concejo Municipal de Bucaramanga, y demás normas concordantes vigentes y complementarias y,

CONSIDERANDO

1. Que Bomberos de Bucaramanga es una entidad pública descentralizada adscrita al Municipio de Bucaramanga, con personería jurídica, autonomía administrativa y patrimonio independiente, creada mediante el Acuerdo No. 058 de 1987 del Concejo de Bucaramanga, que tiene por objeto principal, de conformidad con la Ley 1575 de 2012, la gestión integral del riesgo contra incendio, los preparativos y atención de rescates en todas sus modalidades y la atención de incidentes con materiales peligrosos, sin perjuicio de las atribuciones de las demás entidades que conforman el Sistema Nacional para la Prevención y Atención de Desastres.

2 Que de acuerdo con la Resolución No. 205 del dieciséis (16) de octubre de 2015 por la cual se ajustó el Manual Especifico de Funciones y Competencias Laborales, de Bomberos de Bucaramanga, es función de la Dirección General expedir los actos administrativos, de acuerdo con las facultades concedidas por la Ley y los reglamentos.

3. Que la Constitución Política en su artículo 209, establece:

> (…) *"La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley."*

4. Que con la relación a la implementación del Modelo Integrado de Planeación y Gestión (MIPG) así como el Sistema de Gestión de Calidad bajo la norma ISO 9001:2015, la entidad realizo la implementación del direccionamiento estratégico, con el objetivo de establecer el horizonte a corto y mediano plazo y focalizar todos los procesos en la consecución de los resultados definitivos.

5. Que mediante actas de reunión No. 09 del siete (7) de abril de 2021 que hace parte integral del presente Acto Administrativo, se aprobó por parte del Comité de Calidad el manual y los siguientes y formatos

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6522660 Línea Emergencias 119 – 123
Telefax Dirección General: 6522220

RESOLUCIÓN No. 0085 DE 2021
(ABRIL 13)

"Por medio del cual se adopta un manual y unos formatos del Sistema de Gestión de Calidad de Bomberos de Bucaramanga"

Proceso/Área	Nombres del documento	Fecha de acta de reunión o correo electrónico de aprobación del documento
Talento Humano	F-GT-SGC-110-005– Formato de contención de Incidentes de seguridad	7 de abril de 2021
	F-GT-SGC-110-006– Formato de registro de Incidentes de seguridad	
	M-GT-SGC-110-001 – Manual Protocolo de respuesta en el manejo de incidentes de seguridad en el tratamiento de datos personales.	
	F-TH-SGC-110-021 – Evaluación de desempeño laboral personal provisional	

En mérito de lo anteriormente expuesto, la Dirección General de Bomberos de Bucaramanga.

RESUELVE:

ARTÍCULO PRIMERO: ADOPTAR los el siguiente manual y formatos del Sistema de Gestión de Calidad de Bomberos de Bucaramanga:

Proceso/Área	Nombres del documento	Fecha de acta de reunión o correo electrónico de aprobación del documento
Talento Humano	F-GT-SGC-110-005– Formato de contención de Incidentes de seguridad	7 de abril de 2021
	F-GT-SGC-110-006– Formato de registro de Incidentes de seguridad	
	M-GT-SGC-110-001 – Manual Protocolo de respuesta en el manejo de incidentes de seguridad en el tratamiento de datos personales.	
	F-TH-SGC-110-021 – Evaluación de desempeño laboral personal provisional	

PARAGRAFO: El manual y formatos de que trata el presente Acto Administrativo hacen parte del mismo

RESOLUCIÓN No. 0085 DE 2021
(ABRIL 13)

"Por medio del cual se adopta un manual y unos formatos del Sistema de Gestión de Calidad de Bomberos de Bucaramanga"

ARTÍCULO SEGUNDO: DIVULGAR el presente acto administrativo a través de los medios de comunicación e información de la entidad.

ARTÍCULO TERCERO: DEROGAR los actos administrativo que sean contrarios a la presente resolución.

ARTÍCULO CUARTO: Enviar copia de la presente Resolución a la Dirección Administrativa y Financiera de la Entidad, para sus fines pertinentes.

ARTÍCULO QUINTO: RECURSOS contra la presente Resolución proceden los recursos de ley.

RTÍCULO SEXTO: VIGENCIA la presente Resolución rige a partir de la fecha de expedición.

COMUNÍQUESE Y CÚMPLASE,

Dada en Bucaramanga, a los trece (13) días del mes de abril de 2021.

[redacted]
YELITZA OLIVEROS RAMIREZ
Director General
Bomberos de Bucaramanga

Elaboró: Juan Manuel Lozada Riaño. Contratista Apoyo Jurídico
Revisó aspectos jurídicos: Dr. Deisy Yessenia Villamizar. Jefe Oficina Asesora Jurídica
Revisó aspectos administrativos: Dra. Dahidith Silvana Hernández Isidro. Directora Administrativa y Financiera

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX. 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

084 - 12-04-21

	FORMATO ACTA DE REUNIÓN	Código: F-GD-SGC-110-005
		Versión: 2.0
		Fecha Aprobación: Abril 27 de 2020
		Página: 1 de 1

Fecha:	07/04/2021	LUGAR: Sala de crisis			
ACTA N°	09	HORA INICIO:	11:00 a.m.	HORA FINAL:	11:30 a m.

OBJETIVO DE LA REUNION

Elaboración, revisión y aprobación de formatos de Gestión Tecnológica – Habeas data.

ASISTENTES

N°	NOMBRE	ÁREA
1	Javier Enrique Sandoval Gómez	Apoyo habeas Data.
2	Karen Daniela Landazábal Beltrán	Profesional Apoyo Calidad.

ORDEN DEL DÍA

1) Revisión de contenido de los formatos solicitados.
2) Elaboración de codificación y aprobación de los formatos.

DESARROLLO

De acuerdo a la solicitud realizada vía correo electrónico por el señor Javier Sandoval, referente a la creación de dos formatos y un manual correspondientes a contención de incidentes de seguridad, registro de incidentes de seguridad y manual de protocolo de respuesta en el manejo de incidentes de seguridad en el tratamiento de datos personales, respectivamente; posterior a la revisión del contenido el equipo de calidad procede a asignar la codificación de los mismos así:

- ✓ F-GT-SGC-110-005 Formato de Contención de Incidentes de Seguridad.
- ✓ F-GT-SGC-110-006 Formato de Registro de Incidentes de Seguridad.
- ✓ M-GT-SGC-110-001 Manual Protocolo de respuesta en el manejo de incidentes de seguridad en el tratamiento de datos personales.

COMPROMISOS

No.	DESCRIPCIÓN DE LA ACTIVIDAD	NOMBRE DEL RESPONSABLE	FECHA COMPROMISO
1	Incluir en la carpeta compartida de la entidad el formato codificado, así como su registro en el listado maestro de la dependencia.	Equipo Calidad	15/04/2021
2	Iniciar su implementación.	Gestión Tecnológica – Habeas Data	N/A

Asistentes:

NOMBRE	CARGO	FIRMA
Javier Enrique Sandoval Gómez	Apoyo habeas Data.	[redacted]
Karen Daniela Landazábal Beltrán	Profesional Calidad.	[redacted]

AUTORIZACIÓN DEL TRATAMIENTO DE DATOS PERSONALES. Como Titular de los datos personales autorizo a BOMBEROS DE BUCARAMANGA para realizar la recolección, almacenamiento, uso, circulación y/o supresión de mis datos personales aquí recolectados para las siguientes finalidades: 1) Dejar registro de la realización de la presente reunión. 2) Confirmar las personas que asistieron a la presente reunión. 3) Validar que las personas asistentes a la presente reunión tienen claridad acerca del desarrollo, conclusiones y compromisos establecidos en ella. Confirmo que he sido informado de tengo derecho a conocer, actualizar y rectificar mis datos personales, solicitar prueba de la presente autorización, ser informado sobre el uso que se ha dado a estos datos, presentar quejas ante la Superintendencia de Industria y Comercio por infracción a la ley, revocar la autorización y/o solicitar la supresión de sus datos en los casos en que sea procedente y acceder en forma gratuita a los mismos. Declaro conocer la Política de Tratamiento de Datos Personales de BOMBEROS DE BUCARAMANGA, la cual está disponible para su consulta en la página web www.bomberosdebucaramanga.gov.co/contenido/%20politica-proteccion-de-datos/

	FORMATO ACTA DE REUNIÓN	Código: F-GD-SGC-110-005
		Versión: 2.0
		Fecha Aprobación: Abril 27 de 2020
		Página: 1 de 1

Fecha:	07/04/2021	LUGAR: Sala de crisis			
ACTA N°	12	HORA INICIO:	2:30 p.m.	HORA FINAL:	3:00 p.m.

OBJETIVO DE LA REUNION

Elaboración, revisión y aprobación del formato para la evaluación de desempeño laboral del personal provisional (EDL).

ASISTENTES

N°	NOMBRE	ÁREA
1	Silvana Hernandez Isidro	Directora Administrativa
2	Jorge Peña Gonzalez	Capitán Operaciones
3	Karen Daniela Landazábal Beltrán	Apoyo Calidad.

ORDEN DEL DÍA

1) Revisión del formato de Evaluación de desempeño laboral EDL.
2) Aprobación del formato en comento.

DESARROLLO

De acuerdo a la solicitud realizada por la Dra. Silvana Hernandez Isidro, Directora Administrativa y financiera, re direcciona al equipo de calidad solicitud proviene del teniente Ochoa, referente a la adopción de un formato para la evaluación de desempeño laboral del personal provisional (EDL), y teniendo en cuenta que a la fecha no existe un formato documentado, el equipo de calidad toma el requerimiento y procede a elaborar la versión inicial del mismo, el cual mediante algunas reuniones fue modificado y actualizado hasta la versión final presentada (F-TH-SGC-110-021 FORMATO EVALUACION PROVISIONALES); por lo que se realiza su respectiva revisión y posterior aprobación.

