

Chief Security Office

Protegiendo nuestra resiliencia con la continuidad de negocio

FAQ Preguntas Frecuentes



www.colt.net

Introducción:

Este documento ha sido creado para dar una visión general de la resiliencia empresarial en Colt.

¿Certificación?

El programa de resiliencia empresarial de Colt, está alineado a la normativa ISO 22301 de Gestión de Continuidad de Negocio. Colt tiene ésta certificación en las localidades donde se encuentran las actividades de operaciones y soporte al cliente.

Además, Colt tiene la certificación ISO 27001.

Alcance:

El programa de resiliencia empresarial de Colt está integrado en el área de Seguridad, Chief Security Office (CSO), relativas a todas las funciones, personas y localidades.

En Colt nos comprometemos a minimizar el riesgo de interrupción del negocio implementando los controles apropiados y manteniendo nuestros programas claves (descritos más abajo) con el fin de responder a interrupciones inesperadas y reanudar los procesos críticos al negocio en tiempos aceptable y niveles de servicio acordados:

- **Resiliencia del negocio** – se refiere a la gestión del riesgo y a la continuidad de los equipos de operaciones ya sea antes, durante o después de una interrupción.
- **Resiliencia de tecnología** – se refiere a la gestión de riesgo y a la continuidad de plataformas de IT, sistemas y redes, ya sea antes, durante o después de una interrupción.
- **Resiliencia de terceros** – se refiere a la gestión de riesgo y a la continuidad de los proveedores de Colt, sus socios o cualquier tercera parte interesada.
- **Gestión de crisis** – se refiere a las activaciones, proceso para la gestión de un evento cuyo impacto sea potencialmente importante.

¿Pueden describir la estructura del programa de gestión establecido?

La responsabilidad final de la gestión de riesgo recae sobre el director general. La responsabilidad de la gestión de riesgo, incluyendo los riesgos sobre la continuidad de negocio, recae sobre los responsables de operaciones de cada área de negocio. El Chief Security Officer (CSO) / director de seguridad de Colt, proporciona liderazgo estratégico al Director de resiliencia de negocio y seguridad física, que es el responsable de mantener y entregar el programa a nivel global. El programa ofrece consistencia a través de cada función, definiendo los requerimientos y supervisando el desarrollo, la implementación, el ejercicio y el mantenimiento del plan.

Los directivos son responsables de asegurarse de que los procesos críticos de sus áreas sean resilientes ante interrupciones y de que tengan los planes adecuados establecidos para minimizar el impacto de las interrupciones.

¿Cómo nos aseguramos de que los planes están actualizados?

El marco del programa requiere que toda documentación sobre resiliencia de las funciones críticas al negocio se revise al menos una vez al año, o después de un cambio significativo en el equipo o en las operaciones. En general, está establecido un ciclo de mantenimiento (PLAN-DO-CHECK-ACT), planear, hacer, chequear y actuar, para todos los procesos que den soporte a los productos y servicios claves de Colt. Debido al ritmo rápido del entorno en el que operamos, la evaluación de los procesos y la mejora de los planes puede ser un proceso continuo.

¿Pueden compartir sus documentos sobre resiliencia?

Estos documentos constan de propiedad intelectual corporativa y siguiendo la normativa ISO 27001, los documentos confidenciales como las estrategias de continuidad de negocio y sus planes, no pueden ser compartidos externamente.

Sin embargo, estaremos encantados de compartir información no-confidencial cuando sea necesario. Además, si desea ver información más detallada y controlada, podemos organizar una demostración remota o una visita a sus instalaciones.

¿Pueden detallar parte del contenido de sus planes de resiliencia?

Los planes incluyen los mecanismos necesarios para una respuesta a tiempo y efectiva que aseguraría el restablecimiento de los procesos acorde con las expectativas del negocio. Definen claramente: “los roles y responsabilidades del equipo, los clientes y proveedores, así como de los procesos de principio a fin, las actividades y tecnologías críticas, las dependencias de terceros. También incluyen las metodologías de mando, control y comunicación y los planes de mantenimiento.

¿El rol del cliente?

A petición de nuestros clientes, en ocasiones hemos creado ejercicios y planes de continuidad conjuntos. Los roles y las responsabilidades están claramente definidos.

¿Se ha realizado alguna evaluación formal de riesgo para identificar las hipótesis de interrupciones?

Si. Estos análisis de riesgos aseguran que todas las amenazas a los procesos críticos de la organización estén evaluadas (impacto y probabilidad) y que los riesgos de niveles excesivos estén mitigados y reducidos a niveles aceptables por dirección. Los planes de reducción de riesgos cubren los equipos técnicos donde las aptitudes son críticas para los Clientes de Colt para asegurar la continuidad del servicio.

¿Qué planes tiene Colt en caso de pandemia?

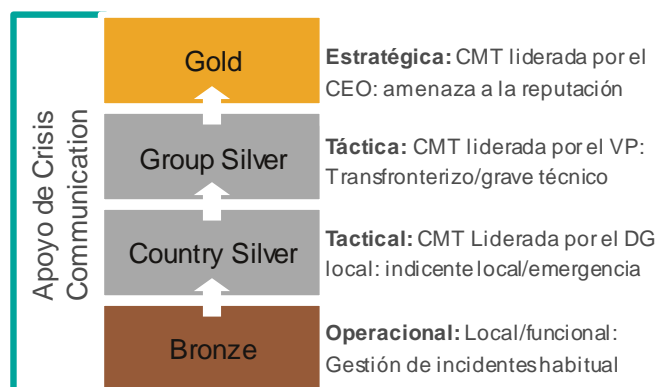
Colt sigue las 6 fases de la OMS (Organización Mundial de la Salud) y la utiliza para implementar medidas preventivas y de recuperación en caso de pandemia.

