ÍNDICE

4.1.3. Los riesgos tecnológicos con impacto sanitario (v.gr. los vertidos, la contaminación, los accidentes industriales, etc.)

4.2. EL IMPACTO ORGANIZATIVO Y DE CUMPLIMIENTO

4.2.1. El Impacto en la salud y a la seguridad de los trabajadores

4.2.2. Alteraciones en la cadena de suministro y en la prestación de servicios

4.2.3. Riesgos laborales, de protección de datos, contractuales y regulatorios

4.3. LAS MEDIDAS DE PREVENCIÓN Y PREPARACIÓN

4.3.1. Protocolos sanitarios internos y planes de contingencia

4.3.2. El teletrabajo, el trabajo híbrido, y la reorganización de turnos

4.3.3. Coordinación con autoridades sanitarias y de protección civil

4.4. LA RESPUESTA DURANTE LA CRISIS

4.4.1. La activación del Comité de Crisis y de los planes internos

4.4.2. La comunicación con empleados, clientes y proveedores

4.4.3. Las medidas temporales extraordinarias (cierres, ERTE, cambios operativos)

4.5. RECUPERACIÓN Y APRENDIZAJE

4.5.1. Vuelta a la normalidad y normalidad “redefinida”

4.5.2. Revisión de políticas y protocolos a la luz de la experiencia

4.5.3. Incorporación de la experiencia de crisis al mapa de riesgos y al BCP

CAPÍTULO 5 - LOS CIBERATAQUES Y LOS RANSOMWARES

5.1. TIPOLOGÍA DE INCIDENTES DE SEGURIDAD

5.1.1. Ransomware y cifrado de sistemas

5.1.2. Brechas de datos personales y fugas de información confidencial

5.1.3. Ataques de denegación de servicio, phishing y suplantación de identidad

5.2. IMPACTOS CRÍTICOS PARA LA ORGANIZACIÓN

5.2.1. Paralización operativa y pérdida de continuidad de negocio

5.2.2. Los daños reputacionales y la pérdida de confianza

5.2.3. Responsabilidades legales, regulatorias y sancionadoras

5.3. LA PREVENCIÓN Y LA CIBERRESILIENCIA

5.3.1. Medidas técnicas: seguridad perimetral, backups, segmentación, etc.

5.3.2. Medidas organizativas: políticas de seguridad, clasificación de la información

5.3.3. Formación y concienciación del personal frente al phishing y el error humano

5.4. GESTIÓN DE INCIDENTES Y RESPUESTA A CIBERATAQUES

5.4.1. Plan de respuesta a incidentes (IRP) y coordinación con BCP y DRP

5.4.2. Detección, contención, erradicación y recuperación

7.2.2. Los stakeholders críticos en cada tipo de crisis (v.gr. sanitaria, ciber, reputacional)

7.3. LAS ESTRATEGIAS DE RELACIÓN EN FASE DE CRISIS

7.3.1. La información, la consulta, la participación y la creación de soluciones

7.3.2. La gestión de conflictos de intereses entre stakeholders

7.3.3. La negociación y los acuerdos de salida o de compensación

7.4. CONSTRUCCIÓN DE CONFIANZA Y CAPITAL RELACIONAL

7.4.1. Transparencia previa como amortiguador de la crisis

7.4.2. Alianzas estratégicas y redes colaborativas

7.4.3. Integración de la gestión de stakeholders en la estrategia ESG y de Compliance

CAPÍTULO 8 - LOS PLANES DE CONTINUIDAD DE NEGOCIO (BCP)