COMPROMISOS

No.	DESCRIPCIÓN DE LA ACTIVIDAD	NOMBRE DEL RESPONSABLE	FECHA COMPROMISO
1	Incluir en la carpeta compartida de la entidad el formato actualizado	Equipo Calidad	30/04/2021
2	Iniciar su implementación.	Dirección Administrativa y financiera	N/A

Asistentes:

NOMBRE	CARGO	FIRMA
Silvana Hernandez Isidro	Directora Administrativa	[redacted]
Jorge Peña Gonzalez	Capitán Operaciones	[redacted]
Karen Daniela Landazábal Beltrán	Apoyo Calidad.	[redacted]

AUTORIZACIÓN DEL TRATAMIENTO DE DATOS PERSONALES. Como Titular de los datos personales autorizo a BOMBEROS DE BUCARAMANGA para realizar la recolección, almacenamiento, uso, circulación y/o supresión de mis datos personales aquí recolectados para las siguientes finalidades: 1) Dejar registro de la realización de la presente reunión. 2) Confirmar las personas que asistieron a la presente reunión. 3) Validar que las personas asistentes a la presente reunión tienen claridad acerca del desarrollo, conclusiones y compromisos establecidos en ella. Confirmo que he sido informado de tengo derecho a conocer, actualizar y rectificar mis datos personales, solicitar prueba de la presente autorización, ser informado sobre el uso que se ha dado a estos datos, presentar quejas ante la Superintendencia de Industria y Comercio por infracción a la ley, revocar la autorización y/o solicitar la supresión de sus datos en los casos en que sea procedente y acceder en forma gratuita a los mismos. Declaro conocer la Política de Tratamiento de Datos Personales de BOMBEROS DE BUCARAMANGA, la cual está disponible para su consulta en la página web www.bomberosdebucaramanga.gov.co/contenido/%20politica-proteccion-de-datos/

	EVALUACIÓN DE DESEMPEÑO LABORAL PERSONAL PROVISIONAL BOMBEROS DE BUCARAMANGA	Código: F-TH-SGC-110-021
		Versión: 0.0
	INFORMACIÓN GENERAL Y ACUERDO DE COMPROMISOS LABORALES	Fecha de aprobación: Abril 8 de 2021
		Página 1 de 1

LA PRESENTE EVALUACION DEL DESEMPEÑO NO GENERA DERECHOS DE CARRERA (RESOLUCION 0227 DEL 27 DE FEBRERO DE 2017)

PERÍODO DE EVALUACIÓN	DIA	MES	AÑO	Hasta	DIA	MES	AÑO	FECHA DE DILIGENCIAMIENTO	DIA	MES	AÑO

EVALUACIÓN INICIAL	X	EVALUACIÓN POR AJUSTES	
EVALUACIÓN INICIAL	**X**	**EVALUACIÓN POR AJUSTES**	

INTERVINIENTES	IDENTIFICACIÓN	EVALUADO	EVALUADOR (Jefe Inmediato)	EVALUADOR (Funcionario de Libre Nombramiento y Remoción en caso de constituir Comisión Evaluadora)
	Nombre Completo			
	Documento de Identidad			
	Nivel Jerárquico y Denominación del Empleo			
	Dependencia o Área Funcional			

PROPÓSITO PRINCIPAL DEL EMPLEO OBJETO DE LA EVALUACIÓN

Ejecutar los protocolos previstos en la Ley y la reglamentación interna de la entidad para la gestión integral del riesgo contra incendios, los preparativos y atención de rescates en todas sus modalidades, y la tención de incidentes con materiales peligrosos, en el Municipio de Bucaramanga, y las zonas definidas por Convenios, teniendo en cuenta las funciones, responsabilidades y visión en el ejercicio del cargo, y la misión institucional.

COMPROMISOS LABORALES

	Metas de la Dependencia a las cuales contribuye el empleo	Compromisos Laborales Pactados con sus Condiciones de Resultado	Evidencias o Soportes	Porcentaje de Cumplimiento Pactado (Entre 1% y 100%)	% de Avance durante el Semestre	% de Avance durante el Semestre	TOTAL
1				20%	100%	100%	100%
2				20%	100%	100%	100%
3				20%	100%	100%	100%
4				20%	100%	100%	100%
5				20%	100%	100%	100%
	CANTIDAD DE COMPROMISOS LABORALES PACTADOS	**5**	**TOTAL**	**100%**	**100,0%**	**100,0%**	**100%**

FIRMA DEL EVALUADO	FIRMA DEL JEFE INMEDIATO	FIRMA DEL FUNCIONARIO DE LIBRE NOMBRAMIENTO Y REMOCIÓN	Renuencia del Evaluado para firmar el formulario	NOMBRE DEL TESTIGO	FIRMA DEL TESTIGO	FECHA (dd/mm/aa)

RECLAMACIÓN EN ÚNICA INSTANCIA ANTE LA COMISIÓN DE PERSONAL (Num 5.8 Art. 5 Acuerdo 137 de 2010)		DECISIÓN DE LA COMISIÓN DE PERSONAL	MOTIVACIÓN DE LA DECISIÓN
Número de Radicado			
Fecha Reclamación (dd/mm/aa)			

	EVALUACIÓN DE DESEMPEÑO LABORAL PERSONAL PROVISIONAL BOMBEROS DE BUCARAMANGA	Código: F-TH-SGC-110-021
		Versión: 0.0
	INFORMACIÓN GENERAL Y ACUERDO DE COMPROMISOS LABORALES	Fecha de aprobación: Abril 8 de 2021
		Página 2 de 7

LA PRESENTE EVALUACION DEL DESEMPEÑO NO GENERA DERECHOS DE CARRERA (RESOLUCION 0227 DEL 27 DE FEBRERO DE 2017)

PERÍODO DE EVALUACIÓN	DIA	MES	AÑO	Hasta	DIA	MES	AÑO	FECHA DE DILIGENCIAMIENTO	DIA	MES	AÑO
	0	0	0								
EVALUACIÓN INICIAL		X	EVALUACIÓN POR AJUSTES								

INTERVINIENTES	IDENTIFICACIÓN	EVALUADO	EVALUADOR (Jefe Inmediato)	EVALUADOR (Funcionario de Libre Nombramiento y Remoción en caso de constituir Comisión Evaluadora)
	Nombre Completo	0	0	0
	Documento de Identidad	0	0	0
	Nivel Jerárquico y Denominacion del Empleo	0	0	0
	Dependencia o Área Funcional	0	0	0

PROPÓSITO PRINCIPAL DEL EMPLEO OBJETO DE LA EVALUACIÓN

PERMANECER SIEMPRE EN ESTADO DE ALISTAMIENTO PARA ATENDER LAS EMERGENCIAS, OPERACIONES DE RESCATE EN SALVAMENTO, SINIESTROS Y CALAMIDADES PUBLICAS AL IGUAL QUE LA PRESTACION DE LOS SERVICIOS INHERENTES A LA ENTIDAD.

COMPROMISOS COMPORTAMENTALES

	Competencia - Descripción	Conducta Asociada	Semestre I % de Avance durante el Semestre	Semestre II % de Avance durante el Semestre	Porcentaje promedio de Cumplimiento Pactado (Entre 1% y 100%) suma I y II	TOTAL AVANCE POR COMPONENTE
1	UNIFORMIDAD y PRESENTACION Personal utiliza con respeto y adecuadamente los uniformes y dotaciones intitucionales de que dispone	Usa y mantiene el uniforme y ropa de trabajo de acuerdo a protocolos y lineamientos establecidos por Bomberos de Bucaramanga	100%	100%	100%	100%
		Se presenta a las formaciones con el uniforme completo y en orden	100%	100%	100%	
		Mantiene pla presentación personal acorde a la dignidad de bombero	100%	100%	100%	
2	ORIENTACIÓN AL USUARIO Y AL CIUDADANO - Dirigir las decisiones y acciones a la satisfacción de las necesidades e intereses de los usuarios internos y externos, de conformidad con las responsabilidades públicas asignadas a la entidad.	• Atiende y valora las necesidades y peticiones de los usuarios y de ciudadanos en general.	100%	100%	100%	100%
		•Establece diferentes canales de comunicación con el usuario para conocer sus necesidades y propuestas y responde a las mismas.	100%	100%	100%	
		Da respuesta oportuna a las necesidades de los usuarios de conformidad con el servicio que ofrece la entidad.	100%	100%	100%	
3	DISCIPLINA Adaptarse a las políticas institucionales y buscar información de los cambios en la autoridad competente.	•Acepta instrucciones aunque se difiera de ellas.	100%	100%	100%	100%
		•Realiza los cometidos y tareas del puesto de trabajo. . Acepta la supervisión constante.	100%	100%	100%	
		•Realiza funciones orientadas a apoyar la acción de otros miembros de la organización.	100%	100%	100%	
4	COMPROMISO CON LA ORGANIZACIÓN Realizar las funciones y cumplir los compromisos organizacionales con eficacia y calidad.	Cumplo con oportunidad en función de estándares, objetivos y metas establecidas por la entidad, las funciones que le son asignadas.	100%	100%	100%	98%
		• Asume la responsabilidad por sus resultados. • Compromete recursos y tiempos para mejorar la productividad tomando las medidas necesarias para minimizar los riesgos.	100%	100%	100%	
		• Realiza todas las acciones necesarias para alcanzar los objetivos propuestos enfrentando los obstáculos que se presentan.	100%	100%	95%	

