Cámara de Comercio de Facatativá y del Noroccidente de Cundinamarca

PBX (601) 8902833
WhatsApp: 3106691309
correspondencia@ccfacatativa.org.co

DECISION EJECUTIVA No. 110
(17 de junio de 2025)

"POR MEDIO DE CUAL SE MODIFICA DECISIÓN EJECUTIVA N° 104 DE NOVIEMBRE 27 DE 2023 "SE ADOPTA EL DOCUMENTO TÉCNICO DEL PLAN DE CONTINUIDAD DE NEGOCIO DE LA CÁMARA DE COMERCIO DE FACATATIVÁ"

De conformidad con la Norma Internacional ISO 22301, referente al Sistema de Gestión de la Continuidad del Negocio (SGCN), publicada por la Organización Internacional de Normalización (ISO), esta norma tiene como propósito proporcionar un marco estructurado que permita a las organizaciones prevenir, prepararse, responder y recuperarse frente a incidentes inesperados. La ISO 22301 está orientada a facilitar la implementación y gestión eficaz de un sistema de continuidad del negocio, garantizando la resiliencia operativa ante situaciones de crisis o interrupciones.

La ISO 22301 tiene como objetivo proteger a la Entidad de una amplia gama de posibles amenazas e interrupciones brindándonos buenas prácticas y formas para llevar a cabo la gestión de continuidad del negocio con el fin de minimizar los impactos que puedan traer la materialización de un riesgo afectando de manera directa la entidad.

Que el día veintisiete (27) de noviembre de dos mil veintitrés (2023), la Cámara de Comercio de Facatativá profirió la Decisión Ejecutiva No. 104 del 27 de noviembre de 2023, mediante la cual "se adopta el documento técnico del Plan de Continuidad de Negocio", instrumento logístico y estratégico que tiene por objeto garantizar la recuperación y restablecimiento eficaz, oportuno y ordenado de la prestación de los servicios institucionales, ante cualquier eventualidad que pudiere afectar la operación misional y administrativa de la Entidad, sugerencia presentada en el año 2020 por auditoría externa realizada por INCOTEC

Que, conforme a lo dispuesto en la Decisión Ejecutiva N° 034 del veintiocho (28) de febrero de dos mil veinticinco (2025), se modifica el Artículo 15 de la Resolución N° 115 de 2017, adoptando modificaciones en la denominación de los empleos que integran la Planta de Personal de la Cámara de Comercio de Facatativá, así mismo, se modifica el Artículo Cuarto de la Decisión Ejecutiva N° 090 del nueve (9) de octubre de dos mil veinte (2020) por la cual se modificó el artículo 19 la Resolución N°. 115 de 2017, mediante el cual se introducen cambios al Manual de Funciones, Requisitos y Competencias aplicable a los empleos previstos en la Planta de Personal de la Cámara de Comercio de Facatativá.

Que en mérito de lo anteriormente expuesto:

RESUELVE

PRIMERO: modificar la DECISIÓN EJECUTIVA N° 104 DE NOVIEMBRE 27 DE 2023 por medio de la cual "SE ADOPTA EL DOCUMENTO TÉCNICO DEL PLAN DE CONTINUIDAD DE NEGOCIO DE LA CÁMARA DE COMERCIO DE FACATATIVÁ", el cual quedara así:

ARTÍCULO PRIMERO: OBJETO. La Cámara de Comercio de Facatativá ha definido un plan de continuidad del negocio con el fin de reducir la vulnerabilidad frente amenazas externas e internas, facilitar una respuesta planificada y ordenada frente a incidentes que puedan interrumpir la operación, asegurar la disponibilidad de los procesos críticos, en términos de tiempos y costos e identificar los puntos débiles de la Entidad, requiriendo establecer unos roles y responsabilidades de administrar, promover, apoyar y hacer seguimiento del Plan de Continuidad del Negocio.

ARTICULO SEGUNDO: ALCANCE. El Plan de continuidad del negocio contempla los siguientes roles y responsabilidades, encaminados a administrar, promover, apoyar y hacer el respectivo seguimiento, acorde con las partes interesadas, directrices y requerimientos, así:

I. La Brigada de Emergencia.
II. Director(a) Administrativo(a) y Financiero(a).
III. Director(a) de Registros Públicos.
IV. Director(a) de Asuntos Jurídicos.
V. Director(a) de Desarrollo Empresarial
VI. Director(a) de Desarrollo Institucional.
VII. Director(a) de Control Interno.
VIII. Coordinador de transformación digital y formación empresarial
IX. Coordinador de Planeación
X. Coordinador Financiero
XI. Profesional II de Talento Humano.
XII. Profesional II de Calidad
XIII. Profesional I de SG-SST.
XIV. Líder de Comunicaciones y Posicionamiento empresarial

ARTÍCULO TERCERO: DEFINICIONES. Para efectos de la aplicación del presente plan de continuidad del negocio se tendrá en cuenta los siguientes conceptos:

Plan de continuidad del negocio: procedimientos documentados que guían a una organización para responder, recuperar, reanudar y restablecer un nivel de funcionamiento predefinido tras una interrupción.

Análisis del impacto en el negocio: proceso de análisis de las actividades y del efecto que puede tener en ellas una interrupción del negocio.

Equipo de brigadas de emergencia: grupo de funcionalidad individual responsable de dirigir el desarrollo y la ejecución del plan de respuesta y continuidad operativa, de declarar una interrupción operativa o una situación de crisis de emergencia, y de proporcionar dirección durante el proceso de recuperación, tanto antes como después del incidente perturbador.

Par del cargo: persona para desempeñar las funciones de otro cargo, temporalmente o en ausencia del titular original por vacaciones, incapacidades, licencias o cuando se requiera asegurando la continuidad de las funciones y procesos de la entidad.

ARTÍCULO CUARTO: EJECUCIÓN. Establecer el plan de continuidad del negocio de la Cámara de Comercio de Facatativá, la cual quedara así:

1. PRESENTACIÓN

Con el desarrollo del presente documentos se da inicio al plan de continuidad de negocio, a través del cual se sugiere la estrategia(s) de recuperación que pueda permitir la continuidad de las funciones de la **CÁMARA DE COMERIO DE FACATATIVÁ,** la entidad es consciente de la importancia que tiene la infraestructura la tecnología de la información como soporte a los procesos estratégicos, operativos y de apoyo de la entidad. Por lo cual se revisa la protección que tiene los COLABORADORES activos, dentro de un nivel de riesgo aceptable, por lo tanto la estrategia de recuperación de la infraestructura, tecnología, o ausencia de un colaborador de la **CÁMARA DE COMERCIO DE FACATATIVÁ** debe estar alineada con la misión, visión y en general a la política de calidad de la entidad; de igual forma que permita su capacidad de adaptación ante eventos no deseados que amenacen la supervivencia o la continuidad de sus operaciones durante la ocurrencia de un desastre, garantizando principalmente, la preservación de tres características:

Integridad: que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento.

Confidencialidad: que la información sea accesible solo a las personas autorizadas.
Disponibilidad: que los usuarios autorizados tengan acceso a la información y los recursos cuando lo necesiten.

Con el fin de contar con un mecanismo que permita prevenir o reaccionar ante posibles incidentes que pongan en riesgo los activos de la Entidad, la prestación y continuidad del servicio, la, Dirección Administrativo y Financiero, Dirección de Asuntos Jurídicos, Dirección de Desarrollo Empresarial, Dirección de Desarrollo institucional, Dirección de Control Interno, Dirección de Registros Públicos y el área de Talento Humano en trabajo con el área de Planeación institucional revisan las acciones a desarrollar en el Plan de continuidad del negocio que, permitirían responder de manera eficaz ante una eventualidad y restablecer en menor tiempo posible la disposición de los servicios que se prestan y mitigar el impacto negativo que pueda ocasionar.

Así pues, este plan de continuidad del negocio tiene en cuenta lo dispuesto en el MAN-TI-01-MANUAL DE SEGURIDAD DE LA INFORMACIÓN, el cual se encuentra publicado en el portal web de la Cámara de Comercio de Facatativá, articulado al plan estratégico de la entidad.

El plan de continuidad adquiere mayor relevancia una vez sea apropiado por todos los colaboradores, usuarios y contratistas de manera anticipada y será actualizado y comunicado según las necesidades de la entidad.

2. MARCO LEGAL

El desarrollo del plan de continuidad de negocio se fundamenta en la necesidad de preservar la disponibilidad y continuidad de los servicios que presta la Entidad Cámara de Comercio de Facatativá, bajo los lineamientos generales en el uso de servicios digitales para los usuarios y afiliados. Finalmente, la integración de las estrategias se realiza para la preservación de la seguridad y la vida de los grupos de valor de la Entidad, incorporar los lineamientos de gestión y tratamiento de riesgos y desastres de la Ley 1523 de 2012, política nacional de gestión del riesgo de desastres y las obligaciones en materia de Sistema de seguridad y Salud en el Trabajo (SG-SST) de decreto 1072 de 2015.

Ley 1523 de 2012, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres.

Artículo 2°. De la responsabilidad. La gestión del riesgo es responsabilidad de todas las autoridades y de los habitantes del territorio colombiano. En cumplimiento de esta responsabilidad, las entidades públicas, privadas y comunitarias desarrollarán y ejecutarán los procesos de gestión del riesgo, entiéndase: conocimiento del riesgo, reducción del riesgo y manejo de desastres, en el marco de sus competencias, su ámbito de actuación y su jurisdicción, como componentes del Sistema Nacional de Gestión del Riesgo de Desastres.

Ley 2294 de 2023, por el cual se expide el Plan Nacional de Desarrollo 2022 - 2026. "COLOMBIA POTENCIA MUNDIAL DE LA VIDA"

Artículo 143. TRANSFORMACIÓN DIGITAL COMO MOTOR DE OPORTUNIDADES E IGUALDAD. El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará e implementará una estrategia integral para democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología en el país, mediante las siguientes medidas:

7. Promover un entorno digital seguro para generar confianza en el uso y apropiación de las TIC.

Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

"TÍTULO 17 lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

ARTICULO 2.2.17.1.6. Principios. Además de los principios previstos en el artículo 209 de la Constitución Política, en el artículo 2 de la Ley 1341 de 2009, en el artículo 3 de la Ley 1437 de 2011, en el artículo 4 de la Ley 1581de 2012 y los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015 la prestación de los servicios ciudadanos digitales se orientará por los siguientes principios:

6. Seguridad, privacidad y circulación restringida de la información: Toda la información de los usuarios que se genere, almacene, transmita o trate en el marco de los servicios ciudadanos digitales deberá ser protegida y

custodiada bajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, disponibilidad, confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital.

ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, en la cual deberán hacer periódicamente una evaluación del riesgo de seguridad digital que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Decreto 1072 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo

Artículo 2.2.4.6.4. Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST). El Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua y que incluye la política, la organización, la planificación, la aplicación, la evaluación, la auditoría y las acciones de mejora con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y la salud en el trabajo.

- NTC 5722: Gestión de Continuidad del negocio: Esta norma especifica los requisitos para planificar, establecer, implementar, operar, supervisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de los incidentes perjudiciales que puedan surgir.
- ISO 31000:2018: norma internacional para la Gestión de Riesgos. Proporciona principios y guías para que las organizaciones lleven a cabo su análisis y evaluación de riesgos.

- ISO 17799:2000: estándar para la administración de la seguridad de la información, publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. A partir del 2007, se propone incorporar una edición nueva del ISO/IEC 17799 en este nuevo esquema de numeración con el nombre ISO/IEC 27002.

- COBIT: Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC.

- ITIL: "Information Technology Infraestructura Library", es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Jovenmente Commerce, una entidad independiente de la tesorería del gobierno británico.

- ISO Serie 27000: es una serie de estándares, que incluye, definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información), (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoría y certificación de SGSI (ISO 27006), una guía de auditoría de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario.

3. OBJETIVOS

Objetivo General

Definir las actividades preventivas y correctivas para reaccionar de manera eficiente ante una eventualidad que comprometa el desarrollo de las actividades cotidianas, la seguridad del personal o la prestación del servicio.

Objetivos específicos

- Determinar la vulnerabilidad en el centro de datos e instalaciones y definir las medidas preventivas que se pueden tomar para reducir al mínimo la probabilidad y el impacto en la perdida de información de la Cámara de Comercio de Facatativá.
- Definir los servicios de la plataforma tecnológica, definir en que condición nos encontramos y los tiempos máximos de recuperación ante fallas o eventos catastróficos.
- Definir niveles de alerta que permitan identificar posibles amenazas a la seguridad de la infraestructura y la tecnológica.
- Disminuir los tiempos de interrupción de la operación de los procesos.
- Definir las acciones para minimizar el tiempo de inactividad y la pérdida de activos de la entidad.
- Dar continuidad a los procesos con los "Pares" en los cargos.

4. ALCANCE

El plan de continuidad del negocio inicia con la identificación y socialización de los elementos críticos de la **CÁMARA DE COMERCIO DE FACATATIVÁ** que puedan definirse como incidente, desastre y continuidad de los procesos administrativos que impidan continuar la operación y finaliza con el análisis y acciones de mejora identificadas de la reacción ante la situación presentada mínimo una vez al año (simulacro o realidad).

El plan de continuidad del negocio de la Cámara de Comercio de Facatativá identificará a profundidad todos los elementos necesarios para que la prestación del servicio sea de manera satisfactoria y para ello se mitigará toda actividad o acción

que no permita cumplir con la razón de ser de la entidad. Finalmente, se realizará un proceso de background check de las situaciones presentadas por los diferentes actores que llevaran a plantear acciones de mejora y se protegerá sus tres pilares fundamentales como son los misionales frente a la entidad donde encontramos, **Registros Públicos, Mecanismos Alternativos de Solución de Conflictos (MASC) y Desarrollo Empresarial.** Con el fin de contar con una herramienta que nos permita prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo a los colaborares que presta sus servicios en la Entidad, afectar el debido desarrollo de las actividades propias de Función Privada, impedir la prestación y continuidad del servicio a los visitantes, la Entidad ha consolidado el conjunto de acciones que se emprenden para dar respuesta a los eventos en el Plan de continuidad del negocio. Estas acciones diseñadas y ejecutadas de forma planificada, permitirían responder de manera eficiente ante una emergencia, restablecer en el menor tiempo la prestación de los servicios y mitigar el impacto negativo de la perdida de recursos.

5. ROLES Y RESPONSABILIDADES

Con el fin de apoyar la implementación del modelo de continuidad de negocio y gestionar sus resultados, los direcciones deben de dar respuesta a las emergencias que pongan en riesgo la continuidad de sus servicios institucionales, utilizando el plan de continuidad de negocio como una herramienta de preparación para la respuesta que con base en unos escenarios posibles y priorizados (identificados en el proceso de conocimiento del riesgo), se define los mecanismos de organización, coordinación, funciones, competencias, responsabilidades, así como recursos disponibles y necesarios para garantizar la atención efectiva de las emergencias que se puedan presentar. Igualmente, precisa los procedimientos y protocolos de actuación para cada una de ellas minimizando el impacto en las personas, los bienes y el ambiente.

ROL	RESPONSABLE	MECANISMOS
Misionales	• Director de Registros Públicos • Director de Asuntos Jurídicos. • Director Desarrollo Empresarial • Director Administrativo Y Financiero. • Coordinador de transformación digital y formación empresarial. • Coordinador MASC.	Generar las directrices para la Creación, implementación y actualización del plan de continuidad del negocio.
		Realizar seguimiento a los lineamientos estratégicos dispuestos en el plan.
Profesionales de apoyo	• Profesional II de soporte tecnológico. • Profesionales de apoyo de las diferentes áreas involucradas.	Mesas de trabajo
		Gestor de Información
		Análisis de la información.
		Metodologías de riesgos.
		Inclusión plan de acción anual de las actividades.
Aprobación	• Presidente Ejecutivo. • Comité de Brigadas de Emergencia.	Decisión ejecutiva aprobando el plan de continuidad de negocio,

	• Director de Control Interno. • Profesional II De Calidad	haciendo responsable al comité y revisando, validando, ejecutando los documentos emitidos como oficiales para dejar firme la decisión.
Socialización y pruebas del plan de continuidad	• Directores de todas las áreas. • Profesional II de Talento Humano	Campañas de divulgación.
Activación del Plan de emergencia y Plan de restablecimiento	• Grupos de trabajo: • Todos los Directores de Área, • Coordinador de transformación digital y formación empresarial • Coordinador de Planeación • Coordinador Financiero • Profesional II de calidad. • Líder de Comunicaciones y Posicionamiento empresarial • Sistema de Salud Seguridad en el trabajo. • Gestión documental • Talento Humano.	Mesas de trabajo, Análisis y pruebas, Inspección y verificación.
Restablecimiento prestación de servicio		Comunicación con los grupos.

6. GLOSARIO

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la entidad, y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: documento en el que los colaboradores de la **CÁMARA DE COMERCIO DE FACATATIVÁ** o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Amenaza: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
Centro de cómputo: Datacenter, centro de procedimientos de datos; donde llegan todas las comunicaciones de las redes contratadas por la Entidad.
Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
Directorio Activo: Servicios de directorio es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración.
Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada
Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
Evaluación del Riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
Evento de Seguridad de la Información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión del Riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de Seguridad de la Información: un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.
ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
Resiliencia: La capacidad para adaptarse positivamente a situaciones adversas.
Sistema de Información (SI): Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
Seguridad de la Información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.
Sistema de Gestión de la Seguridad de la Información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
Plan de Continuidad del Negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
Tratamiento del Riesgo: proceso de selección e implementación de medidas para modificar el riesgo.
Valoración del Riesgo: proceso global de análisis y evaluación del riesgo.
Riesgo Financiero: se refiere a la probabilidad de ocurrencia de un evento que tenga consecuencias financieras negativas para una organización.
Pérdida Económica: falta o ausencia de dinero de la Entidad por concepto de fraude o robo.
Monitoreo: Proceso sistemático mediante el cual se verifica las instalaciones de la Entidad ante cualquier impacto de robo y saqueo.
Par del cargo: persona para desempeñar las funciones de otro cargo, temporalmente o en ausencia del titular original por vacaciones, incapacidades, licencias o cuando se requiera asegurando la continuidad de las funciones y procesos de la entidad.

7. PLAN DE CONTINUIDAD DE NEGOCIO

El presente documento enmarca todo evento denominado emergencia que podría llegar a pasar en la entidad y a su vez las posibles acciones que cada área podría realizar para controlar dichos eventos. Para ello, se ha dispuesto de diferentes

herramientas de análisis y seguimiento que son conocidas por los lideres de cada dirección.

8. GENERALIDADES DEL PLAN DE CONTINUIDAD

El Plan de Continuidad reúne un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la entidad y la prestación de sus servicios tecnológicos, para lo cual se establecen los siguientes aspectos:

- **Preventivo**: Dentro de este aspecto se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan articular a la gestión de los diferentes procesos.
- **Reactivo**: Este aspecto va dirigido a fortalecer las políticas internas de restauración y comunicarlas oportunamente para ponerlas en marcha una vez detectada la contingencia.
- **Recuperación**: Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia.

9. ANÁLISIS DEL ENTORNO INSTITUCIONAL

Teniendo en cuenta las funciones y obligaciones normativas de la Entidad, así como los lineamientos establecidos por Confecámaras, se consolidan y respaldan las actividades institucionales dentro del marco legal vigente. En este contexto, se realiza una revisión integral con el fin de identificar posibles factores que puedan afectar el adecuado desarrollo en la prestación de los servicios. Dichos factores se buscan mitigar mediante la implementación de un Plan de Continuidad, el cual se estructura en los siguientes aspectos:

Aspectos Externos

- **Económicos:** Disminución presupuestal, demoras o dificultades para el traslado de recursos de inversión o de funcionamiento, cambios de gobierno en la priorización y traslado de recursos.
- **Políticos**: Cambio de mesa directiva, nuevas prioridades del Senado, jornada electoral.
- **Sociales:** Manifestaciones y protestas frecuentes en el centro de la ciudad, dificultad de acceso para el grupo técnico y los usuarios de los sistemas, daños intencionados a la infraestructura de la Entidad. Y agresiones verbales

y/o físicas que se puedan presentar por parte de los usuarios a los colaboradores de la cámara de comercio de Facatativá por estar en desacuerdo o insatisfecho del servicio y/o políticas establecidas por la entidad

- **Tecnológicos:** Deficiencia en la interoperabilidad de los sistemas de administración, monitoreo y gestión, diferencia en las plataformas tecnológicas del negocio, ataques externos e internos a la información y las herramientas tecnológicas.

- **Medio Ambientales:** Ubicación de la entidad cerca a los cerros, incendios, terremotos, Inundaciones, desastres naturales.