8.1. CONCEPTOS BÁSICOS DE CONTINUIDAD DE NEGOCIO

8.1.1. Diferencia entre BCP, DRP y plan de emergencia

8.1.2. Objetivos: mantener funciones críticas, reducir tiempo de interrupción y pérdidas

8.2. METODOLOGÍA DE ELABORACIÓN DE UN BCP

8.2.1. Business Impact Analysis (BIA): identificación de procesos críticos

8.2.2. La definición de RTO, RPO y niveles de servicio mínimos aceptables

8.2.3. Identificación de recursos esenciales: personas, tecnología, instalaciones, proveedores

8.3. DISEÑO DE ESTRATEGIAS DE CONTINUIDAD

8.3.1. Las redundancias y las alternativas operativas

8.3.2. Acuerdos con terceros, externalización y centros alternativos

8.3.3. Estrategias de continuidad para pandemias, ciberataques y crisis reputacionales

8.4. IMPLEMENTACIÓN, PRUEBAS Y MANTENIMIENTO DEL BCP

8.4.1. Planes específicos por escenario y por área

8.4.2. Simulacros, ejercicios y lecciones aprendidas

8.4.3. Actualización periódica y alineamiento con cambios en el negocio

8.5. VINCULACIÓN DEL BCP CON EL SISTEMA DE COMPLIANCE

8.5.1. Obligaciones legales y regulatorias relacionadas con la continuidad

8.5.2. Evidencias documentales, auditorías y seguimiento

8.5.3. Integración en el mapa de riesgos y en el plan de Compliance

CAPÍTULO 9 - LA CULTURA DE LA RESILIENCIA Y EL APRENDIZAJE POST-CRISIS

9.1. DE LA “CULPA” A LA CULTURA DE APRENDIZAJE Y MEJORA CONTINUA

9.2. EVALUACIONES POST-MORTEM Y COMITÉS DE REVISIÓN DE CRISIS

9.3. LOS AJUSTES DE POLÍTICAS, DE PROCEDIMIENTOS Y DE ESTRUCTURAS ORGANIZATIVAS

9.4. FORMACIÓN ESPECÍFICA BASADA EN CASOS REALES VIVIDOS POR LA ORGANIZACIÓN

9.5. LA INCORPORACIÓN DE LA RESILIENCIA COMO VALOR Y COMO COMPETENCIA CLAVE

CAPÍTULO 10 - LA MEDICIÓN, LOS INDICADORES Y EL REPORTING EN LA GESTIÓN DE CRISIS Y LA RESILIENCIA

10.1. LOS INDICADORES DE PREPARACIÓN (V.GR. PLANES, SIMULACROS, FORMACIÓN, COBERTURA DE BCP)

10.2. INDICADORES DE IMPACTO EN CRISIS (V.GR. TIEMPOS DE RESPUESTA, TIEMPOS DE RECUPERACIÓN, PÉRDIDAS)

10.3. LOS INDICADORES DE RESILIENCIA (V.GR. CAPACIDAD DE RECUPERACIÓN, ADAPTACIÓN, MEJORA)

10.4. EL REPORTING INTERNO A LA ALTA DIRECCIÓN Y AL CONSEJO

10.5. EL REPORTING EXTERNO EN INFORMES DE SOSTENIBILIDAD, ESG Y MEMORIAS DE GESTIÓN

CAPÍTULO 11 - EL ROADMAP PARA IMPLANTAR O MADURAR EL SISTEMA DE GESTIÓN DE CRISIS Y RESILIENCIA

11.1. DIAGNÓSTICO INICIAL DE MADUREZ (GAP ANÁLISIS)

11.2. LA DEFINICIÓN DE LOS OBJETIVOS Y LAS PRIORIDADES ESTRATÉGICAS

11.3. EL PLAN DE ACCIÓN: LAS POLÍTICAS, LAS ESTRUCTURAS, LOS RECURSOS, Y LA FORMACIÓN

11.4. EL CRONOGRAMA, LAS RESPONSABILIDADES Y EL PRESUPUESTO

11.5. LA REVISIÓN PERIÓDICA Y MEJORA CONTINUA

CAPÍTULO 12 - ALGUNAS CONCLUSIONES

12.1. LA GESTIÓN DE CRISIS COMO PARTE ESENCIAL DEL BUEN GOBIERNO Y DEL COMPLIANCE

12.2. LA RESILIENCIA CORPORATIVA COMO VENTAJA COMPETITIVA SOSTENIBLE

12.3. LAS LECCIONES CLAVE DE PANDEMIAS, CIBERATAQUES Y CRISIS REPUTACIONALES

12.4. LOS DESAFÍOS FUTUROS: LA COMPLEJIDAD, LA INTERDEPENDENCIA, Y LOS RIESGOS SISTÉMICOS