CANTIDAD DE COMPROMISOS LABORALES PACTADOS	4	TOTAL CALIFICACION		100,00%	100,0%	100%	100%
FIRMA DEL EVALUADO	FIRMA DEL JEFE INMEDIATO	FIRMA DEL FUNCIONARIO DE LIBRE NOMBRAMIENTO Y REMOCIÓN	Renuencia del Evaluado para firmar el formulario	NOMBRE DEL TESTIGO	FIRMA DEL TESTIGO		FECHA (dd/mm/aa)

RECLAMACIÓN EN ÚNICA INSTANCIA ANTE LA COMISIÓN DE PERSONAL (Num 5.8 Art. 5 Acuerdo 137 de 2010)		DECISIÓN DE LA COMISIÓN DE PERSONAL	MOTIVACIÓN DE LA DECISIÓN
Número de Radicado			
Fecha Reclamación (dd/mm/aa)			

	EVALUACIÓN DE DESEMPEÑO LABORAL PERSONAL PROVISIONAL **BOMBEROS DE BUCARAMANGA**	Código: F-TH-SGC-110-021 Versión: 0.0 Fecha de aprobación: Abril 8 de 2021 Página 3 de 7
	INFORMACIÓN GENERAL Y ACUERDO DE COMPROMISOS LABORALES	

LA PRESENTE EVALUACION DEL DESEMPEÑO NO GENERA DERECHOS DE CARRERA (RESOLUCION 0227 DEL 27 DE FEBRERO DE 2017)

COMPETENCIAS COMPORTAMENTALES			**SEGUIMIENTO**			
			I SEMESTRE		**II SEMESTRE**	
Tipo de Competencia	**Competencia**	**Conducta Asociada**	**Fortalezas**	**Aspectos a Corregir**	**Fortalezas**	**Aspectos a Corregir**
Uniformidad y presentación personal	UTILIZA CON RESPETO Y ADECUADAMENTE LOS UNIFORMES Y DOTACIONES INTITUCIONALES DE QUE DISPONE	Usa y mantiene el uniforme y ropa de trabajo de acuerdo a protocolos y lineamientos establecidos por Bomberos de Bucaramanga				
		Se presenta a las formaciones con el uniforme completo y en orden				
		Mantiene pla presentación personal acorde a la dignidad de bombero				
Disciplina	ADAPTARSE A LAS POLITICAS INSTITUCIONALES Y BUSCAR INFORMACION DE LOS CAMBIO EN LA AUTORIDAD COMPETENTE	ACEPTA Y SE ADAPTA FACILMENTE LOS CAMBIOS				
		RESPONDE AL CAMBIO CON FLEXIBILIDAD				
		PROMUEVE EL CAMBIO				
Orientación al usuario y al ciudadano	Dirigir las decisiones y acciones a la satisfacción de las necesidades e intereses de los usuarios internos y externos, de conformidad con las responsabilidades públicas asignadas a la entidad.	• Atiende y valora las necesidades y peticiones de los usuarios y de ciudadanos en general.				
		•Establece diferentes canales de comunicación con el usuario para conocer sus necesidades y propuestas y responde a las mismas.				
		•Considera las necesidades de los usuarios al diseñar proyectos o servicios. •Da respuesta oportuna a las necesidades de los usuarios de conformidad con el servicio que ofrece la entidad. •Reconoce la interdependencia entre su trabajo y el de otros.				

FIRMA DEL EVALUADO	**FIRMA DEL JEFE INMEDIATO**	**FIRMA DEL FUNCIONARIO**	**Renuncia del Evaluado para firmar el formulario**	**NOMBRE Y FIRMA DEL TESTIGO**

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119–129–139
Telefax: Dirección General: 6522220

	EVALUACIÓN DE DESEMPEÑO LABORAL PERSONAL PROVISIONAL BOMBEROS DE BUCARAMANGA		Código: F-TH-SGC-110-021
			Versión: 0.0
	INFORMACIÓN GENERAL Y ACUERDO DE COMPROMISOS LABORALES		Fecha de aprobación: Abril 8 de 2
			Página 4 de 7

LA PRESENTE EVALUACION DEL DESEMPEÑO NO GENERA DERECHOS DE CARRERA (RESOLUCION 0227 DEL 27 DE FEBRERO DE 2017)

EVALUADO	Nombre Completo		Documento de Identidad	
	Nombre Completo		Dependencia o Area Funcional	

EVIDENCIAS

Compromiso Laboral al que apunta la Evidencia	Descripción de la Evidencia	Fecha de inclusión en el Portafolio (dd/mm/aa)	Observaciones	Evidencia Aportada p

FIRMA DEL EVALUADOR		**FIRMA DEL EVALUADO**	

EXCELENCIA Y COMPROMISO

	EVALUACIÓN DE DESEMPEÑO LABORAL PERSONAL PROVISIONAL BOMBEROS DE BUCARAMANGA	Código: F-TH-SGC-110-021
		Versión: 0.0
	INFORMACIÓN GENERAL Y ACUERDO DE COMPROMISOS LABORALES	Fecha de aprobación: Abril 8 de 2021
		Página 5 de 7

LA PRESENTE EVALUACION DEL DESEMPEÑO NO GENERA DERECHOS DE CARRERA (RESOLUCION 0227 DEL 27 DE FEBRERO DE 2017)

EVALUADO	Nombre Completo	0	Documento de Identidad	0
	Nivel Jerarquico y Denominación	0	Dependencia o Area	0
EVALUADOR Jefe Inmediato	Nombre Completo	0	Documento de Identidad	0
	Nivel Jerarquico y Denominación	0	Dependencia o Area	0
EVALUADOR Libre Nombramiento y Remoción	Nombre Completo	#¡VALOR!	Documento de Identidad	#¡VALOR!
	Nivel Jerarquico y Denominación	0	Dependencia o Area	#¡VALOR!

#¡VALOR!

EVALUACION DEL PRIMER SEMESTRE - COMUNICACION -

% Avance Evaluación 1er Semestre	100%	Fecha de la Evaluación DIA	MES	AÑO

Firma del Servidor Público Evaluado _____

Firma del Jefe Inmediato _____

Firma del Funcionario de Libre Nombramiento y Remoción en caso de constituir Comisión Evaluadora _____

EVALUACION DEL SEGUNDO SEMESTRE- COMUNICACION -

% Avance Evaluación 2º Semestre	100%	Fecha de la Evaluación DIA	MES	AÑO

Firma del Servidor Público Evaluado _____

Firma del Jefe Inmediato _____

Firma del Funcionario de Libre Nombramiento y Remoción en caso de constituir Comisión Evaluadora _____

CALIFICACION DEFINITIVA - NOTIFICACION -

Calificación Definitiva	100%	Fecha de la Notificación DIA	MES	AÑO

DESTACADO

Firma del Servidor Público Evaluado _____

Firma del Jefe Inmediato _____

CALIFICACION DEL NIVEL SOBRESALIENTE

¿Es posible acceder a la calificación en el Nivel Sobresaliente? SI

FACTORES DEL NIVEL SOBRESALIENTE	CUMPLIMIENTO
Evaluación de la Gestión por Dependencias	NO CUMPLE
Por calidad y oportunidad	
Por aportes, propuestas o iniciativas adicionales	
Por iniciativas tendientes a acciones proactivas en las actividades que cumplió	
Por participación y aprovechamiento de capacitación relacionada con las actividades propias del empleo y que genere un valor agregado para la entidad o la dependencia	
Por participación en grupos o en actividades que requieren de disposición voluntaria	

CANTIDAD DE FACTORES DEL NIVEL SOBRESALIENTE CUMPLIDOS 0

MOTIVACION DE LA CALIFICACION DEFINITIVA

INTERPONE RECURSOS	SI	NO

FECHA Y NUMERO DE RADICACION DEL RECURSO

RECURSOS

PRIMERA INSTANCIA

		(dd/mm/aa)	MOTIVACION
CONFIRMA			
MODIFICA			
REVOCA			

NOMBRE DEL SERVIDOR PÚBLICO NOTIFICADO	
FIRMA DEL SERVIDOR PÚBLICO NOTIFICADO	
NOMBRE DEL NOTIFICADOR	
FIRMA DEL NOTIFICADOR	

SEGUNDA INSTANCIA

		(dd/mm/aa)	MOTIVACION
CONFIRMA			
MODIFICA			
REVOCA			

NOMBRE DEL SERVIDOR PÚBLICO NOTIFICADO	
FIRMA DEL SERVIDOR PÚBLICO NOTIFICADO	
NOMBRE DEL NOTIFICADOR	
FIRMA DEL NOTIFICADOR	

CALIFICACIÓN DEFINITIVA

CALIFICACIÓN DEFINITIVA EN FIRME		FIRMA DEL NOTIFICADO		FIRMA DEL NOTIFICADOR	
CALIFICACIÓN DEFINITIVA	100%	DESTACADO Y 0 FACTORES DE CUMPLIMIENTO.			