Aspectos Internos

- **Financieros**: Dificultad para la priorización de recursos, cambios frecuentes en el plan de adquisición, comunicación inoportuna de los cambios, demoras en la apropiación de recursos, fallas en los sistemas de registro Sistema Integrado de Información Financiera (SIIF).
- **Personal:** Planta de personal insuficiente, nuevas exigencias de competencias del personal en el nuevo modelo de operación, tiempo insuficiente para el desarrollo de habilidades, falta de motivación e involucramiento del personal, alta rotación de personal.
- **Procesos:** nuevos procesos, desconocimiento de las características de los procesos, desconocimiento del nivel de responsabilidad y autoridad de los procesos, baja apropiación del nuevo modelo, baja asistencia a las capacitaciones de socialización y las mesas de creación de los procesos.
- **Tecnología**: Desconocimiento de un Plan estratégico de TI, desarticulación de las herramientas y aplicativos internos, fallas en la infraestructura tecnológica, fallas en el sistema de seguridad de la información, desconocimiento de los niveles de responsabilidad y autoridad frente a los sistemas.
- **Estratégicos**: Cambios en la gestión institucional sin planificación y comunicación oportuna, fallas en la comunicación y solicitud de información a las dependencias, ausencia de Acuerdo de nivel de servicio (ANS) concertados, fallas en la comunicación interna, solicitud de información múltiple, fallas en los sistemas de información.
- **Comunicación Interna**: Desconocimiento en los temas gestionados por parte de Confecámaras, Inapropiada distribución de canales internos, Inoportunidad en la entrega de información, falta de registros de información y contactos actualizados y protegidos.
- **Par del cargo:** ausencia del titular del cargo por vacaciones, incapacidades, licencias o cuando se requiera asegurando la continuidad de las funciones y procesos de la entidad.

10. RIESGOS ASOCIADOS A LA CONTINUIDAD DEL NEGOCIO

La **CÁMARA DE COMERICO DE FACATATIVÁ** en sus procesos identifican y administran los riesgos como práctica para impedir eventualidades internas o externas que impidan cumplir sus metas institucionales, por lo cual, al desarrollar el plan de continuidad del negocio se integra la metodología de riesgos aplicada y el control preventivo, detectivo y correctivo de dicho, este plan estaría asociado al mapa de riesgos institucional.

Para el monitoreo preventivo del ejercicio de continuidad del negocio y del servicio de la CÁMARA DE COMERCIO DE FACATATIVÁ **La Brigada De Emergencia** tendrá en cuenta los siguientes riesgos existentes:

Clasificación del riesgo	Nombre del riesgo	Descripción del riesgo
TIC	Perdida de información institucional	Se asocia con la pérdida de información física y digital de los archivos, bases de datos, servidores y Sistemas de Información de la Entidad
TIC	No restablecimiento de los servicios tecnológicos de la entidad	Contempla la disponibilidad para uno de la información y de los servicios que tiene la entidad con sus usuarios.
ADMINISTRATIVA	Pérdida de credibilidad y confianza en la entidad.	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la Entidad.
ADMINISTRATIVA	Daño o deterioro de los activos tangibles	Comprende el daño o deterioro de los bienes muebles o inmuebles de la Entidad.
TIC	Afectación de la infraestructura y tecnológica.	Está relacionado con el daño, pérdida, siniestro o deterioro a nivel de hardware, networking y enlaces de datos.
TIC	Inadecuados servicios de Tecnologías de la Información.	Contempla la pertinencia, calidad y oportunidad de los servicios de tecnología y las

Clasificación del riesgo	Nombre del riesgo	Descripción del riesgo
		deficiencias en la prestación de los mismos.

Estos riesgos están integrados a la matriz de riesgos del proceso que maneja la **CÁMARA DE COMERCIO DE FACATATIVÁ**, que son monitoreados a través del sistema de gestión de control interno de acuerdo a su regularidad.

11. PRUEBAS Y REVISIONES

Las acciones preventivas se llevarán a cabo en toda la entidad según la planificación contando como las direcciones involucrados como son Planeación, líder de comunicaciones y Coordinador de trasformación digital en conjunto de todas las Direcciones de la entidad y el área de Recursos Humanos, haciendo la verificación con el área de Control Interno; durante la definición de la planificación institucional se definirán y aprobarán los simulacros, interrupción del servicio, evacuación de emergencia o pruebas aleatorias del plan de continuidad, según los recursos económicos con los que se cuente en cada vigencia; de igual manera el seguimiento se realizará dos veces al año por **La Brigada De Emergencia.**

12. GESTIÓN DEL PLAN DE CONTINUIDAD

La Cámara de Comercio de Facatativá deberá emprender las acciones necesarias para comunicarlo a todos los colaboradores, contratistas y terceros de la entidad y de esta manera estar preparados para enfrentar situaciones de emergencia y restablecer en el menor tiempo posible el servicio, para lo cual se seguirá el siguiente protocolo:

OBJETIVO	ACCIÓN	RESPONSABLE	EVIDENCIA
Determinar la vulnerabilidad en el centro de datos e instalaciones de negocios y definir las medidas preventivas que se pueden tomar para reducir al mínimo la probabilidad y el impacto en la perdida de información de la Entidad	Registro de la emergencia presentada	**La Brigada De Emergencia**	Registro plataforma DocxFlow
	Convocar grupo de trabajo seguridad de la información	**La Brigada De Emergencia**	Acta de reunión
Definir la situación y los tiempos máximos de recuperación ante fallas o eventos catastróficos.	Revisión de la afectación de la Infraestructura.	**La Brigada De Emergencia**	FOR-PRE-08 – Acta de Reunión.
Definir niveles de alerta que permitan identificar posibles amenazas a la seguridad de la infraestructura tecnológica	Revisión de la afectación de la información Analizar daños	**Equipo de sistemas más La Brigada De Emergencia**	FOR-PRE-08 – Acta de Reunión.
Asegurar una pronta recuperación en los servicios misionales de la Entidad.	Analizar daños	**La Brigada De Emergencia**	Lista de los servicios afectados por cada líder de área.
	Contacto con sistemas de soporte	Equipo de Sistemas.	Registro en la plataforma de DocxFlow las actas.
	Restablecimiento de los servicios en un corto tiempo.	**La Brigada De Emergencia**, Coordinador de Planeación, Sistemas y Control Interno. Talento humano y Dirección Administrativa y financiera.	Registro en la plataforma de DocxFlow las actas. Registro en la plataforma de DocxFlow las actas.
Disminuir los tiempos de interrupción de la operación de los procesos.	Restablecimiento de los sistemas de información	**La Brigada De Emergencia**, Coordinadores de transformación digital y formación empresarial Verificando el área de Control Interno.	Registro en la plataforma de DocxFlow las actas.

OBJETIVO	ACCIÓN	RESPONSABLE	EVIDENCIA
Determinar la vulnerabilidad en el centro de datos e instalaciones de negocios y definir las medidas preventivas que se pueden tomar para reducir al mínimo la probabilidad y el impacto en la perdida de información de la Entidad	Registro de la emergencia presentada	**La Brigada De Emergencia**	Registro plataforma DocxFlow
	Convocar grupo de trabajo seguridad de la información	**La Brigada De Emergencia**	Acta de reunión
Definir las acciones para minimizar el tiempo de inactividad y la pérdida de datos de la entidad	Análisis de la situación	**La Brigada De Emergencia**	Informe de situación - Plan de Establecer, Plan mejoramiento.
	Establecer plan de mejoramiento a partir del análisis	**La Brigada De Emergencia** y Equipo de sistemas	

13. ESCENARIO DE EMERGENCIAS:

Escenario	*Grupo de respuesta especifico*
Emergencia social Se da una emergencia social en el momento en el que se presenten alteraciones de orden público, y afecte de manera directa y progresiva a la población del municipio de Facatativá y sus alrededores.	Líder de respuesta: **Profesional II de Talento Humano** Equipo de respuesta: **La Brigada De Emergencia**
Desastre natural y colapso de infraestructuras Se da una emergencia en el momento que se presente fenómenos naturales que obliguen la evacuación del personal con el objetivo primario de salvaguardar la vida (incendio, sismo, inundación,	Líder de respuesta: **Profesional I De SG-SST** Equipo de respuesta: **La Brigada De Emergencia.**

Escenario	*Grupo de respuesta especifico*
falla de servicios eléctricos, hidráulicos, sanitarios).	
Tecnológico Falla de sistemas de información, pérdida de datos, fallas en sistemas de telecomunicaciones que interrumpen los procesos institucionales e inhabiliten el uso de servicios de tecnología de información y comunicaciones para el normal funcionamiento de la entidad	Líder de respuesta: **Coordinador De transformación digital y formación empresarial** Equipo de respuesta: **La Brigada De Emergencia.**
Financiero Eventos que imposibiliten a la Entidad de contar con los recursos económicos para cumplir con compromisos misionales o con terceros como proveedores de servicios, estos eventos incluyen emergencia económica declarada por la Superintendencia de Sociedades, recortes presupuestales o cambios económicos abruptos que desestabilizan el normal funcionamiento de la Cámara de Comercio de Facatativá.	Líder de respuesta: **Director(a) Administrativo(a) y Financiero(a)** Equipo de respuesta: **La Brigada De Emergencia.**
Sanitario En esta categoría se agrupan los eventos causados por agentes biológicos que afectan a la salud de todos los seres vivos en particular la seguridad de los seres humanos, incluidos fenómenos como: pandemia, epidemias, crisis sanitaria que impide el funcionamiento de los procesos institucionales, entre otros.	Líder de respuesta: **Profesional I De SG-SST** Equipo de respuesta: **La Brigada De Emergencia.**

PBX (601) 8902833
WhatsApp: 3106691309
correspondencia@ccfacatativa.org.co

El Plan de Continuidad reúne un conjunto de actividades y procedimientos que mantienen en niveles aceptables el funcionamiento de la misionalidad de la Entidad Cámara de Comercio de Facatativá y la prestación de sus servicios durante eventos que impidan de manera significativa sus procesos normales. El plan de Continuidad se establece en tres momentos:

Prevención y Detección

Dentro de este aspecto se involucran los recursos humanos, operativos, técnicos, profesionales, coordinadores y directivos administrativos quienes deben estar preparados en caso de presentarse un evento inesperado, las acciones y la preparación de las áreas para iniciar su contingencia, las cuales se puedan articular a la gestión institucional en los diferentes procesos. Incluye las acciones de monitorización de los indicadores de la ocurrencia potencial de una emergencia. Las acciones de prevención incluyen el fortalecer la difusión de las políticas internas, los canales de comunicación, las estrategias de activación de la respuesta a contingencias, la difusión de los planes de respuesta.

Confirmación y Reacción

Este aspecto está orientado a las acciones necesarias para confirmar la materialización de un incidente que pondrá en riesgos la continuidad de la prestación de los servicios de la Entidad Cámara de Comercio de Facatativá, comunicar la emergencia identificada y la toma de decisión por parte del equipo de gestión de emergencias.

La Brigada De Emergencia que se creará, deberá de regular todas las tareas que se ejecutan para mantener las operaciones de los servicios institucionales en niveles aceptables mientras se resuelve las afectaciones generadas a la Entidad.

