

Fecha de creación: 12/10/2023 8:50 p.m. Última actualización: 12/10/2023 8:50 p.m.

ANEXO DE REQUERIMIENTOS DE CIBERSEGURIDAD

Contrato

CON-10162

Continuidad del negocio y recuperación ante desastres

- RTC09:** Todo Tercero que esté relacionado con los procesos y activos críticos para el negocio de la organización debe: 1. Contar con una estrategia de continuidad para los servicios críticos prestados a Ecopetrol que incluya requisitos de seguridad 2. Contar con planes de continuidad para asegurar la disponibilidad del servicio ante situaciones adversas que puedan comprometer la prestación del servicio contratado. Los planes de continuidad, contingencia y recuperación de desastres deben ser revisados y probados al menos una vez al año durante la vigencia del contrato pactado entre las partes. De igual forma, los planes de recuperación deben estar acordes a los acuerdos a los niveles de servicios acordado entre las partes.
- RTC10:** Mantener un plan de recuperación de desastres documentado para cada sistema crítico relacionado con Ecopetrol y para las aplicaciones de negocio, probarlo anualmente como mínimo, notificar a Ecopetrol cuando se realice y compartir los informes de resultado de la prueba.
- RTC11:** Implementar medidas de respaldo adecuadas, incluido el almacenamiento de los archivos de datos de respaldo en lugares seguros fuera del sitio de procesamiento, para permitir la recuperación eficiente del sistema
- RTC12:** Contar con un esquema de copias de respaldo de la información, software, imágenes de los sistemas y medios de almacenamiento, el cual debe ser probado periódicamente, para garantizar la disponibilidad de la información.

Gestión de Vulnerabilidades

- RTC24:** El Tercero debe permitir que Ecopetrol realice monitoreo de sus dominios públicos y debe garantizar la gestión y resolución a inmediato o corto plazo de las vulnerabilidades detectadas que puedan afectar de manera alguna el servicio contratado por Ecopetrol.
- RTC25:** Aplicar políticas y procedimientos de gestión de parches y actualizaciones para todos los sistemas operativos y software autorizados

Gobierno

- RTC28:** Cumplir con las regulaciones locales e internacionales de Privacidad, Seguridad de la información y Ciberseguridad. Contar con políticas, normas y estándares de Seguridad de la información y ciberseguridad al interior de su organización, las cuales deben desarrollarse y mantenerse actualizadas acorde con los riesgos a los que se ve enfrentada su organización.
- RTC29:** Permitir que Ecopetrol realice evaluaciones y revisiones periódicas de riesgos y cumplimiento de controles de seguridad establecidos en el contrato.
- RTC30:** Mantener y documentar la gestión de auditorías, evaluaciones, verificaciones y planes de mejora que se realicen sobre seguridad de la información y ciberseguridad

Seguridad de la red

- RTC35:** Instalar, configurar y activar un sistema integral de protección contra intrusiones (en la red y el host), de conformidad con las mejores prácticas de la industria, para que en forma continua evite, detecte e informe la ocurrencia de ataques no autorizados a la red y en contra de sus sistemas, incluidos, entre otros, intentos de penetración, ataques por denegación de servicio y sondeos excesivos
- RTC36:** Instalar cortafuegos (firewall) para redes basados en las mejores prácticas de la industria entre los servidores y las puertas de enlace (gateways) a la red pública de modo que excluyan los protocolos de comunicación que no sean necesarios para procesar el tráfico de Internet
- RTC37:** Registrar toda la actividad de los cortafuegos y puertas de enlace y almacenar los datos de dicha actividad de una manera apropiada y en un periodo establecido
- RTC40:** Restringir, por tecnologías de filtrado, el acceso a internet con el fin de bloquear sitios web maliciosos y sospechosos, servicios de correo electrónico personal y no empresarial, servicios de nube públicos personales y no aprobados por la organización
- RTC41:** Utilizar un cifrado fuerte para la autenticación y la transmisión, como WPA2 o WAP2 Enterprise, en las redes inalámbricas que acceden a los sistemas de información
- RTC43:** Asegurar que únicamente estén habilitados los puertos de red, protocolos y servicios requeridos por cada sistema.
- RTC44:** Establecer prácticas de conexión segura a la red y segmentación de su red basado en niveles de seguridad
- RTC45:** Contar con logs de acceso a los sistemas y realizar el respectivo análisis periódicamente.