EXCELENCIA Y COMPROMISO

	EVALUACIÓN DE DESEMPEÑO LABORAL PERSONAL PROVISIONAL BOMBEROS DE BUCARAMANGA	Código: F-TH-SGC-110-021 Versión: 0.0 Fecha de aprobación: Abril 8 de 2021 Página 6 de 7
	INFORMACIÓN GENERAL Y ACUERDO DE COMPROMISOS LABORALES	

LA PRESENTE EVALUACION DEL DESEMPEÑO NO GENERA DERECHOS DE CARRERA (RESOLUCION 0227 DEL 27 DE FEBRERO DE 2017)

EVALUADO	Nombre Completo		Documento de Identidad	
	Nivel Jerarquico y Denominación		Dependencia o Area Funcional	
CIRCUNSTANCIA DE LA EVALUACIÓN				
EVALUADOR Jefe Inmediato	Nombre Completo		Documento de Identidad	
	Nivel Jerarquico y Denominación		Dependencia o Area Funcional	
EVALUADOR Libre Nombramiento y Remoción	Nombre Completo		Documento de Identidad	
	Nivel Jerarquico y Denominación		Dependencia o Area Funcional	

Período Evaluado	DIA		MES		AÑO		al	DIA		MES		AÑO	

EVALUACIÓN PARCIAL EVENTUAL

Compromisos Laborales Pactados	Estado de Avance de los Compromisos	Porcentaje de Cumplimiento Pactado por Semestre (Entre 1% y 100%)	No. De Días A evaluar	Porcentaje de Cumplimiento por Días Laborados	Porcentaje de Cumplimiento Efectivamente Alcanzado
0		20%		0,00%	
0		20%	0	0,00%	
0		20%	0	0,00%	

COMUNICACIÓN DE LA EVALUACIÓN PARCIAL EVENTUAL

EVALUACIÓN PARCIAL EVENTUAL EFECTUADA EN EL 1er.PERÍODO

Fecha de la Evaluación		
DIA	MES	AÑO

Firma del Servidor Público Evaluado _____

Firma del Jefe Inmediato _____

Firma del Funcionario de Libre Nombramiento y Remoción en caso de constituir Comisión Evaluadora _____

EVALUACIÓN PARCIAL EVENTUAL EFECTUADA EN EL 2do. PERÍODO

Fecha de la Evaluación		
DIA	MES	AÑO

Firma del Servidor Público Evaluado _____

Firma del Jefe Inmediato _____

Firma del Funcionario de Libre Nombramiento y Remoción en caso de constituir Comisión Evaluadora _____

Consolidado Ev. Parciales Eventuales

	Ev. Parcial Eventual	# Días	% Alcanzado
Primer Semestre	1		
	2		
	3		
	4		
	5		
	6		
Segundo Semestre	7		
	8		
	9		
	10		
	11		
	12		
TOTAL			0%

EXCELENCIA Y COMPROMISO

	EVALUACIÓN DE DESEMPEÑO LABORAL PERSONAL PROVISIONAL BOMBEROS DE BUCARAMANGA	Código: F-TH-SGC-110-021
		Versión: 0.0
	INFORMACIÓN GENERAL Y ACUERDO DE COMPROMISOS LABORALES	Fecha de aprobación: Abril 8 de 2021
		Página 7 de 7

LA PRESENTE EVALUACION DEL DESEMPEÑO NO GENERA DERECHOS DE CARRERA (RESOLUCION 0227 DEL 27 DE FEBRERO DE 2017)

EVALUADO	Nombre Completo		Documento de Identidad	
	Nivel Jerarquico y Denominación		Dependencia o Area Funcional	
EVALUADOR Jefe Inmediato	Nombre Completo		Documento de Identidad	
	Nivel Jerarquico y Denominación		Dependencia o Area Funcional	
EVALUADOR Libre Nombramiento y Remoción	Nombre Completo		Documento de Identidad	
	Nivel Jerarquico y Denominación		Dependencia o Area Funcional	

Compromisos Laborales Pactados con sus Condiciones de Resultado	Estado de Cumplimiento de los Compromisos	Evidencias	Porcentaje de Cumplimiento Pactado (Entre 1% y 100%)	Porcentaje Obtenido (Entre 1% y 100%)
0		0	20%	
0		0	20%	
0		0	20%	
		TOTAL	60%	0%

MOTIVACIÓN DE LA CALIFICACIÓN EXTRAORDINARIA DEFINITIVA

Firma del Evaluador y Fecha de la Evaluación Extraordinaria

DIA	MES	AÑO

NOTIFICACIÓN

Nombre del Evaluado _____

Firma del Servidor Público Evaluado _____

Nombre del Jefe Inmediato _____

Firma del Jefe Inmediato _____

RECURSO

SI	
NO	

FECHA Y NUMERO DE RADICACIÓN DEL RECURSO

RECURSOS

PRIMERA INSTANCIA				SEGUNDA INSTANCIA			
CONFIRMA		(dd/mm/aa)	MOTIVACIÓN	CONFIRMA		(dd/mm/aa)	MOTIVACIÓN
MODIFICA				MODIFICA			
REVOCA				REVOCA			
NOMBRE DEL SERVIDOR PÚBLICO NOTIFICADO				NOMBRE DEL SERVIDOR PÚBLICO NOTIFICADO			
FIRMA DEL SERVIDOR PÚBLICO NOTIFICADO				FIRMA DEL SERVIDOR PÚBLICO NOTIFICADO			
NOMBRE DEL NOTIFICADOR				NOMBRE DEL NOTIFICADOR			
FIRMA DEL NOTIFICADOR				FIRMA DEL NOTIFICADOR			

CALIFICACIÓN DEFINITIVA

CALIFICACIÓN DEFINITIVA EN FIRME		FIRMA DEL NOTIFICADO		FIRMA DEL NOTIFICADOR	

EXCELENCIA Y COMPROMISO

CONTENIDO

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

1. OBJETIVO

Establecer los parámetros y reglas para que **BOMBEROS DE BUCARAMANGA** actúe de forma rápida, ordenada y eficaz ante cualquier incidente que afecte la confidencialidad, disponibilidad e integridad de los datos personales bajo su protección.

2. ALCANCE

Las disposiciones contenidas en el presente documento se aplicarán en los casos en que se presenten vulneraciones a los archivos físicos y a los sistemas de información donde se realizan operaciones de tratamiento de datos personales, esto es: recolección, almacenamiento, uso y circulación de dichos datos.

3. GLOSARIO

Para la interpretación del presente protocolo se comparten las siguientes definiciones:

3.1. Acceso
Con relación a la seguridad de la información se refiere a la identificación, autenticación y autorización de una persona a los sistemas, recursos y áreas de la entidad en un momento dado.

3.2. Acceso físico
Significa ingresar a las instalaciones o a las diferentes dependencias o áreas de la entidad.

3.3. Acceso lógico
Es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información.

3.4. Amenaza
Cualquier factor de riesgo con suficiente potencial para provocar un daño o perjuicio a los Titulares sobre cuyos datos de carácter personal se realiza un tratamiento.

3.5. Base de Datos
Conjunto organizado de datos personales que sea objeto de Tratamiento.

3.6. Brecha de Seguridad
Es el resultado no autorizado de una serie de eventos realizados por un agente que aprovechan o explotan vulnerabilidades de un servicio, tecnología, sistema de información o base de datos.

3.7. Dato personal
Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que permita identificar a una persona natural.

3.8. Encargado del tratamiento
Es la persona natural o jurídica, pública o privada que, solo o conjuntamente con otros, trata datos personales por cuenta de la entidad, quien es el Responsable del tratamiento. La institución también podrá ser Encargado del tratamiento de terceros que Responsables de los datos personales.

3.9. Equipo de gestión de incidentes
Equipo experto en seguridad encargado de evaluar y gestionar la resolución de incidentes de seguridad que pudieran causar algún impacto en la entidad.

3.10. Evento de seguridad
Presencia identificada de una condición, que indica posible incumplimiento a la política de protección de datos personales o fallas de las medidas de seguridad.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

3.11. Gestión de riesgos
Es el conjunto de actividades y tareas que permiten controlar la incertidumbre relacionada con una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación.

3.12. Incidente de seguridad.
Un Incidente de seguridad de datos personales se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado a datos personales que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado.

3.13. Impacto
Se refiere al "resultado negativo" ocasionando por la materialización de una amenaza.

3.14. Oficial de Protección de Datos Personales
Es la persona que deberá velar por la implementación efectiva de las políticas y procedimientos, así como implementar las mejores prácticas; además de administrar el Sistema de Protección de Datos Personales.

3.15. Probabilidad
Se entiende como la posibilidad de que cierta amenaza se materialice.

3.16. Responsable del Tratamiento
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre los datos personales y/o el Tratamiento de ellos.

3.17. Riesgo
Se puede definir como la combinación entre: la posibilidad de que se materialice una amenaza y sus consecuencias negativas o impactos negativos.

3.18. Titular
Persona natural propietaria de los datos sobre los cuales la entidad realiza cualquier tipo de tratamiento.

3.19. Tratamiento
Cualquier operación o procedimiento, sea automatizado o no, que permita la recolección, almacenamiento, uso, circulación y/o supresión (RAUCS).

3.20. Usuario
Persona que utiliza un sistema informático, incluyendo equipos de cómputo, equipos de impresión, o sistemas de información.

3.21. Vulnerabilidad
Capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

4. DOCUMENTOS DE REFERENCIA

4.1. Guía de Implementación del Principio de la Responsabilidad Demostrada de la Superintendencia de Industria y Comercio.

4.2. Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales"

4.3. Plan Estratégico de las Tecnologías de la Información – PETI - de BOMBEROS DE BUCARAMANGA.

4.4. Modelo Integrado de Planeación y Gestión - MIPG - de BOMBEROS DE BUCARAMANGA.

4.5. NTC ISO 27001:2013. Sistemas de gestión de la seguridad de la información (SGSI).

4.6. NTC-ISO 31000:2018. Directrices para Gestionar el Riesgo.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

5. MARCO LEGAL

5.1. Artículo 15 de la Constitución Política. Por el cual se establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

5.2. Ley Estatutaria 1581 de 2012 por la cual se establecen las disposiciones para la protección de los datos personales.