Recuperación y restablecimiento

Esta etapa incluye todas las actividades necesarias para retomar las actividades en su estado normal de funcionamiento una vez se han superado las situaciones que generaron la emergencia, se han restablecido los sistemas afectados o se han reparado las estructuras afectadas.

De igual manera, se define la estrategia para cada uno de los escenarios así:

Escenario 1: Emergencia social

Escenario 1: Emergencia Social
Líder de respuesta: **Profesional II de Talento Humano**
Equipo de respuesta: **La Brigada De Emergencia**
Fase 1: Detección
Identificación de alertas 1) El área de Comunicaciones a través de la revisión de mensajes en redes sociales identifica mensajes de alerta asociados a convocatorias de manifestaciones y reuniones con el propósito de realizar protestas en la zona de trabajo de la Entidad. **Confirmación** 1) El área de Talento Humano remitirá el comunicado a **La Brigada De Emergencia** donde se establecerá los respectivos mecanismos de reacción.
Fase 2: Activación
1) El Equipo de **La Brigada De Emergencia** evalúa la información y decide si se debe activar o no el plan de evacuación, activación de manejo de crisis por emergencia social y autorización de hora cierre de las instalaciones y salida del personal. 2) Cuando **Profesional II de Talento Humano** reciba la confirmación sobre ocurrencia de crisis por emergencia social, por parte de los miembros de **La Brigada De Emergencia** se considerará hacer el comunicado pertinente por medio de los correos institucionales.
Fase 3: Plan de operación alterno
1) Profesional II de Talento Humano comunica al Director de Administrativa y Financiera vía telefónica o mediante correo institucional, que se deben cerrar las instalaciones y publicar en la página oficial de la Cámara de Comercio de Facatativá sobre la suspensión de actividades por el día. 2) Profesional II de Talento Humano coordina con el área de seguridad y salud en el trabajo que se transmita el comunicado estandarizado de activación de plan de

evacuación a través del voz a voz, correo electrónico y grupos cerrados de mensajería instantánea de las diferentes dependencias. 3) Profesional I de Comunicaciones ordena la publicación en sitio web la suspensión de servicio presencial. 4) El director de Administrativo y Financiero notifica al director de Registros Públicos la suspensión de atención de ciudadanos y se debe coordinar la salida de los externos de esa dependencia. 5) Los jefes de dependencia ordenan la activación del trabajo en casa utilizando las herramientas de la Cámara de Comercio de Facatativá, Correo electrónico, grupos, se aplica el protocolo de trabajo remoto usando las herramientas que genera la Entidad. 6) Los COLABORADORES, contratistas y externos de la entidad deben abandonar la sede, dirigirse a sus casas y notificar a sus jefes inmediatos por los grupos internos de mensajería instantánea su llegada a casa validando su llegada segura a demás su trabajo se monitorea a través del formato FOR-TH- 24 SEGUIMIENTO TRABAJO EN CASA para ser revisado y evaluado por cada director de área. 7) Los directores de cada dependencia comunican al Profesional II de Talento Humano el resultado del reporte de llegada a casa de sus colaboradores. 8) El Profesional II de Talento Humano genera informe de resultado de evacuación de instalaciones a **La Brigada De Emergencia** vía correo institucional. 9) Servidores y contratistas realizan sus actividades asignadas en modalidad de trabajo en casa hasta que los jefes de dependencia notifiquen el retorno a la sede normal de trabajo. 10) El trabajo en casa se debe mantener hasta que se reciba comunicación formal de **La Brigada De Emergencia** indicando la solución de la emergencia.
Fase 4: Solución del incidente
1) **La Brigada De Emergencia** a través de los correos institucionales informa al Profesional II de Talento Humano sobre el comunicado que se debe remitir a la superintendencia de sociedad de acuerdo con el director de registros públicos sobre el cierre. 2) El Equipo de **La Brigada De Emergencia** define si se debe autorizar el reinicio de operaciones en la sede. En caso de autorizar el reingreso a la sede se comunicarla decisión mediante correos institucionales.

3) El Profesional II de Talento Humano gestiona con el área de Comunicaciones la transmisión del mensaje de retorno a la sede principal a través de correo electrónico, mensajes instantáneos por grupos cerrados de WhatsApp 4) Se publica en la página oficial de la Cámara de Comercio de Facatativá la notificación de la normalidad de actividades. 5) Servidores y contratistas retornan a sus labores en la sede principal de la Entidad 6) Si se realizó movimiento de equipos de cómputo durante la activación del trabajo en casa el coordinador de sistemas de información organiza el reintegro de los equipos que salieron de las instalaciones nuevamente a la sede de la Entidad revisando el FOR-DAF-52 SALIDA DE ACTIVOS.

Escenario 2: Desastre natural y colapso de infraestructuras.

Escenario 2: Desastre natural y colapso de infraestructuras.
Líder de respuesta: **Profesional I De SG-SST**
Equipo de respuesta: **La Brigada De Emergencia**
Fase 1: Detección
Identificación de alertas En caso de sismo: se detectan movimientos súbitos en todo el edificio, se observa oscilaciones en objetos suspendidos. En caso de fuego / incendio: **Profesional I de SS-SGT** identifica evento de riesgo asociado a fuego, la detección se puede realizar mediante el sistema de detección de humo, notificación de testigo o inspección directa de la escena. En caso de fenómeno natural: vendaval, granizada, inundación por borrasca o lluvia intensa: **La Brigada De Emergencia** identifica evento de riesgo asociado a inundación, la detección se realiza por inspección directa de la escena. **Confirmación**

PBX (601) 8902833
WhatsApp: 3106691309
correspondencia@ccfacatativa.org.co

En caso de sismo: la confirmación de sismo es inmediata, todo el personal dentro de las instalaciones percibe el fenómeno. En caso de sísmo personal dentro de edificio: buscan refugio bajo escritorios, mesas o estructuras fuertes, permanecen allí hasta que cese el movimiento, alejarse de ventanales, estantería alta, lámparas o cualquier otro elemento que esté suspendido o pueda caer protegerse la cabeza y cuello con las manos, prepárese para evacuar en caso de que se dé la señal de alarma; no debe devolverse por ningún motivo al edificio. Nunca use ascensores para evacuar. En caso de incendio, fuga de gases o líquidos peligrosos: El o la directora(a) de Administrativo(a) y Financiero(a) confirma el evento de fuego, evalúa nivel de riesgo y notifica necesidad o no de realizar evacuación de las instalaciones. Si el fuego esta fuera de control se deben ordenar la evacuación inmediata iniciando con el área afectada, las áreas próximas y luego las más alejadas. Se debe dar inicio la fase de activación del escenario de crisis 2 desastre natural, colapso de infraestructura. Se llama al cuerpo de bomberos del municipio de Facatativá. Si el fuego se puede controlar con la brigada de emergencia institucional, se realiza su control con los equipos disponibles y se notifica al cuerpo de bomberos. Se ejecuta la fase de activación del escenario de crisis 2 **[Desastre Natural y colapso de infraestructuras]** En caso de fenómeno natural: vendaval, granizada, inundación por borrasca o lluvia intensa: el o la directora(a) administrativo(a) y financiero(a) confirma que el evento de inundación, borrasca o daño por inundación, evalúa nivel de riesgo y notifica necesidad o no de realizar evacuación de las instalaciones. Si la inundación imposibilita el desarrollo de las actividades institucionales convoca al Equipo de Comité de Emergencia para evaluación de activación de escenario de crisis 2. **[Desastre Natural y colapso de infraestructuras]**
Fase 2: Activación
En caso de sismo, fuego, fuga de materiales peligrosos o gases, sismo; • **Profesional I de SS-SGT** activa la alarma sonora y notifica a los brigadistas de la orden de evacuación • **Profesional I de SS-SGT** alerta por radio al personal de vigilancia para realizar apertura de puertas y preparación para evacuación preventiva del edificio

• **Profesional I de SS-SGT** determina momento adecuado para ordenar evacuación si es necesario.

• Brigadistas de piso inician protocolo de evacuación por dependencia, coordinan el proceso de evacuación hasta el punto de encuentro si es necesario.

• Cuando el personal haya sido evacuado en su totalidad el **Profesional I de SS-SGT** evalúa por inspección visual el detalle de daño a estructuras, presencia de víctimas o desarrollo particular de la emergencia en su sector.

• Si se detectan fallas en la estructura que hacen evidente que NO se puede reingresar:

• **Profesional I de SS-SGT**, gestiona la interrupción inmediatamente suministros eléctrico, de gas, de combustibles desde registros externos al edificio si es factible hacerlo, en caso contrario deben esperar al personal de Bomberos o grupo de atención de emergencia

• **El coordinador de transformación digital y formación empresarial**, define, de acuerdo con resultado de evaluación de daños en la estructura y por la naturaleza de la emergencia SI aún es viable apagar el centro de datos ordenadamente, en caso contrario los equipos tendrán apagado por el corte de energía preventivo

• **La Brigada De Emergencia** escala el manejo de la emergencia sobre la edificación en las autoridades competentes, Cuerpo de Bomberos del municipio de Facatativá de acuerdo con la opinión del **Profesional I de SS-SGT**, se envía mensaje por grupos de mensajería instantánea la orden para que el personal se dirija a sus lugares de habitación y espere instrucciones de su jefe de dependencia

• Servidores y contratistas se dirigen a sus casas y reportan a su jefe inmediato su llegada y estado de salud mediante los grupos cerrados de WhatsApp.

• Los directores de cada dependencia comunican al **Profesional II de talento humano** el resultado del reporte de llegada a casa de sus subalternos

• **El Profesional II de Talento Humano** genera informe de resultado de evacuación de instalaciones a **La Brigada De Emergencia** vía correo institucionales.

• **El Coordinador de transformación digital y formación empresarial y Líder de comunicaciones y posicionamiento empresarial** evalúa con su equipo de trabajo el estado de funcionamiento de los sistemas informáticos dentro del centro de cómputo y los servicios de información que estén en funcionamiento fuera del centro de cómputo.

• El Coordinador de sistemas de información activa plan de recuperación antes tecnológico [escenario de crisis Nro. 3], Desastre tecnológico

• Cuando se cuente con servicios informáticos alternos, los jefes de dependencia ordenan la activación de trabajo en casa utilizando las herramientas colaborativas que dispongan.

• Servidores y contratistas realizan sus actividades asignadas en modalidad de trabajo en casa hasta que los jefes de dependencia notifiquen el retorno a la sede normal de trabajo

• El trabajo en casa se debe mantener hasta que se reciba comunicación formal de **La Brigada De Emergencia** reportando la solución de la emergencia.