Se revisan anualmente la flexibilidad operativa de los recursos de Colt y las “familias” de puestos de trabajo con aptitudes similares, esto permite disponer de soporte/recursos adicionales en caso de ausentismo. Nuestros planes incluyen respuestas remotas y automáticas. Ya que una pandemia es un incidente relacionado con las personas podríamos al igual que nuestros clients, padecer una pérdida de empleados, por lo tanto, en el peor de los casos, nos centraríamos en las operaciones que dan soporte a los servicios esenciales y a las organizaciones críticas a nivel nacional.

¿Cuáles son los mecanismos de respuesta de Colt en caso de crisis?

Cuando un corte no planificado va más allá de lo habitual, nuestro programa de resiliencia está diseñado para soportar los diferentes niveles de gestión de corte/crisis (ver diagrama más abajo) y para instruir y coordinar todos los recursos críticos que soportan nuestra actividad principal.

Además, el programa tiene la autoridad para instruir a la línea de gestión Bronce con el fin de estar preparados para ejecutar dichos planes si la invocación de cualquier plan de resiliencia fuese necesaria.



¿Cuándo se convierte un corte en crisis y requiere la invocación del plan?

El programa de resiliencia de Colt, está alineado con los SLAs y los contratos de clientes. La gestión de crisis empieza cuando nuestros controles de resiliencia de infraestructura fallan, o cuando eventos externos a Colt impactan nuestras operaciones. Esto incluye por ejemplo huelgas, pandemia, desastres naturales, terrorismo, incendio o inundaciones.

¿Cómo se asegura Colt de que se mantienen informados a los clientes?

En caso de corte de gran escala o perturbación de la actividad habitual, que pueda ocasionar una perturbación seria para algunos o todos nuestros clientes, tenemos procesos para comunicar rápidamente para proporcionar rápidamente información a los contactos relevantes. El primer punto de contacto para los clientes es el service desk a través del cual los clientes que experimenten cortes reciben actualizaciones periódicas gracias al proceso de registro de tickets. Los esfuerzos se centran en la resolución del incidente y las actualizaciones se comparten prioritariamente a través del mecanismo de tickets. Todas las comunicaciones iniciales se hacen en inglés con soporte en idioma local cuando sea posible.

¿Cómo podemos asegurar que los servicios provistos por Colt son completamente resilientes?

Los clientes que requieran mayor nivel de resiliencia además de sus soluciones estándar pueden comentarlo con su responsable de ventas o gestor de cuenta.

¿Cómo se asegura Colt de que los planes son adecuados?

Los planes existentes requieren ser testeados y ejercitados regularmente para ser efectivos. También se revisa regularmente para asegurar su mantenimiento y relevancia. Colt tiene un calendario de test con ejercicios que van desde simulaciones a fallos técnicos. La frecuencia de estas actividades depende de la naturaleza y criticidad de la función, el equipo o proceso en cuestión.

¿Comparten los resultados de los tests públicamente? Cuáles son los pasos para abordar las posibles lagunas y las lecciones aprendidas?

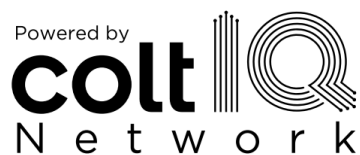
Cuando el contrato de nuestros clientes requiere un test conjunto, compartimos los resultados con el cliente. Después de cada test, documentamos los resultados. Cualquier acción requerida es monitorizada y se hace el seguimiento desde central hasta su resolución.

¿Qué áreas de su cadena de suministro consideran en sus programas de resiliencia?

Cuando procedemos al análisis de riesgo, consideramos todas las áreas de la cadena de suministro y el rol que desempeñan nuestros proveedores para evitar puntos únicos de fallo (SPOF). Para ello, revisamos sus planes de continuidad. Completamos test y ejercicios conjuntos con proveedores críticos seleccionados.

¿Qué formación le dais a los empleados sobre la resiliencia del negocio?

Todos los empleados de Colt reciben información y una presentación de introducción y completan una formación obligatoria en la plataforma de formación electrónica. Además, las partes interesadas claves (que aparecen en nuestra documentación), reciben training y participan a test y ejercicios para familiarizarse con los planes, procesos y procedimientos.



For more information
visit www.colt.net

Tel: +44 (0)20 7863 5510

E-mail: sales@colt.net

Acerca de Colt

Colt es el Nuevo estándar en redes de alto ancho de banda y servicios de voz para empresas en Europa, Asia y en los mayores centros de negocios de América del Norte. Con un alcance global y una fuerte presencia local, Colt es lo suficientemente grande como para entregar y lo suficientemente pequeña para importarle.

Conecta a más de 850 data centers a nivel global, con más de 27500 edificios en red y creciendo. Colt también está reconocida como una empresa innovadora y pionera en redes definidas por software (SDN) y virtualización de las funciones de red (NFV).