5.3. Decreto 1377 de 2013, integrado en el Capítulo 25 del Decreto Reglamentario 1074 de 2015, por el cual se reglamenta la Ley 1581 de 2012.

5.4. Capítulo II del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

6. DESARROLLO

6.1. ¿QUÉ ES UN INCIDENTE DE SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES?

Es cualquier evento en los sistemas de información o bases de datos manuales o sistematizadas, que ocasionen violación a los códigos de seguridad o la pérdida, robo, consulta, uso, circulación, acceso no autorizado o fraudulento, destrucción, o alteración accidental o ilícita de los datos personales que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado.

6.2. TIPOS DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES

Los incidentes de seguridad en el Tratamiento de los Datos Personales pueden clasificarse dependiendo del grado de pérdida de las siguientes características de la información:

6.2.1. Afecta la Confidencialidad de los datos personales
Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Confidencialidad de los datos personales, siendo ésta, la característica que evita la divulgación de la información a personas o procesos que no estén debidamente autorizados.

Ejemplo: Cualquier acceso no autorizado a los datos personales.

6.2.2. Afecta la Disponibilidad de los datos personales
Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Disponibilidad de los datos personales, que es la característica que garantiza el acceso a la información por las personas o procesos autorizados, siempre que sea requerida.

Ejemplo: Caída en los sistemas de información, ataques de denegación de servicio

6.2.3. Afecta la Integridad de los datos personales
Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Integridad de los datos personales que es aquél que garantiza que la información se mantenga, tal como fue recolectada o generada, sin alteraciones o modificaciones no solicitadas o autorizadas.

Ejemplo: Alteración en los datos personales frente a los datos entregados por el titular, sin trazabilidad de solicitud de actualización.

6.2.4. Afecta Confidencialidad y Disponibilidad de los datos personales
Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad y disponibilidad de los datos personales.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

Ejemplo: Acceso no autorizado a la base de datos personales y eliminación de algunos o todos los datos personales encontrados en la misma.

6.2.5. Afecta Confidencialidad e Integridad de los datos personales

Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad e Integridad de los datos personales.

Ejemplo: Acceso no autorizado a la base de datos personales y adulteración de algunos o todos los datos personales encontrados en la misma.

6.2.6. Afecta Disponibilidad e Integridad de los datos personales

Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la disponibilidad e Integridad de los datos personales.

Ejemplo: Acceso autorizado a la base de datos personales con adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

6.2.7. Afecta la Confidencialidad, Disponibilidad e Integridad de los datos personales

Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad, disponibilidad e integridad de los datos personales

Ejemplo: Acceso no autorizado a la base de datos con información personal y adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

6.3. FACTORES PARA ESTABLECER EL TIPO DE INCIDENTE DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

Los factores que se pueden considerar a la hora de establecer el tipo de los incidentes de seguridad en el tratamiento de datos personales son, entre otros:

a. Tipo de amenaza: código dañino, intrusiones, fraude, etc. Se trata de una breve descripción del incidente en función de la información de la que se disponga.

b. Contexto u origen de la amenaza: interna o externa.

c. Categoría de seguridad de los sistemas y datos afectados.

d. El perfil de los Titulares afectados.

e. Número y tipología de los sistemas o bases afectadas.

f. Impacto del incidente en la entidad y en los derechos y libertades de los Titulares afectados.

g. Requerimientos legales y regulatorios.

h. Vector de ataque o método: ruta o medio por el que se ha materializado el incidente. El concepto de “vector de ataque” suele ser uno de los criterios más aceptados a nivel mundial y está directamente relacionado con la identificación del mismo.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

6.4. CAUSALES DE LOS INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

6.4.1. Fraude interno

Delito no violento efectuado con la participación de los funcionarios, contratistas o personas de confianza del Responsable o Encargado del Tratamiento, bien sea en forma directa o indirecta.

Ejemplo: Cualquier apropiación, acceso o uso indebido o no lícito de los datos personales a los cuales el Responsable o Encargado les realice tratamiento, a través de engaños, gestiones no reales, falsificación o adulteración de documentos, administración mal intencionada, cometido por los empleados o personas de confianza dentro de la organización; quienes valiéndose de su posición o de la información privilegiada de la que disponen, realizan un manejo indebido de los datos personales o cualquier tipo de infraestructura que pueda incidir o representar un riesgo en el tratamiento de los mismos.

6.4.2. Fraude externo

Cualquier acto efectuado por una persona ajena al Responsable o Encargado del tratamiento, buscando acceder, apropiarse, causar adulteración o eliminación a los datos personales a los cuales estos les realizan tratamiento.

Ejemplo: Cualquier apropiación, acceso o uso indebido o no lícito de los datos personales a los cuales el Responsable o Encargado les realice tratamiento, a través de los sistemas informáticos, robo, atraco, engaños, falsificación o adulteración de documentos, cometido por personas que no pertenecen a la organización.

6.4.3. Daños a activos físicos

Pérdida, deterioro o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realicen tratamiento, causados por daños a los activos físicos de los mismos.

Ejemplo: Daño físico en los computadores de la empresa, archivos físicos como papel, cintas, discos, etc. Causados por cualquier tipo de incidencia como fenómenos naturales, accidentales o por problemas de orden público.

6.4.4. Falla de tecnología informática

Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realicen tratamiento, causados por fallas en la infraestructura tecnológica de uno u otro.

Ejemplo: Daño en el funcionamiento de los sistemas de información, daño en las redes de datos, problemas con los canales de transmisión de información, VPN, aplicaciones, etc.

6.4.5. Ejecución y/o administración de procesos

Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realice tratamiento, causados por fallas en la ejecución, aplicación y/o administración de procesos, procedimientos, protocolos, políticas de uno u otro.

Ejemplo: Toda vulneración que se detecte por la mala aplicación o ejecución de un procedimiento ya establecido, el cual debe estar documentado y llevar una trazabilidad de su correcta ejecución.

6.4.6. Falla por negligencia o actos involuntarios de los Titulares

Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realicen tratamiento, causados por negligencia o actos involuntarios del mismo titular, que puede ver afectados tanto sus propios datos como los de otros titulares.

Ejemplo: Por lo general, este riesgo se materializa cuando el titular no acata las recomendaciones de seguridad frente al manejo de sus propios datos personales, como el uso de contraseñas de acceso a sistemas de información o cuentas bancarias, cuentas de

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

correo electrónico, números de tarjetas bancarias, utilización de éstos en medios no seguros o excesiva confianza en la entrega de sus datos personales o de otros titulares a personas no autorizadas.

6.5. CONFORMACIÓN DEL EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

El equipo de respuesta es el responsable de definir e implementar las acciones necesarias para prevenir, minimizar, reducir o remediar cualquier impacto o daño de un incidente de seguridad en los Titulares asociado al tratamiento de sus datos personales.

Este equipo estará conformado por:

1. Director General.
2. Oficial de Protección de Datos Personales y
3. Personal de apoyo en Hábeas Data.
4. Director Administrativo y Financiero.
5. Jefe de la Oficina Asesora Jurídica.
6. Jefe de la Oficina de Control Interno
7. Atención al Ciudadano.
8. Telemática.

6.6. ESTRATEGIA PARA RESPONDER A UN INCIDENTE DE SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES

6.6.1. Identificación del Incidente de Seguridad en el Tratamiento de Datos Personales

El análisis de las fuentes de información permitirá determinar si se está ante un incidente de seguridad o no, así como su naturaleza, clase, tipo, si dicho incidente ha afectado a datos de carácter personal y el nivel de riesgo al que se enfrenta la entidad.

Las incidencias relativas a datos de carácter personal no se limitan únicamente al tratamiento automatizado, sino que también incluyen los medios de tratamiento no automatizado. Así pues, las incidencias que afecten a dichos medios, como por ejemplo la pérdida de listados en papel con datos de carácter personal, deberán ser también obligatoriamente reportadas y registradas por el sistema descrito en el presente apartado.

Es necesario tener en cuenta que las incidencias pueden aparecer en cualquier actividad relacionada con el manejo y gestión de bases de datos físicas o automatizadas, así como en el desarrollo de las actividades que afecten a la seguridad de los datos contenidos en las mismas.

A continuación, citamos algunos ejemplos de incidentes de Seguridad en el Tratamiento de Datos Personales:

- Recabar datos de carácter personal sin la autorización del Titular y sin informarle de sus derechos.

- Uso de los datos de carácter personal con una finalidad diferente a la registrada en la autorización.

- Intento o violación de las seguridades y controles de acceso a lugares físicos, a bases de datos automatizadas o a espacios donde se custodia documentos físicos que contienen información personal.

- Alterar la información contenida en las bases de datos con información personal (borrado, modificación o inclusión de datos que atente contra la calidad de los datos).

- Sacar datos en soportes sin la autorización pertinente.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

- Sacar datos en soportes diferentes a los autorizados.
- Incumplir lo establecido por la entidad para la recuperación de datos.
- Incumplir los plazos establecidos para resolver y contestar las solicitudes para ejercer los derechos del Titular.
- Usar ilícitamente datos de carácter personal.
- Gestionar incorrectamente los backups.
- Perdida de activo material (Computadores, tabletas, portátiles, carpetas físicas, archivadores, etc.).
- Imposibilidad de acceder al sistema con nuestro usuario/contraseña habitual cuando se ingresan correctamente los datos de usuario y contraseña.
- Contraseña de acceso posiblemente comprometida.
- Comportamiento anormal del sistema (información incompleta o irreal, fallos inesperados, etc.).

La identificación de un incidente de seguridad puede producirse a través de fuentes internas o fuentes externas a la entidad.