• Si se detecta que es viable volver a entrar al edificio, se debe esperar la autorización de los organismos de emergencia para el reingreso a las instalaciones. El **Profesional I de SS-SGT** debe comunicar el resultado de la evaluación que formule el organismo de emergencia e indicar a **La Brigada De Emergencia** la recomendación de reingreso o no al edificio.

En caso de natural: vendaval, granizada, inundación por borrasca o lluvia intensa

a) Cuando el **Profesional I de SS-SGT** confirma la ocurrencia de crisis por fenómeno natural y la evaluación determina que no se pueden continuar operando en la sede, recopila la información de confirmación de la crisis y en llamada grupal con los miembros de **La Brigada De Emergencia** expone la situación y somete a consideración la necesidad de iniciar la activación del plan de continuidad por la ocurrencia del escenario 2. **[Desastre Natural y colapso de infraestructuras]**

b) **La Brigada De Emergencia** evalúa la información y decide si se debe activar o no el plan de evacuación, activación de manejo de crisis por desastre natural y colapso de infraestructuras, confirman la autorización de hora cierre de las instalaciones y salida del personal.

c) El **Profesional I de SS-SGT** activa la alarma sonora y notifica a los brigadistas de la orden de evacuación

d) El **Profesional I de SS-SGT** alerta por radio al personal de vigilancia para realizar apertura de puertas y preparación para evacuación preventiva del edificio.

Fase 3: Plan de operación alterno

PBX (601) 8902833
WhatsApp: 3106691309
correspondencia@ccfacatativa.org.co

1) El **Líder de comunicaciones y posicionamiento empresarial** ordena la publicación en sitio oficial de la Cámara de comercio de Facatativá la suspensión de servicio presencial. Por grupos cerrados de WhatsApp se comunica a los servidores y contratistas que deben trabajar desde sus casas. 2) **Profesional I de SS-SGT** notifica al Director(a) de Registros Públicos la suspensión presencial de atención a ciudadanos y se fija cartel en la edificación 3) Los jefes de dependencia ordenan la activación de trabajo en casa utilizando las herramientas colaborativas, Correo electrónico, grupos de mensajería. 4) Servidores y contratistas realizan sus actividades asignadas en modalidad de trabajo en casa hasta que los jefes de dependencia notifiquen el retorno a la sede normal de trabajo. 5) El trabajo en casa se debe mantener hasta que se reciba comunicación formal de **La Brigada De Emergencia** reportando la resolución de la emergencia.
Fase 4: Solución del incidente
1) **La Brigada De Emergencia** coordina con el **profesional I de SS-SGT** las actividades de reparación de las instalaciones físicas afectadas. 2) De acuerdo con la naturaleza de la emergencia puede llegar a ser necesario: reparar la sede por daños causados por agua o fuego. Limpieza de áreas con personal especializado en materiales peligrosos o en el peor escenario búsqueda de sedes alternas en caso de que la sede principal quede inutilizable. 3) **La Brigada De Emergencia** define si se debe autorizar el reinicio de operaciones en la sede. En caso de autorizar el reingreso a la sede se comunicarla decisión mediante correos institucionales y mensaje instantáneo vía Whats App. 4) El **Profesional II de Talento Humano** coordina con el **Líder de comunicaciones y posicionamiento empresarial** la transmisión del mensaje de retorno a la sede principal a través de correos institucionales, mensajes instantáneos por grupos cerrados de WhatsApp. 5) Se publica en la página oficial de la Cámara de Comercio De Facatativá, notificando la vuelta a normalidad de actividades.

Escenario 3: Desastre tecnológico

Cámara de Comercio de Facatativá y del Noroccidente de Cundinamarca

PBX (601) 8902833
WhatsApp: 3106691309
correspondencia@ccfacatativa.org.co

Escenario 3: Desastre tecnológico
Líder de respuesta: **Coordinador De Transformación digital y formación empresarial**
Equipo de respuesta: **La Brigada De Emergencia**
Fase 1: Detección

Identificación de alertas, el equipo de la Oficina de Sistemas de Información monitoriza los componentes que soportan los sistemas de información, servicios informáticos y la infraestructura de servicio esenciales del centro de datos para identificar eventos no deseados que puedan generar fallas que conduzcan a pérdida de continuidad de servicio, los elementos que se monitorización continuamente incluyen:

Subsistemas de telecomunicaciones

- Router de acceso a Internet
- Canal de acceso a servicios de Internet
- Equipos de seguridad

Servicios de mensajería electrónica y sistema colaborativo Office 365

Servidores virtuales y físicos que soportan sistemas de información institucionales

- Sitio web Institucional
- Sistema de gestión documental DocXFlow
- Sistema de soporte tecnológico
- Canales virtuales de comunicación

Confirmación

A partir de los resultados de la revisión de los sistemas de información, monitorización de alertas, reportes de los usuarios y notificación de partes interesadas sé determina la ocurrencia de emergencias que suspenderán la prestación de servicios informáticos de la Entidad como:

- Ataques cibernéticos como denegación de servicios.
- Secuestro de la información institucional por ataque de software malicioso.
- Falla eléctrica por voltaje severamente reducido, depresión es, picos y sobre voltajes.
- Caída total del servicio de acceso a Internet o red local institucional.

• Caída de canales de comunicación principales a cargo de los proveedores de acceso a Internet que alteren y/o interrumpan el normal funcionamiento de los equipos que se utiliza para los procesos misionales. • Fuego o inundación del centro de datos que obliga al apagado de todo el centro de datos. • Falla total del sistema de almacenamiento masivo de datos compartidos • Falla total del sistema de virtualización de servidores. • Indisponibilidad total de bases de datos por corrupción de datos. • Pérdida acceso a sistemas críticos por finalización de licencia de uso. • Manipulación incorrecta de sistemas informáticos debido a: Actividad errónea de administración de base de datos, corrupción de la base de datos, acceso indebido a la base de datos para modificarla, errores en puesta en producción / regresión con impacto en base de datos y errores en generación y restauración de respaldos que conlleven a la pérdida total o parcial de los servicios • Por problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques externos para obtención/modificación indebida de información. Los profesionales responsables de la administración de los sistemas afectados realizan un diagnóstico sobre el incidente, teniendo en cuenta: • Naturaleza e impacto del incidente. • Estrategias definidas en el Plan de Recuperación ante desastres aplicables u otras soluciones potenciales definidas por la base de conocimientos de la mesa de servicio. • Tiempo estimado de solución del incidente. **Componente tecnológico/ Tiempo máximo tolerable de caída Sistema de información** Suministro de energía eléctrica de Consultar tabla de análisis de impacto al centro de datos negocio.
Fase 2: Activación
1) El **Coordinador de transformación digital y formación empresarial** alerta a **La Brigada De Emergencia** de la necesidad de aplicar el plan de recuperación ante desastres de tecnología y la necesidad de activar los planes de operación alterna de cada una de las dependencias ante la caída de los servicios informáticos

por un periodo superior al tiempo máximo tolerable definido en el análisis de impacto. Dentro su comunicación incluye aspecto como:

- Sistemas y servicios afectados.
- Resultados del diagnóstico sobre los sistemas afectados.
- Acciones de recuperación realizadas hasta el momento.
- Tiempo estimado para el restablecimiento de los servicios afectados.
- Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles.
- Recomendación de activar el plan de continuidad institucional e iniciar la ejecución del plan recuperación ante desastres de tecnología.

2) **La Brigada De Emergencia** evalúa la información y decide si se debe activar el plan de continuidad y plan de operación alterno de cada una de las dependencias. Si se aprueba la ejecución del plan de operación alterno por desastre tecnológico, el **Coordinador de transformación digital y formación empresarial** comunica por correo institucional al **Profesional II de Talento Humano** que se debe notificar a los jefes de dependencia la necesidad de aplicar sus respectivos planes de operación alterno por crisis de infraestructura tecnológica.

3) **La Brigada De Emergencia** define el mensaje oficial de respuesta que se comunicará a los grupos de valor que incluyen: SOPORTE TECNOLÓGICO DE LA CÁMARA DE COMERCIO DE FACATATIVÁ <<freshservicecomsupport@facatativa.freshservice.com>> y COLABORADORES, contratistas de la Entidad a través de los grupos de mensajería instantánea.

Dentro de la comunicación a divulgar el equipo de gestión de emergencia define:

- ¿Qué información concreta se tiene sobre la crisis (incidente presentado, diagnóstico, tiempo de solución)?
- ¿Qué información está en proceso de verificación e investigación?
- ¿Qué información válida se puede comunicar inmediatamente (mensaje)?
- ¿Qué información se debe manejar al interior de la entidad?
- ¿Quiénes fueron afectados por la crisis (audiencia)?
- ¿Qué otras audiencias deberían saber sobre la crisis?
- ¿Cómo se comunicará la información a los interesados o afectados (medio)?

6) **La Brigada De Emergencia** activa su protocolo de comunicación a los grupos de valor considerando los siguientes lineamientos:

- Informar rápida y periódicamente a **La Brigada De Emergencia** ante una situación de emergencia tecnológica de alto impacto, la entidad se debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malentendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus grupos de trabajo.
- Decir la verdad: ser honestos en los comunicados, sin embargo, no significa transmitir TODA la información, soló aquella que es suficiente para generar confianza y tranquilidad son sus grupos de trabajo.
- La información que esté calificada como clasificada o reservada solo se debe transmitir a los debidamente autorizados el Coordinador de Sistemas de Información determina con el apoyo en seguridad digital la sensibilidad de la información a publicar
- Emitir reportes lo más exactos posible: publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. Evitar toda clase de especulación o falsa expectativa.

7) Siguiendo el plan de operación alterno de cada dependencia los jefes de dependencia imparten las ordenes correspondientes a los subalternos para mantener las actividades misionales críticas usando los recursos disponibles. Si paralelamente a la ocurrencia de la emergencia de desastre tecnológico se presentan los escenarios 1 Emergencia social y 2 Falla de infraestructura física, **La Brigada De Emergencia** sigue el protocolo de actuación de esos escenarios para determinar si el edificio se debe evacuar o no. Si no es necesaria la evacuación del edificio todas las actividades misionales continúan ejecutándose desde el edificio hasta que se supere la emergencia o el Equipo de gestión de emergencia determine lo contrario.