Respuesta y gestión ante Incidentes

- RTC58:** Tener definido, documentado e implementado un proceso o procedimiento de gestión de incidentes de seguridad de la información, que abarque aspectos como: los roles y responsabilidades, el reporte, la evaluación, la respuesta y las lecciones aprendidas de los incidentes de seguridad de la información de la organización
- RTC59:** Contar con una gestión para la atención y respuestas de incidentes que ocurriesen en su infraestructura tecnológica y que este afecte los niveles de servicios que se pactaron entre las partes. Al presentarse un incidente y que este haya afectado el servicio contratado, el Tercero debe priorizar la atención y resolución de manera oportuna para no afectar los acuerdos de niveles de servicio definidos. Así mismo, el Tercero debe entregar en los tiempos acordados entre las partes, el informe detallado del incidente y que acciones se tomaron para que este no se vuelva a presentar.
- RTC60:** Notificar a Ecopetrol los incidentes de seguridad de la información y ciberseguridad al profesional de gestión contractual y vía correo electrónico a ciberseguridadproveedores@ecopetrol.com.co

Transferencia de información

- RTC64:** Implementar controles y procedimientos para garantizar el borrado seguro de la información de Ecopetrol a la que tenga acceso, en tanto esta ya no sea requerida para el producto o servicio prestado
- RTC67:** Implementar políticas y medidas de seguridad en su organización para proteger la información a la que se tiene acceso desde la modalidad de

trabajo remoto

Seguridad en el recurso Humano

- RTC68:** Certificar que todos los empleados del Tercero que tengan acceso a la información de Ecopetrol firman acuerdos de confidencialidad o de no divulgación de información y establecer o incluir claramente en los acuerdos contractuales con empleados y subcontratistas sus responsabilidades en cuanto a la seguridad de la información
- RTC69:** Velar por que todos sus empleados den cumplimiento a los acuerdos de confidencialidad establecidos con la organización, con motivo de la prestación del servicio, con el fin de proteger la información de la organización a la cual tiene acceso.
- RTC70:** Certificar que todos los dispositivos utilizados por los empleados del Tercero que tengan acceso a los sistemas de información de Ecopetrol cumplan y sigan cumpliendo los siguientes requisitos: 1. Deben aplicarse y estar al día los paquetes de actualizaciones (service pack) más recientes y todos los parches de seguridad aplicables a todos los sistemas operativos y software residentes en los dispositivos, 2. Los dispositivos deben tener el software estándar de la industria contra programas maliciosos (malware) instalado, funcionando y actualizado con el último archivo de firma, 3. El dispositivo debe tener instalado y activo un producto de seguridad tipo cortafuego (firewall) personal y estándar de la industria.
- RTC71:** Certificar que sus empleados reciban información profesional y capacitación de sensibilización sobre ciberseguridad al momento de la contratación y posteriormente de forma periódica.
- RTC72:** Certificar la ejecución de verificación de antecedentes de los empleados de su organización, que tendrán acceso a información de Ecopetrol

Seguridad de los servidores

- RTC76:** Reforzar la seguridad de todos los servidores utilizados para procesar, almacenar o transmitir datos e información de Ecopetrol, debiendo dicho reforzamiento incluir, entre otros, la eliminación de todos los privilegios y servicios salvo aquellos que sean esenciales para la ejecución de las operaciones para las que están instalados dichos servidores
- RTC77:** Implementar herramientas de análisis de la seguridad de los servidores para informar periódicamente sobre el estado de cada servidor y verificar que todas las configuraciones, parámetros y opciones estén conformes con el estado de reforzamiento acordado para ese dispositivo y para detectar cambios no autorizados a partir de la línea base de la configuración aprobada del servidor
- RTC78:** Registrar toda la actividad de acceso del servidor y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de sesenta días (60) días
- RTC79:** Revisar periódicamente (al menos una vez al año) todos los controles de seguridad de los servidores definidos anteriormente para asegurarse de que todavía estén vigentes.

Seguridad de los archivos de datos y bases de datos

- RTC80:** Almacenar la información "Clasificada" y "Reservada" de Ecopetrol en un formato cifrado de conformidad con las mejores prácticas de la industria

Protección contra programas maliciosos (Malware)

- RTC88:** Instalar, configurar, activar y mantener actualizado un software antimalware y antivirus basado en las mejores prácticas de la industria, en todos los servidores, dispositivos, computadoras portátiles y estaciones de trabajo que procesen o almacenen las transacciones y cualquier otro dato de Ecopetrol
- RTC89:** Configurar dicho software anti-malware para invocarlo automáticamente en el arranque y ejecutarlo interactivamente de forma continua, en todos los dispositivos donde esté instalado.
- RTC90:** Tener implementados controles de detección, prevención y recuperación para proteger los sistemas contra códigos maliciosos o cualquier tipo de ciberataque
- RTC91:** Implementar y mantener un software que detecte, prevenga, elimine y corrija códigos maliciosos en la infraestructura tecnológica que soporta los servicios contratados por Ecopetrol
- RTC92:** Presentar reportes sobre incidentes relacionados con programas maliciosos (específicos de Ecopetrol y que presentan la posibilidad de afectar de manera crítica sus sistemas) a Ecopetrol dentro de un plazo no mayor a 24 horas, tras la confirmación del Tercero de que el incidente es específico de Ecopetrol y tiene la posibilidad de afectar de manera crítica sus sistemas.