6.6.1.1. Fuentes internas

Se refiere a los controles y mecanismos de seguridad dentro y alrededor de las instalaciones de la entidad, así como los medios de acceso remoto a la información.

Desde el punto de vista de la seguridad física, la detección se produciría ante el incumplimiento o vulneración de las medidas de seguridad adoptadas, como, por ejemplo:

- Política de escritorios limpios, bloqueo de pantallas, accesos con usuario y contraseña, etc.
- Controles físicos como ingreso de visitantes, videos de vigilancia, control y registro de accesos a determinadas zonas, etc.
- Controles y procedimientos frente a daños ambientales o desastres naturales, como terremotos, goteras, incendios, etc.
- En cuanto al entorno de ciberseguridad, la detección se produciría ante la notificación de problemas por parte de los funcionarios y contratistas, como por la generación de alertas de virus.

  Se pueden considerar las siguientes fuentes de información:

  - Notificaciones de usuarios: presencia de archivos con caracteres inusuales, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información.
  - Alertas generadas por software antivirus.
  - Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
  - Anomalías de tráfico de red o picos de tráfico en horas inusuales.
  - Alertas de sistemas de detección/prevención de intrusión (IDS/IPS).

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

- Alertas de sistemas de correlación de eventos.
- Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos.
- Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.
- Análisis de registros en herramientas DLP (Data Loss Prevention).
- También se debe considerar un posible indicio de la ocurrencia de un incidente de seguridad en el futuro, como el análisis del resultado de un escáner de vulnerabilidades del sistema, el anuncio de un nuevo 'exploit' dirigido a atacar una vulnerabilidad que podría estar presente en el sistema o amenazas explícitas anunciando ataques a los sistemas de información de la organización.

6.6.1.2. Fuentes externas

En muchas ocasiones es posible que la detección del incidente se produzca a través de la comunicación de un tercero (proveedores de servicios informáticos, proveedores de servicios de internet o fabricantes de soluciones de seguridad), por un usuario o por la comunicación o notificación que realice alguna autoridad en el tema e, incluso mediante información publicada en medios de comunicación.

6.6.1.3. Comunicación del Incidente de Seguridad en el Tratamiento de Datos Personales

Todo el personal está obligado a comunicar cualquier incidencia de seguridad relativa a los datos de carácter personal al Oficial de Protección de Datos Personales al correo habeas.data@bomberosdebucaramanga.gov.co

6.6.2. Contención del incidente de seguridad en el Tratamiento de Datos Personales y realización de una investigación preliminar

Cuando una alerta permite distinguir un incidente de seguridad en el Tratamiento de Datos Personales, el Oficial de Protección de Datos Personales procede a realizar la fase de contención, con el fin de limitar el alcance o impacto del incidente identificado.

En esta primera etapa, también se debe realizar una investigación inicial sobre el evento u ocurrencia.

Esta investigación preliminar deberá ayudar a responder las siguientes preguntas respecto del incidente de seguridad en el Tratamiento de Datos Personales:

- ¿Cómo se produjo?
- ¿Cuándo y dónde tuvo lugar?
- ¿Cuál fue la naturaleza y quién lo detectó?
- ¿Se continúa compartiendo o divulgando información personal sin autorización?
- ¿Quién tiene acceso a la información personal?
- ¿Qué se puede hacer para asegurar la información o detener el acceso, divulgación o disponibilidad no autorizada y reducir el riesgo de daños a los afectados?
- ¿Es un incidente de seguridad relacionado con Datos Personales que requiere la notificación a las personas tan pronto como sea posible?

Adicionalmente, se debe recabar, y tener cuidado de no destruir, la evidencia que pueda ser valiosa para:

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

- Establecer la causa del incidente de seguridad relacionado con el Tratamiento de Datos Personales.

- Identificar todos los riesgos generados a los Titulares de los datos.

- Responder los requerimientos de la SIC u otras autoridades.

Durante la contención se deben realizar las siguientes actividades:

1. Aislar los activos afectados. Por ejemplo, si se trata de medios de almacenamiento físico, se aísla el entorno donde ocurrió el incidente como el archivador. O bien, si se trata de un medio de almacenamiento electrónico, se separan los equipos de cómputo afectados de la red, para evitar, por ejemplo, la propagación de una infección de software malicioso.

2. Aislamiento de sistemas y, de ser necesario, la puesta en operación de respaldos.

3. Diligenciar el Formato de Contención de Incidentes de seguridad en el tratamiento de datos personales (Anexo No. 2).

4. Identificación de las vulnerabilidades explotadas en los activos, así como las medidas de seguridad que pudieron hacer falta, para su posterior implementación.

Es importante tener en cuenta lo siguiente:

- Las medidas de contención podrán ser inmediatas o de aplicación progresiva en función del desarrollo de la resolución del incidente.

- Es conveniente determinar las medidas a implantar estableciendo un orden de prioridad, los responsables asignados, tiempos estimados y los efectos esperados.

- Algunas medidas de contención serán sencillas y las podrá iniciar el usuario, sin embargo, otras medidas son más complejas y deben estar en manos de personal especializado en el tema.

A continuación, se enumeran someramente algunas de las medidas de contención que podrían ser de aplicación en función de cada caso:

- Si es posible, impedir el acceso al origen de la divulgación: dominios, puertos, servidores, la fuente o los destinatarios de la divulgación.

- Dependiendo del vector de ataque, impedir el acceso al origen: dominios, conexiones, equipos informáticos o conexiones remotas, puertos, parches, actualización del software de detección (antivirus, IDS, etc.) bloqueo de tráfico, deshabilitar dispositivos, servidores, etc.

- Suspender las credenciales lógicas y físicas con acceso a información privilegiada.

- Cambiar todas las contraseñas de usuarios privilegiados o hacer que los usuarios lo hagan de manera segura.

- Hacer una copia de la base (clonada), hacer una copia bit a bit del disco duro que contiene la base, y luego analizar la copia utilizando herramientas forenses.

- Aislar la herramienta utilizada para vulnerar la seguridad de los datos personales con el fin de realizar un análisis forense más tarde.

- Si los datos han sido enviados a servidores públicos, solicitar al propietario (o webmaster) que elimine los datos divulgados.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

- Si no es posible eliminar los datos divulgados, proporcionar un análisis completo al Equipo de Respuesta y a la Dirección General.

- Vigilar la difusión de los datos personales filtrados en los diferentes sitios web y redes sociales.

6.6.3. Registro del Incidente de Seguridad en el Tratamiento de Datos Personales

Una vez se ha contenido el incidente de seguridad relacionado con el Tratamiento de Datos Personales, se realizarán las siguientes acciones:

1. El Oficial de Protección de Datos Personales registrará formalmente dicho incidente en el formato de Registro de Incidentes de seguridad en el tratamiento de datos personales (Anexo No. 3).

   En este sentido, se detallará al menos la siguiente información:

   - Tipo de incidente de acuerdo con la tipología descrita en el subtítulo 6.2. del presente documento.

   - La fecha y hora del incidente de seguridad y del descubrimiento del mismo.

   - Causa del incidente.

   - Fecha de la notificación.

   - Persona que reporta el incidente.

   - Una descripción general de las circunstancias del incidente de seguridad (incluidas las Bases de Datos y las clases de datos -sensibles, privados, etc.- comprometidos).

   - Cantidad y las categorías de Titulares afectados.

   - Las indagaciones preliminares e investigaciones realizadas por la organización.

   - Los responsables del manejo del incidente de seguridad.

   - La evaluación del nivel de riesgo derivado del incidente de seguridad en los Titulares y los factores tenidos en cuenta.

2. En el caso de que sea necesario, el Oficial de Protección de Datos Personales coordinará con el Encargado del Tratamiento para el análisis del incidente de seguridad.

3. Adicionalmente, el Oficial de Protección de Datos Personales podrá solicitar soporte técnico de responsables de departamentos durante la fase de análisis del incidente.

6.6.4. Evaluación de los riesgos e impactos asociados con el incidente de seguridad en el Tratamiento de los datos personales

La adecuada gestión del incidente de seguridad en el Tratamiento de los datos personales incluye la evaluación de su nivel de severidad teniendo en cuenta:

- la probabilidad de daño para los Titulares de los datos personales,

- el impacto o afectación para sus derechos y libertades,

- y el tratamiento o gestión que se dará a esos riesgos.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

6.6.4.1. Nivel de riesgo del incidente de seguridad frente a los Titulares de la información.

El riesgo del incidente de seguridad frente a los Titulares de los datos personales puede ser calificado en:

- **Riesgo bajo:** es improbable que el incidente de seguridad tenga un impacto en las personas, y de generarlo, este sería mínimo.
- **Riesgo medio:** el incidente de seguridad puede tener un impacto en las personas, pero es poco probable que el impacto sea sustancial.
- **Riesgo alto:** el incidente de seguridad puede tener un impacto considerable en las personas afectadas.
- **Riesgo grave:** el incidente de seguridad puede tener un impacto crítico, extenso o peligroso en las personas afectadas.

6.6.4.2. Factores que pueden ser tenidos en cuenta para determinar el nivel de riesgo del incidente

6.6.4.2.1. En los Titulares de la información

- ¿Qué cantidad de personas fueron afectadas?
- ¿Qué categoría de personas fueron afectadas?
- ¿Cuáles son las características especiales de las personas afectadas? Por ejemplo: niños, niñas y/o adolescentes; personas en estado de vulnerabilidad; personal del sindicato, etc.