Fase 4: Solución del incidente

1) Cuando se realice el restablecimiento de los sistemas informáticos afectados **El Coordinador de transformación digital y formación empresarial**, notifica a **La Brigada De Emergencia** cuales servicios han sido restablecidos y que sistemas informáticos ha sido recuperados

2) Con la información de estado de funcionamiento de los sistemas informáticos, **La Brigada De Emergencia** autoriza la reactivación de procesos a sus condiciones normales tomando en cuenta el orden de restablecimiento de servicios definido en

el análisis de impacto al negocio, para lo cual Consulta la tabla de análisis de impacto al negocio. 3) **El Coordinador de transformación digital y formación empresarial**, siguiendo el orden de reanudación de procesos y la disponibilidad de servicios TIC requerido por cada proceso, notifica al director de cada dependencia respectiva para que realice las actividades de vuelva a operación normal. 4) Los directores de dependencia aplican las acciones definidas de vuelta a operación normal definidas en sus respectivos planes de operación alterna 5) **El Coordinador de transformación digital y formación empresarial**, informa A **La Brigada De Emergencia** el avance en la reactivación de procesos. Cuando todos los procesos hayan finalizado su plan de operación alterno, se prepara informe final de resolución de la emergencia para **La Brigada De Emergencia**. Confirmando que todos los procesos y dependencias se encuentran funcionando en condiciones normales y se prepara comunicado oficial de finalización de la emergencia para los grupos de valor.

Escenario 4: Crisis Financiera

Escenario 4: Crisis Financiera
Líder de respuesta: **Director(a) Administrativo(a) y Financiero(a)**
Equipo de respuesta: **La Brigada De Emergencia**
Fase 1: Detección
Identificación de alertas **Análisis del entorno interno** Mediante evaluación y seguimiento variables institucionales, se identifican signos de posibles restricciones financieras. 1) Relevancia de las iniciativas del Plan de Gobierno asociadas a obligaciones institucionales 2) Análisis previo de las iniciativas consignadas en el plan financiero 3) Análisis de entorno y variables macroeconómicas.

4) Tiempos destinados a la planeación sectorial vs los tiempos asignados a la planeación institucional.

Se identifican señales de alerta de escenario de crisis financiera a partir de:

1) Seguimiento a los resultados de presupuesto.

2) Seguimiento a la definición del marco de gasto de mediano plazo.

3) Seguimiento a posibles recortes al presupuesto cuando se recomponen partidas.

4) Distribución de presupuesto.

Por otro lado, Superintendencia financiera de Colombia regula toda acción que afecte a nivel general, por lo que se mantiene una comunicación constante.

Fase 2: Activación

Respecto a la activación del Plan de Continuidad, se identifica que, a partir del resultado de la asignación de presupuesto y la priorización de los proyectos, la Alta dirección debe ser notificada acerca de la suficiencia de recursos para cumplir con las obligaciones del Plan Presupuestal. En caso de detectar que el presupuesto asignado no será suficiente la Alta dirección debe activar las acciones de tratamiento de crisis financiera. Usando la información de resultados de la negociación del presupuesto y la priorización de proyectos, la alta dirección activa las acciones para contrarrestar los efectos de la eventual crisis financiera con acciones como:

1) Verificar la priorización de los diferentes proyectos de acuerdo con criterios que se diseñan en el mismo instante que se detecta la potencial emergencia.

2) Posibilidad de renegociar la asignación de presupuesto.

3) Búsqueda de fuentes alternativas para suplir recursos financieros para los proyectos

4) Sustentar la necesidad de obtener recursos de otras entidades.

Fase 3: Plan de operación alterno

Considerando la obligatoriedad de cumplir con los compromisos del Plan Presupuestal, la alta dirección define estrategias para:

• Priorizar la ejecución de ciertas iniciativas de alto impacto en los compromisos y desarrollo de planes alternos para cumplir con los compromisos durante la vigencia • Nivel de prioridad de las necesidades versus el ante proyecto de presupuesto. • El ajuste de prioridades de ejecución de los proyectos de acuerdo con los recursos disponibles para la vigencia y prioridades. • Fuentes alternas como convenios interinstitucionales Las acciones de respuesta a la crisis financiera se mantienen para monitorizar el porcentaje de ejecución real de los compromisos versus la ejecución presupuestal planificada, lo que implica el uso de tableros de indicadores precisos.
Fase 4: Solución del incidente
1. Cuando los compromisos de Gobierno están subsanados financieramente mediante la gestión de consecución de otras fuentes. 2. Cuando el presupuesto de funcionamiento e inversión corresponde a las necesidades. 3. Cuando las brechas de presupuesto (sin imprevistos) se han gestionado mediante recursos internos.

Escenario 5: Pandemia - Epidemia

Escenario 5: Pandemia - Epidemia
Líder de respuesta: **Profesional I De SG-SST**
Equipo de respuesta: **La Brigada De Emergencia**
Fase 1: Detección
Identificación de alertas A través de la monitorización de riesgos y alertas del sistema de gestión de seguridad y salud en trabajo, los reportes oficiales entidades y organizaciones de la salud, el Grupo de Gestión de Talento Humano se entera de brotes epidemiológicos a nivel Colombia o el continente: Ministerio de Salud y la Protección Social (MinSalud), La Secretaria de salud departamento de

Cundinamarca (sistema SIVIGILA), Organización Panamericana de la Salud (OPS Alertas) Organización Mundial de la Salud (OMS Alertas).

Confirmación

1. La información sobre la evolución y recomendaciones para la prevención de brotes epidemiológicos de diferente naturaleza se consulta con la Administradora de Riesgos Laborales quienes generan recomendaciones a la Entidad.

2. El Grupo de Talento Humano utiliza la información generada por la ARL y la información oficial del Ministerio de Salud, para alertar a **La Brigada De Emergencia**, sobre el nivel de alerta del país.

3. La información sobre niveles de alerta, medidas de mitigación y acciones que determine el gobierno nacional son evaluadas por **La Brigada De Emergencia** para tomar la decisión de activar el plan de contingencia de trabajo en casa y otras medidas que determine la rama ejecutiva.

Fase 2: Activación

Con base en las ordenes de la rama ejecutiva, el **Director (a) Administrativo(a) y Financiero(a)** autoriza la activación del plan de contingencia para el escenario de pandemia / Epidemia siguiendo los protocolos que defina el gobierno nacional:

1) Seguir el protocolo de salud que defina el Ministerio de Salud y la Protección social. Ejemplo: decreto 666 de 2020 Protocolo general de Bioseguridad Normativa COVID-19 2) el Profesional II de Talento Humano se comunica con el Profesional I SS-SGT Y Oficina Asesora de Comunicaciones para publicar en el sitio web institucional, redes sociales de la Entidad e instalaciones de la Entidad, mensaje comunicando a todos los grupos de valor indicando las medidas adoptadas por la Entidad para la atención al público en caso de epidemia o pandemia.

3) El **profesional II de Talento Humano** se comunica con **La Brigada De Emergencia** para que inicie la coordinación de los protocolos de trabajo en casa con todas las dependencias.

4) Los Directores de las dependencias coordinan con sus equipos de trabajo, el cargue de información vital o esencial para el trabajo en casa en los servicios de nube (office 365 / OneDrive), los coordinadores de grupo confirman con los servidores y contratistas de sus dependencias, el cargue de información vital para iniciar el trabajo remoto. De acuerdo con las instrucciones del Presidente Ejecutivo de la Entidad y directores de las diferentes dependencias se ordena la activación del trabajo en casa utilizando las herramientas colaborativas TEAMS, Correo

electrónico, grupo de mensajería instantánea a partir del día y hora definidos la entidad aplica sus protocolos de trabajo en casa.

5) Una vez se ha activado la modalidad de trabajo en casa para cada una de las dependencias, el **Profesional II de Talento Humano** genera un informe para **La Brigada De Emergencia** sobre los resultados del inicio de la contingencia por Pandemia/Epidemia.

6) El trabajo en casa debe mantener hasta que se reciba comunicación formal **La Brigada De Emergencia** indicando que se iniciará el retorno a trabajo dentro de la sede de la Entidad.

Fase 3: Plan de operación alterno

1) Durante la activación del trabajo en casa los servidores públicos continuaran realizando sus labores desde sus casas de acuerdo con las instrucciones que para tal fin impartan los Directores de las diferentes dependencias y los supervisores de contrato.

2) Para aquellas dependencias con responsabilidad de atención presencial el director de registro públicos activara planes de activación alterna.

3) Durante la ejecución de labores en la modalidad de trabajo en casa las siguientes actividades pueden llegar a ser actividades por el **Profesional II de SS-SGT:**

a) Realizar capacitación virtual mediante infografías, videos, mensajes o charlas virtuales a todos los servidores y trabajadores sobre prevención de las enfermedades que generaron la alerta de pandemia.

b) Reporte de casos sospechosos por contagio de la Epidemia/ Pandemia antela ARL y la EPS.

c) Establecer canales de comunicación para mantener informados a los COLABORADORES sobre medidas de prevención sobre la prevención, propagación y atención de la enfermedad

d) Determinar en conjunto con al ARL los mecanismos para proveer a los servidores los elementos de protección personal en caso de que sean estos requeridos.

e) Todos los COLABORADORES deberán acatar las instrucciones determinen las autoridades en materia de salud para su cuidado personal.

Fase 4: Solución del incidente
1) **La Brigada De Emergencia** continuamente monitorizan las instrucciones del gobierno nacional como respuesta a la epidemia / pandemia. 2) Cuando las autoridades en materia de salud así lo indiquen y siguiendo los protocolos de bioseguridad que para tal fin se definan, **La Brigada De Emergencia** determina las condiciones de reactivación del trabajo en la sede. 3) **La Brigada De Emergencia** define si se debe autorizar el reinicio de operaciones en la sede. En caso de autorizar el reingreso a la sede se comunica la decisión mediante los canales oficiales establecidos 4) **El Profesional II de Talento Humano coordina con Líder de comunicaciones y posicionamiento empresarial y Profesional I de SS-SGT**, la transmisión del mensaje de retorno a la sede principal a través de correos institucionales, mensajes instantáneos por grupos cerrados de WhatsApp, comunicaciones en la página principal de la Cámara de Comercio de Facatativá.

Escenario 6: Pares de cargos

Escenario 6: Continuidad de los procesos Administrativos "Pares de Cargos"
Líder de respuesta: **Profesional II De Talento Humano**
Equipo de respuesta: **Directores de Área o responsables de proceso**
Fase 1: Detección
Persona que desempeñara las funciones de otro cargo, temporalmente o en ausencia del titular original por vacaciones, incapacidades, licencias, permisos o cuando se requiera asegurando la continuidad de las funciones y procesos de la entidad.