6.6.4.2.2. En los datos personales

- ¿Cuál fue el volumen de los datos afectados?
- ¿Cuál fue el periodo durante el cual los datos fueron afectados o estuvieron comprometidos?
- ¿Qué tipo de información personal fue afectada? Por ejemplo, identificación personal, datos biométricos, datos relacionados con el estado de la salud física o mental, resultados de pruebas académicas, registros de localización, direcciones IP, mensajes de texto, información financiera y crediticia, perfiles de comportamiento, puntajes de crédito, etc.
- ¿Qué tan sensible es la información comprometida? Por ejemplo: datos de niños, niñas y/o adolescentes; datos biométricos o de la salud física o mental; perfiles de comportamiento, orientación sexual, datos políticos, afiliación al sindicato, etc.
- ¿Cuál es el contexto de la información personal comprometida?
- ¿Estaba la información personal adecuadamente custodiada, contaba con elementos para su seguridad como cifrado, anonimización, pseudonimización, restricción de accesos, etc.? ¿Era inaccesible?
- ¿Cómo se puede utilizar la información personal afectada?
- ¿Existe un riesgo a una mayor exposición de la información personal?
- ¿Está la información personal disponible públicamente en internet?
- ¿Se puede utilizar la información personal para fines fraudulentos o puede causar

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

cualquier tipo de daño material y/o inmaterial al Titular?

- ¿Se ha recuperado la información personal?

6.6.4.2.3. En la entidad

- ¿Qué causó el incidente de seguridad?
- ¿Cuándo ocurrió el incidente de seguridad y si éste había ocurrido anteriormente?
- ¿Es este un problema sistemático o es aislado?
- ¿Cuál fue el alcance del incidente de seguridad?
- ¿Qué medidas se han tomado para mitigar el daño?
- Las actividades y operaciones que desarrolla la entidad.
- ¿Los datos comprometidos afectarán las transacciones que debe realizar la entidad con terceros?

6.6.4.2.4. Identificar los daños para las personas, organizaciones y público en general

1. ¿Qué daños para las personas podrían resultar de un incidente de seguridad? Entre otros, pueden ser:
    - Riesgo en su seguridad física o psicológica
    - Extorsión económica o sexual
    - Hurto de identidad
    - Suplantación de identidad
    - Pérdida financiera
    - Negación de un crédito o seguro
    - Perfilamiento con fines ilícitos
    - Pérdida de negocios u oportunidades de empleo
    - Discriminación
    - Humillación significativa o pérdida de dignidad y daño a la reputación.
2. ¿Qué daño para la organización podría resultar de un incidente? Los ejemplos incluyen:
    - Pérdida reputacional
    - Pérdida de clientes o usuarios
    - Pérdida de confianza en la organización
    - Honorarios de consultores e ingenieros forenses
    - Pérdida de activos
    - Sanciones, órdenes e instrucciones administrativas

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

- Exposición financiera
- Órdenes judiciales
- Demandas judiciales

3. ¿Qué daño para el público podría resultar de un incidente de seguridad? Los ejemplos incluyen:

   - Riesgo para la salud pública.
   - Riesgo para la seguridad pública.
   - Pánico económico.
   - Alteración de los pilares constitucionales de un país.

6.6.5. Mitigación (Erradicación)

En esta etapa se realiza el tratamiento profundo del incidente de seguridad para minimizar la posibilidad de que éste se vuelva a repetir.

La etapa de mitigación considera la creación de un plan de implementación de medidas de Seguridad, teniendo en cuenta que:

1. Para reforzar la seguridad de los medios de almacenamiento físico, se deben mejorar las políticas y los controles de acceso físico, por ejemplo, mejores cerraduras.

2. Para los medios de almacenamiento electrónico, la mitigación incluye actualizaciones de hardware y software, así como revisiones con herramientas automatizadas sobre los respaldos que se pusieron en operación.

3. Cuando se cuenta con equipos de respuesta a incidentes avanzados, propios o subcontratados, se inicia el proceso de recolección de evidencia para el análisis forense digital. Es decir, de los activos en medios de almacenamiento electrónicos que se aislaron en la etapa de contención, se realizan imágenes forenses o copias exactas bit a bit, que se analizan en laboratorios (privados o de una autoridad competente), con herramientas especiales de hardware y software, a fin de obtener más información del incidente.

6.6.6. Notificación a la Superintendencia de Industria y Comercio

La entidad deberá reportar la ocurrencia del incidente de seguridad en el tratamiento de los datos personales ante la Superintendencia de Industria y Comercio a más tardar dentro los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

La notificación de un incidente de seguridad en Datos Personales debe contener, como mínimo, la información que establece el aplicativo del Registro Nacional de Bases de Datos (RNBD), los detalles se recogen en el “Manual de Usuario del Registro Nacional de Bases de Datos – RNBD”.

6.6.7. Comunicación a los Titulares de los datos personales

La comunicación a los Titulares de la Información brinda la oportunidad para que ellos mismos puedan adoptar las medidas necesarias para protegerse de las consecuencias de un incidente de seguridad. Por ejemplo, cambiar su nombre de usuario y contraseña; monitorear su historial crediticio; cancelar su tarjeta de crédito; etc.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

6.6.7.1.1. ¿Cuándo comunicar?

Se comunicará a los Titulares cuando el incidente de seguridad presente un Nivel de Riesgo Medio, Alto o Grave de acuerdo con lo establecido en el presente documento.

Esta comunicación debe permitir a los Titulares afectados la toma de medidas para protegerse de las consecuencias del incidente.

6.6.7.1.2. ¿Cómo comunicar?

La notificación se realizará mediante correo electrónico, SMS, correo físico o por teléfono e incluirá la siguiente información:

- Datos de contacto del Oficial de Protección de Datos Personales o, en su caso, del medio de contacto en el que pueda obtenerse más información.
- Descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias del incidente en la seguridad de los datos personales.
- Descripción de los datos e información personal afectados.
- Resumen de las medidas implementadas hasta el momento para controlar los posibles daños.
- Cualquier otra información que le sea a los Titulares para proteger sus datos o prevenir posibles daños.

Se debe tener en cuenta:

- Las comunicaciones deben ser lo suficientemente claras y precisas para permitir que los Titulares de la información comprendan la importancia del incidente y que tomen las medidas, si es posible, para reducir los riesgos que podría resultar de su ocurrencia.
- Es primordial no incluir información personal innecesaria en el aviso para evitar una posible divulgación no autorizada.

6.6.7.1.3. ¿Quién debe comunicar?

El Director General notificará a los Titulares el incidente, debiendo comunicarlo a los mismos en un tiempo prudencial.

No obstante, será el Oficial de Protección de Datos Personales quien apoye con la proyección del texto de dicha notificación.

6.6.8. Excepción a la notificación / comunicación

No será necesaria la notificación cuando la entidad pueda demostrar, de forma fehaciente, que el incidente de seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de los Titulares, es decir, presentaba un Nivel de Riesgo Bajo.

Asimismo, no será necesaria la comunicación a los afectados cuando:

1. La entidad ha tomado medidas técnicas y administrativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad al incidente de seguridad de datos personales (mediante el uso de: cifrados de datos de última generación, minimización, disociación de datos, acceso a entornos de prueba sin datos reales, etc.).

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

2. Por ejemplo, es probable que no sea necesaria la notificación si se pierde un dispositivo móvil y los datos personales que contiene están cifrados. Sin embargo, sí es posible que se requiera de notificación si esta fuera la única copia de los datos personales, o por ejemplo, la clave de cifrado en posesión del responsable estuviera comprometida.

3. La entidad ha tomado con posterioridad al incidente de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de las medidas contra la persona que ha accedido a los datos personales antes de que pudieran hacer algo con ellos.

4. Cuando la notificación a los Titulares suponga un esfuerzo desproporcionado a nivel técnico y administrativo. Por ejemplo, cuando los detalles de contacto se hayan perdido como resultado del incidente o aquellos casos en los que se tenga que desarrollar un nuevo sistema o proceso para realizar la notificación, o se requiera la dedicación excesiva de recursos internos para la identificación de los Titulares. Ante esta situación, se realizará la notificación de manera pública a través de los canales establecidos por el responsable.

6.6.9. Prevención futuros incidentes de seguridad en Datos Personales

En caso de que se haya presentado un incidente de seguridad en el Tratamiento de los datos personales, la entidad deberá tener en cuenta la realización de las siguientes actividades:

- Revisar las condiciones del Tratamiento de los datos personales.
- Realizar auditorías al Sistema de Protección de Datos Personales.
- Robustecer las políticas de seguridad en la información física y automatizada, los procesos y los procedimientos en donde se realiza tratamiento de los datos personales.
- Ajustar las evaluaciones de impacto en el Sistema de Administración de los riesgos asociados al Tratamiento de los datos personales.
- Establecer esquemas de trabajo a corto, mediano y largo plazo. Así como los roles y responsabilidades.
- Generar apoyo y compromiso de la Dirección General para desplegar los cambios que se requieran al interior de la entidad.
- Una vez se haya gestionado el incidente de seguridad, el equipo de respuesta deberá revisar el protocolo, y hacer los ajustes pertinentes.

Igualmente, la entidad podrá implementar cualquiera de las siguientes medidas con posterioridad a la ocurrencia de un incidente:

- Reforzar los programas de capacitación y educación del personal.
- Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención de la brecha de seguridad.
- Identificar y eliminar malware o desactivar cuentas de usuarios vulnerables.
- Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.
- Actualizar el antivirus de la entidad.
- Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

- Garantizar que la estrategia adoptada encuentre un balance entre la continuidad del negocio y el riesgo intrínseco en los activos que se hayan visto afectados por el incidente de seguridad.

- Elaborar un informe final tendiente a recopilar la información, plazos de actuación y medidas adoptadas, de cara a una revisión por terceras personas.