RELACIÓN DE PARES DE CARGOS:

Nivel	Código	Denominación Empleo	Par de Cargo	N°. De Cargos
Directivo	D-201	Presidente Ejecutivo	Director de Registros Públicos	1
	D-101	Director de Control Interno	Profesional II de Control Interno	1
	D-102	Director de Desarrollo Institucional	Coordinador de Planeación	1
	D-103	Director Administrativo y Financiero	Coordinador Financiero	1
	D-104	Director de Asuntos Jurídicos	Coordinador M.A.S.C	1

	D-105	Director de Registros Públicos	Coordinador de Registro	1
	D-106	Director de Desarrollo Empresarial	Sub - Director de desarrollo Empresarial	1
Sub-Director	S-101	Sub - Director de desarrollo Empresarial	Gestor de Proyectos y competitividad empresarial	1
Profesional	P-301	Coordinador de Servicios Empresariales y Territoriales	Coordinador de Registro / Profesional II De Revisión Jurídica	2
	P-302	Coordinador de Planeación	Coordinador de Transformación Digital y Formación Empresarial / Profesional I de Presupuesto y Contabilidad	2
	P-303	Coordinador de Transformación Digital y Formación Empresarial	Profesional II de Soporte Tecnológico	1
	P-304	Coordinador Financiero	Profesional I de Presupuesto y Contabilidad / Profesional II De Tesorería	2
	P-305	Coordinador de Registro	Coordinador de Servicios Empresariales y Territoriales	1
	P-306	Coordinador M.A.S.C	Líder I Asesoría jurídica y formación empresarial	1
	P-307	Coordinador de gestión de Proyectos y servicios empresariales	Gestor de Proyectos y competitividad empresarial	1
	P-201	Profesional II de Talento Humano	Profesional I De SG-SST / Profesional II De Apoyo Jurídico	2
	P-202	Profesional II de Revisión Jurídica	Profesional II De Revisión Jurídica	4
	P-203	Profesional II de Gestión de Calidad	Profesional I De Gestión Documental / Líder de Comunicaciones y Posicionamiento empresarial	2
	P-204	Profesional II de Tesorería	Coordinador Financiero / Profesional I de Nómina e Inventarios / Profesional I De Presupuesto y Contabilidad	3
	P-205	Profesional II de Contratación	Profesional II de Apoyo Jurídico	1
	P-206	Profesional II de Apoyo Jurídico	Profesional II de Contratación	1
	P-207	Líder I asesoría jurídica y formación empresarial	Profesional II De Contratación / Gestor Jurídico y de desarrollo empresarial	1
	P-208	Profesional II de Control Interno	Director de Control Interno / Profesional II de Apoyo Jurídico	2
	P-209	Profesional II de Soporte Tecnológico	Coordinador de Transformación Digital y Formación Empresarial	1
	P-101	Líder de Comunicaciones y Posicionamiento empresarial	Director de Desarrollo Institucional / Coordinador de Transformación Digital y Formación Empresarial / Profesional I De Gestión Documental	3
	P-102	Profesional I de Gestión Documental	Técnico II de Gestión Documental	1

	P-103	Profesional I de Presupuesto y Contabilidad	Coordinador Financiero	1
	P-104	Profesional I de Nómina e Inventarios	Profesional II de Tesorería	1
	P-105	Profesional I de Revisión Financiera	Profesional I de Revisión Financiera	3
	P-106	Gestor de Proyectos y competitividad empresarial	Gestor de Proyectos y competitividad empresarial	3
	P-107	Profesional I de Revisión Jurídica	Profesional I de Revisión Jurídica	2
	P-108	Profesional I de SG-SST	Profesional II de Talento Humano	1
	P-109	Profesional I de Registro	Profesional I de Revisión Financiera	1
	P- 110	Gestor Jurídico y de desarrollo empresarial	Líder I asesoría jurídica y formación empresarial	1
Técnico	T-201	Técnico II de Registro y CAE	Técnico II de Registro y CAE	8
	T-202	Gestor I de apoyo al emprendimiento	Gestor II en apoyo a la asociatividad	1
	T-203	Técnico II de compras	Técnico II Financiero y Contable	1
	T-204	Técnico II Financiero y Contable	Técnico I de Contabilidad	1
	T-205	Técnico II de Gestión Documental	Profesional I de Gestión Documental	1
	T-206	Técnico II De Presidencia	Técnico I de Contabilidad / Técnico I De Talento Humano	2
	T-207	Técnico II de Registro y Vue	Técnico II de Registro y Vue	2
	T-102	Gestor II en apoyo a la asociatividad	Gestor II en apoyo a la asociatividad	2
	T-103	Técnico I de P.Q.R.S.	Técnico I de Correspondencia	1
	T-104	Técnico I de Correspondencia	Técnico I de P.Q.R.S.	1
	T-105	Técnico I de Talento Humano	Técnico I de Contabilidad	1
	T-106	Técnico I de Contabilidad	Técnico I de Talento Humano	1
Operativo	O-201	Gestor III en fortalecimiento y logística empresarial	Gestor III en fortalecimiento y logística empresarial	3
	O-202	Operador de Registro	Operador de Registro	3
	O-203	Operador de Archivo	Operador de Archivo	4
	O-204	Operador de Información	Operador de Información	4
	O-205	Gestor III de apoyo a proyectos de desarrollo empresarial	Gestor III de apoyo a proyectos de desarrollo empresarial	2
	O-101	Operario de Servicios Generales	Operario de Servicios Generales	2
TOTAL, CARGOS				**81**

Fase 2: Activación

En caso de presentarse una ausencia permanente o temporal en un cargo:

1) El profesional II de Talento Humano notificara al Presidente Ejecutivo sobre la ausencia temporal o permanente del cargo que se presentó.

2) El profesional II de Talento Humano se remitirá al cuadro anterior "**RELACIÓN DE PARES DE CARGOS"** para revisar cuál es el par e informar al Presidente Ejecutivo y dar continuidad al proceso y enviar la solicitud por el gestor documental DocXFlow del encargo a la Dirección de Asuntos Jurídicos.

3) El Director de Asuntos Jurídicos realiza la verificación en el DocXFlow y envía el proceso al Profesional II Apoyo Jurídico para realizar el respectivo documento, solicitando un numero de Decisión Ejecutiva al Técnico II de Presidencia para elaborar el documento, este documento es elaborado y revisado por el Director de Asuntos Jurídicos y Profesional II de Talento Humano una vez con vistos buenos se procede a pasar al Técnico II de Presidencia para firma del Presidente Ejecutivo.

4) Una vez firmado el documento el Técnico II de Presidencia notifica por correo a las personas involucradas como lo es: Profesional II de Talento Humano, Coordinar Financiero, Director que halla a lugar del encargo, Profesional I de presupuesto y contabilidad, Profesional I de Nomina e Inventarios y Profesional II de Tesorería.

5) El profesional II de Talento Humano notifica por escrito al colaborador del encargo que se realizó mediante Decisión Ejecutiva, documento que ira soportada con las funciones del cargo que realizara los documento reposaran en el expediente del colaborador.

6)El profesional II de Talento Humano realiza entrega de las novedades en FOR-TH-10 NOVEDADES DE NOMINA presentadas en la quincena del mes correspondiente al Profesional I de Nomina e Inventarios, adjuntando los soportes firmados para realizar los procesos pertinentes.

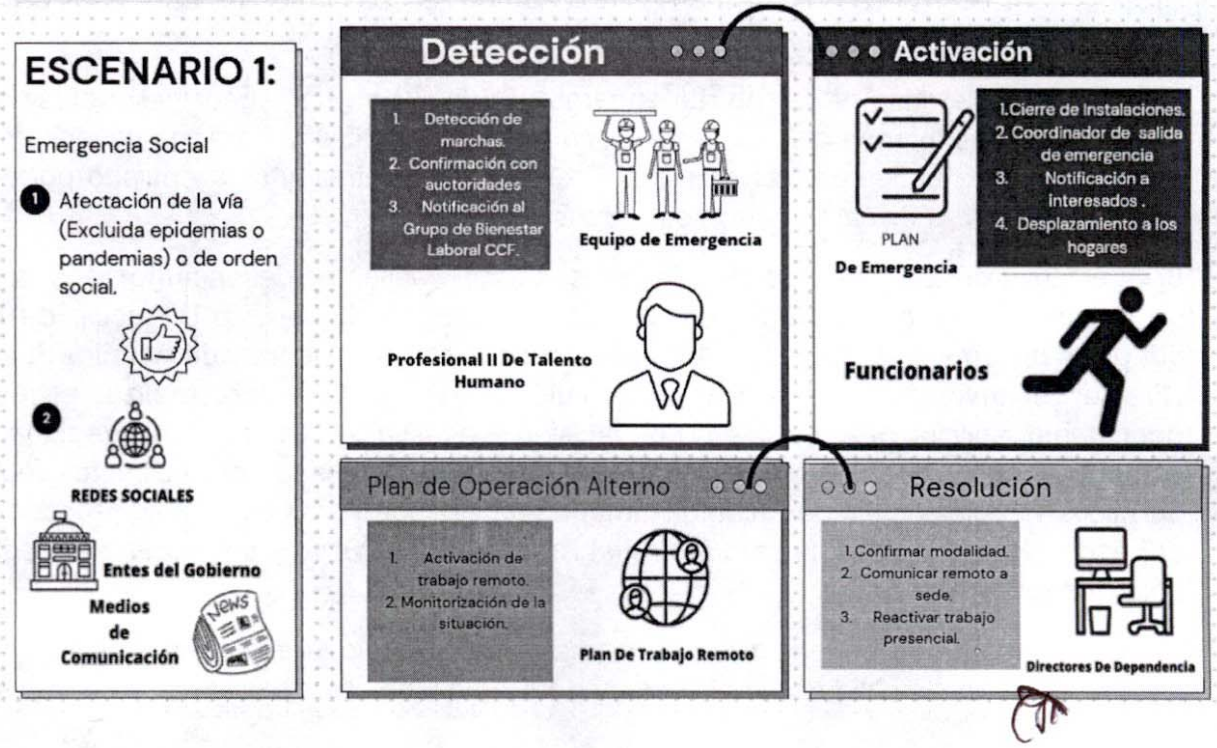
7) Cuando se termina el tiempo del encargo y el titular no ha llegado, el Profesional II de Talento Humano informa al Presidente Ejecutivo para autorizar la prórroga del encargo por le mismo tiempo o el tiempo que defina el Presidente Ejecutivo, y será enviado por el gestor documental DocXFlow al Director de Asuntos Jurídicos.

8) Si el titular del cargo llega antes de que se termine el tiempo del encargo, el Profesional II de Talento Humano envía por el gestor documental DocXFlow a la Dirección de Asuntos Jurídicos documento informado la terminación de encargo al Director de Asuntos Jurídicos el Director lo envía el proceso al Profesional II Apoyo Jurídico para realizar el respectivo documento, solicitando un numero de Decisión Ejecutiva al Técnico II de Presidencia para elaborar el documento, este documento es elaborado y revisado por el Director de Asuntos Jurídicos y Profesional II de Talento Humano una vez con vistos buenos se procede a pasar al Técnico II de Presidencia para firma del Presidente Ejecutivo y se procederá a notificar al colaborador.

9) Cuando los pares pertenecen a la misma línea jerárquica o misma denominación no se realizar encargo, es obligación del Director de Área o Líder de proceso distribuir las tareas en

el personal que está vinculado con la misma denominación para el cumplimiento de las labores.
Fase 3: Plan de operación alterno
1) **El Profesional II de Talento Humano**: Envía por correo electrónico documento firmado por el Presidente Ejecutivo a las personas interesadas informando el encargo que se presentó para realizar los cambios administrativos que allá a lugar. 2) El colaborador que fue asignado en el encargo se presenta al Director para dar cumplimiento a sus funciones.
Fase 4: Solución del incidente
1) **El Profesional II de Talento Humano y el Técnico I de Talento Humano,** realiza seguimiento en la planta para dar cumplimiento a los pares y la elaboración de las solicitud de las decisiones cuando se requiera para dar continuidad a la labor.

14. FICHAS DESCRIPTIVAS DE PROTOCOLO



Cámara de Comercio de Facatativá y del Noroccidente de Cundinamarca

PBX (601) 8902833
WhatsApp: 3106691309
correspondencia@ccfacatativa.org.co

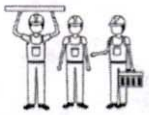
ESCENARIO 2:

Desastre natural y colapso de infraestructura.

1. Daño severo de nuestras instalaciones o el medio ambiente que impide laboral.

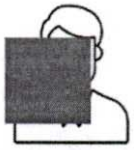
Detección

1. Detección del sismo.
2. Alertar de incendio.
3. Detección de inundación.
4. Identificación de fallas del edificio.



Equipo de Emergencia

Profesional I de SG-SST



Activación

PLAN
De Emergencia

1. Autorización evacuación.
2. Aplicar plan de evacuación.
3. Salvaguardar la vida del personal.
4. Coordinar acciones con las autoridades.

Funcionarios

Plan de Operación Alterno

1. Activación de trabajo remoto.
2. Evaluar daños en la edificación.
3. Aplicar plan de recuperación de desastres.

Plan De Trabajo Remoto

Resolución

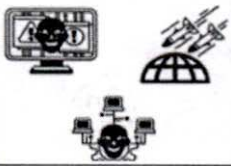
1. Reactivar trabajo presencial si fue suspendido.
2. Reiniciar los procesos de acuerdo con orden de prioridad.
3. Restablecer los datos en el sistema de información.

Directores De Dependencia

ESCENARIO 3:

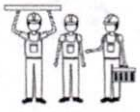
Desastre Tecnologico

1. Daño severo en la infraestructura de los servicios TIC o ataques informáticos como secuestros de datos.



Detección

1. Fallas de comunicaciones.
2. Fallas del sistema.
3. Ataques informáticos.
4. Fallas de equipo de computo.
5. Fuego o inundación en centros de datos.



Equipo de Emergencia

Coordinador de transformación digital y formación empresarial

Activación

PLAN
De Emergencia

1. Negociaciones.
2. Verificación de prioridad de proyectos.
3. Ajustes presupuestales.

Autoridades MITIC Mindefensa

Plan de Operación Alterno

1. Activación de trabajo remoto.
2. Activar el plan de recuperación ante ataques.
3. Mantener informadas a las partes interesadas.

Resolución

1. Reactivar trabajo presencial si fue suspendido.
2. Reiniciar los procesos de acuerdo con orden de prioridad.
3. Restablecer los datos en el sistema de información.

Cámara de Comercio de Facatativá y del Noroccidente de Cundinamarca

PBX (601) 8902833

WhatsApp: 3106691309

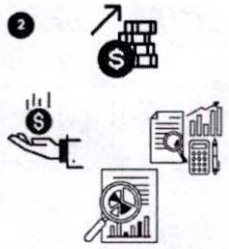
correspondencia@ccfacatativa.org.co

ESCENARIO 4:

Crisis Financiera

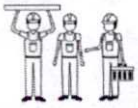
1. Imposibilidad de contar con los recursos económicos para cumplir con los compromisos misionales o con terceros proveedores de servicios.

2.



Detección

1. Marco del gasto. Presupuesto.
2. Disponibilidad de recursos.
3. Compromisos con el plan presupuestal.



Equipo de Emergencia

Director (ar) Administrativo (a) y Financiero (a).

Activación

PLAN

De Emergencia

1. Negociaciones.
2. Verificación de prioridad de proyectos.
3. Ajustes presupuestales.

Equipo Financiero

Plan de Operación Alterno

1. Negociaciones con entidades pertinentes.
2. Prioridad de proyectos de inversión.
3. Búsqueda de recursos.

Resolución

1. Ejecución de los proyectos de acuerdo a los ajustes.
2. Reporte de incumplimiento.
3. Seguimiento institucional.

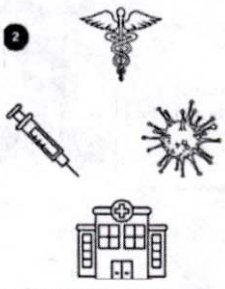
Directores De Dependencia

ESCENARIO 5:

Emergencia Sanitaria

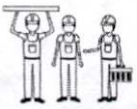
1. Pandemias, epidemias, crisis sanitarias que impiden el funcionamiento de los procesos institucionales.

2.



Detección

1. Declaración oficial de emergencia sanitaria, epidemia o pandemia.



Equipo de Emergencia

Profesional II de talento humano

Activación

PLAN

Protocolo de Bioseguridad

1. Aplicación de protocolo definido por los organismos de salud
2. Aplicación de medios de aislamiento o tratamiento.
3. Preparación para la activación de trabajo remoto.

Funcionarios

Plan de Operación Alterno

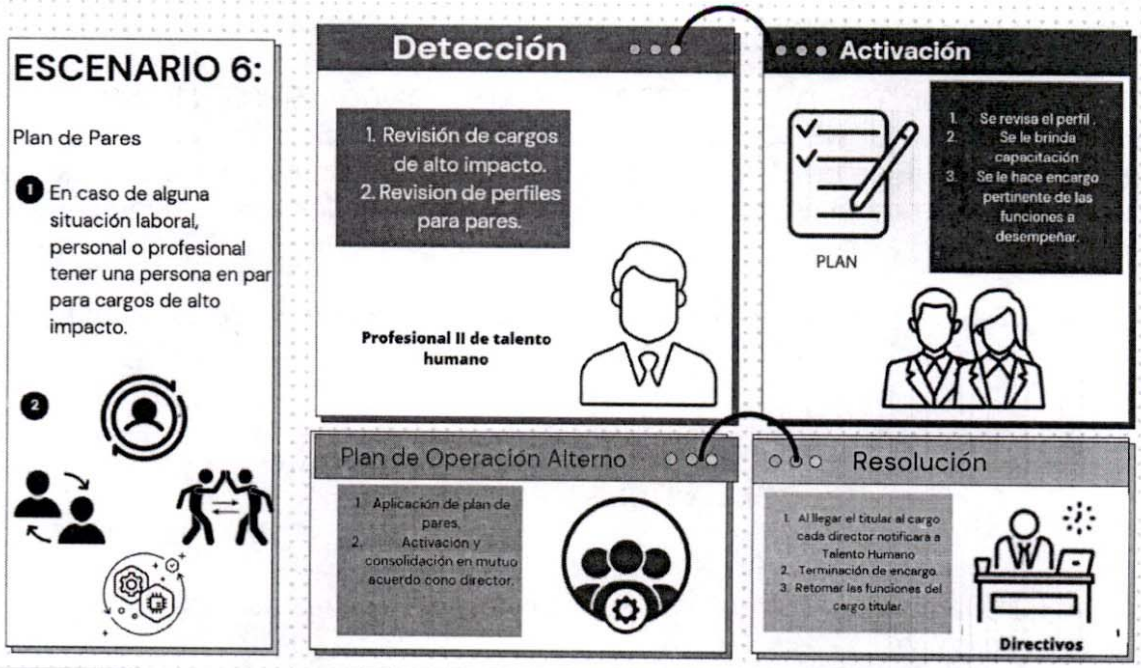
1. Aplicación de los planes de operación.
2. Activación de trabajo remoto.
3. Activación de medidas de seguimiento al personal.
4. Publicación pertinente de información sobre evolución de la situación.

Trabajo Remoto

Resolución

1. Aplicación de protocolo de retorno a normalidad.
2. Seguimiento a condiciones de salud.
3. Finalización de planes de trabajo remoto.

Directivos



15. ANEXOS

Acta N° 1 Revisión y creación del Plan de continuidad del negocio.
Acta N° 2 Socialización y revisión del Plan de continuidad del negocio.

16. DOCUMENTOS RELACIONADOS Y FORMATOS

MAN-TI-01-MANUAL DE SEGURIDAD DE LA INFORMACIÓN
FOR-PRE-08 – ACTA DE REUNIÓN.
FOR-DAF-52 SALIDA DE ACTIVOS.
FOR-TH- 24 SEGUIMIENTO TRABAJO EN CASA

Parágrafo 1°. Integrantes del Comité de Continuidad del Negocio: Estará a cargo por los integrantes de la Brigada de Emergencia de la Cámara de Comercio de Facatativá y su ejecución se realizará acorde con los Escenarios de Emergencia con sus respectivos líderes, contemplados en el literal 13 del documento técnico. La designación del secretario del Comité, estará a cargo del Profesional I del Sistema de Gestión de Seguridad y Salud en el Trabajo SS-SGT.

Parágrafo 2°. Reuniones del Comité: El presente comité se reunirá dos veces en cada anualidad, una vez por semestre, con el fin de revisar y evaluar los riesgos existentes y posibles que se puedan presentar y que afecten su continuidad.

Parágrafo 3°. Hace parte integral de la presente decisión ejecutiva el documento técnico PLAN DE CONTINUIDAD DEL NEGOCIO.

ARTÍCULO QUINTO: IMPLEMENTACIÓN DEL DOCUMENTO TECNICO DE CONTINUIDAD DEL NEGOCIO. La Brigada de Emergencia será la dependencia responsable del Plan de Continuidad del Negocio de la Cámara de Comercio de Facatativá y liderará el proceso buscando el bienestar de los colaboradores y sus familias.

ARTÍCULO SEXTO: La presente decisión rige a partir de la fecha de su aprobación.

COMUNIQUESE Y CUMPLASE

Dada en la Cámara de Comercio de Facatativá, a los 17 días del mes de junio del dos mil veinticinco.

GRATINIANO SUÁREZ SUÁREZ
Presidente Ejecutivo

CONTROL DE LEGALIDAD: **DANIEL FRANCISCO BERNAL RODRIGUEZ / DAJ**
LUIS FERNANDO ARGUMERO SANTIBAÑEZ / PIIAJ
JULIAN ANDRES SEGURA LEON / PII-TH