6.6.10. Elaboración del informe de resolución del incidente

La elaboración del informe de resolución tiene como objetivo servir de base para realizar ejercicios futuros de lecciones aprendidas. Con un carácter meramente interno, y elaborado por el Oficial de Protección de Datos Personales, este informe debe facilitar a todas las personas involucradas en la respuesta al incidente, el entendimiento sobre el porqué de las acciones tomadas, así como las acciones marcadas para seguimiento en el corto, medio y largo plazo. También serán tenidos en cuenta los cambios necesarios que deberían ser incluidos en el análisis de riesgos de la organización.

Este informe deberá incluir, al menos, información relativa a los siguientes apartados:

- Alcance e impacto del incidente.

- Controles preventivos existentes.

- Acciones de respuesta tomadas sobre las diferentes alternativas consideradas para la resolución de la brecha.

- Acciones tomadas para la prevención de futuros incidentes.

- Impacto de las acciones de respuesta tomadas en la resolución del incidente.

- Acciones definidas para el seguimiento.

Una vez cerrado el incidente, el Oficial de Protección de Datos Personales debe regresar a la etapa de preparación, a fin de continuar con la implementación de medidas de seguridad que permitan mejorar la atención y detección de alertas, así como la respuesta cuando se presenten nuevos incidentes de seguridad.

6.7. RESPONSABILIDADES EN LA RESPUESTA ANTE INCIDENTES EN EL TRATAMIENTO DE DATOS PERSONALES

En la siguiente matriz se asignan las responsabilidades dentro del proceso de respuesta ante de incidentes de seguridad en el tratamiento de datos personales.

En esta matriz se asigna en cada una de las tareas, una o más responsabilidades representadas por una letra:

- R: Este rol corresponde a quien realiza la tarea.

- A: Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución.

- C (Consultado): Este rol posee alguna información o capacidad necesaria para realizar la tarea.

- I (Informado): Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea.

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

TAREA O RECURSO	EQUIPO DE RESPUESTA	DIRECCIÓN GENERAL	OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	DEPENDENCIA O ÁREA	FUNCIONARIO O CONTRATISTA
Comunicar el incidente	I	I	I	I	R / A
Registrar el incidente	I	I	R / A	I	
Evaluar el incidente	I / C	I / C	R / A	I / C	
Notificar a la SIC	I	I	R / A	I	
Notificar a los Afectados	I	A	R	I	
Seguimiento y cierre	I	I	R / A	I	
Mejora	I / C	I / C	R / A	I	

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

7. ANEXOS

7.1. Anexo No. 1: Diagrama de Flujo del Manejo de Incidentes de seguridad en el Tratamiento de Datos Personales

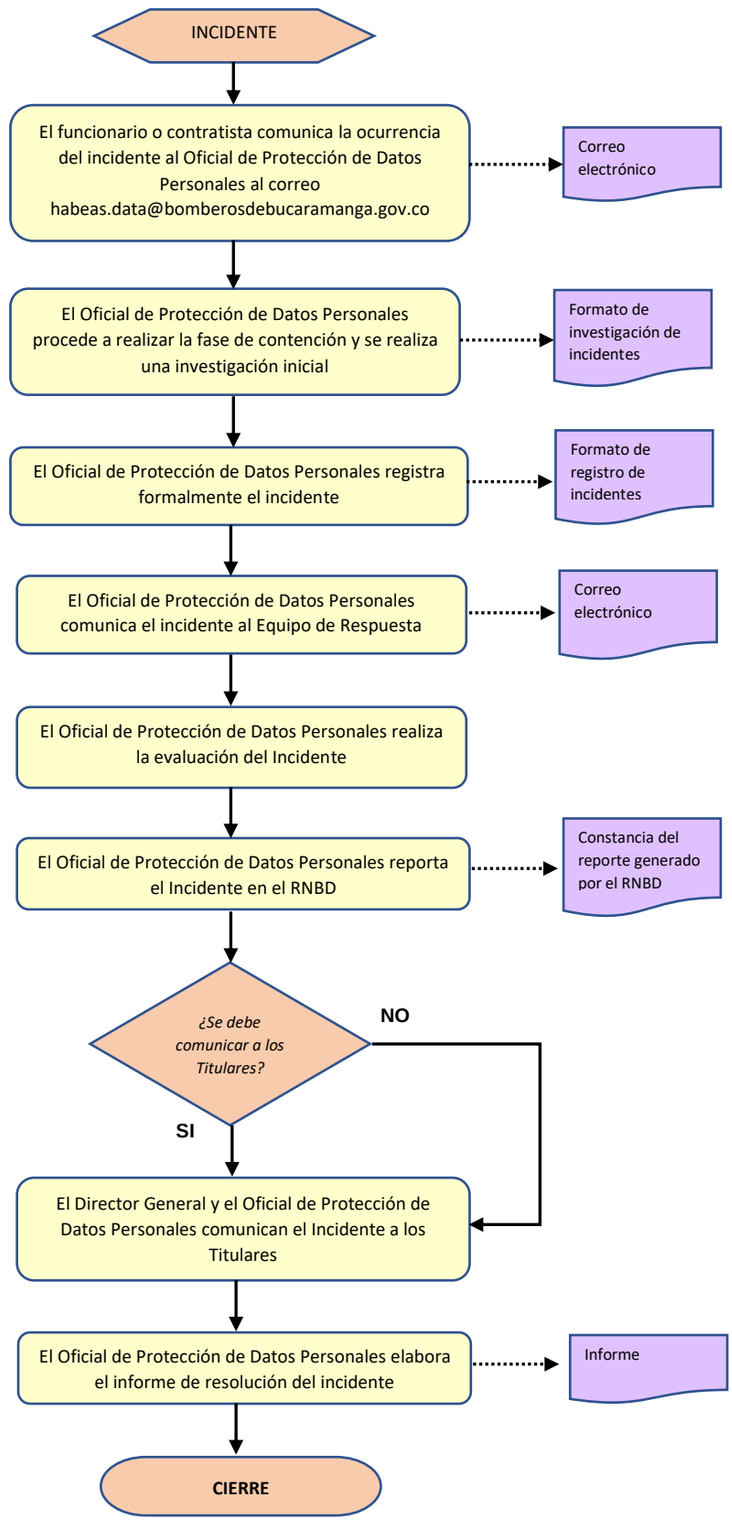

Figura No. 1. Procedimiento para la Gestión de Incidentes

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

7.2. Anexo No. 2: Formato de Contención de Incidentes de Seguridad en el Tratamiento de los Datos Personales

Ciudad y fecha de diligenciamiento del formato:

INFORMACIÓN DEL INCIDENTE DE SEGURIDAD

¿Cuál fue el incidente?	
Lugar donde ocurrió el incidente:	Fecha y hora (aprox.) de detección del incidente:
Causa del Incidente:	Fecha y hora (aprox.) de ocurrencia del incidente:
Persona que detectó el incidente:	Perfil de la persona que detectó el incidente:

Contexto:

◯ Interno no intencionado ◯ Externo no intencionado ◯ Otro:

◯ Interno intencionado ◯ Externo intencionado

Tipo de Incidente

◯ Afecta la Confidencialidad ◯ Afecta la Integridad ◯ Afecta la Disponibilidad

◯ Afecta la Confidencialidad e Integridad ◯ Afecta la Confidencialidad y Disponibilidad

◯ Afecta la Disponibilidad e Integridad ◯ Afecta la Confidencialidad, Disponibilidad e Integridad

CONTENCIÓN DEL INCIDENTE DE SEGURIDAD

¿Cómo se produjo el incidente?
¿Quién tiene acceso a la información personal involucrada en el incidente?
Acciones para asegurar la información o detener el acceso, divulgación o disponibilidad no autorizada y reducir el riesgo de daños a los afectados
Evidencias

Diligenció:	Cargo:

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220

7.3. Anexo No. 3: Formato de Registro de Incidentes de Seguridad en el Tratamiento de los Datos Personales

Ciudad y fecha de diligenciamiento del formato:

INFORMACIÓN DEL INCIDENTE DE SEGURIDAD

¿Cuál fue el incidente?	
Lugar donde ocurrió el incidente:	Fecha y hora (aprox.) de detección del incidente:
Causa del Incidente:	Fecha y hora (aprox.) de ocurrencia del incidente:
Persona que detectó el incidente:	Perfil de la persona que detectó el incidente:

Contexto:

◯ Interno no intencionado ◯ Externo no intencionado ◯ Otro:

◯ Interno intencionado ◯ Externo intencionado

Tipo de Incidente

◯ Afecta la Confidencialidad ◯ Afecta la Integridad ◯ Afecta la Disponibilidad

◯ Afecta la Confidencialidad e Integridad ◯ Afecta la Confidencialidad y Disponibilidad

◯ Afecta la Disponibilidad e Integridad ◯ Afecta la Confidencialidad, Disponibilidad e Integridad

Descripción general de las circunstancias del incidente de seguridad (incluidas las Bases de Datos y las clases de datos comprometidos:	
Cantidad de Titulares afectados:	Categorías de los Titulares afectados:
Resultado de la investigación preliminar:	
Responsables del manejo del incidente de seguridad:	

La evaluación del nivel de riesgo derivado del incidente de seguridad en los Titulares:

◯ Riesgo Bajo ◯ Riesgo Medio

◯ Riesgo Alto ◯ Riesgo Grave

Factores tenidos en cuenta para determinar el nivel de riesgo:

Diligenció:	Cargo:

EXCELENCIA Y COMPROMISO

8. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Creación del documento	13/04/2021

Sede Administrativa: Calle 44 Número 10 - 13
Bucaramanga, Santander
PBX- 6526666 Línea Emergencias 119 — 123
Telefax- Dirección General: 6522220