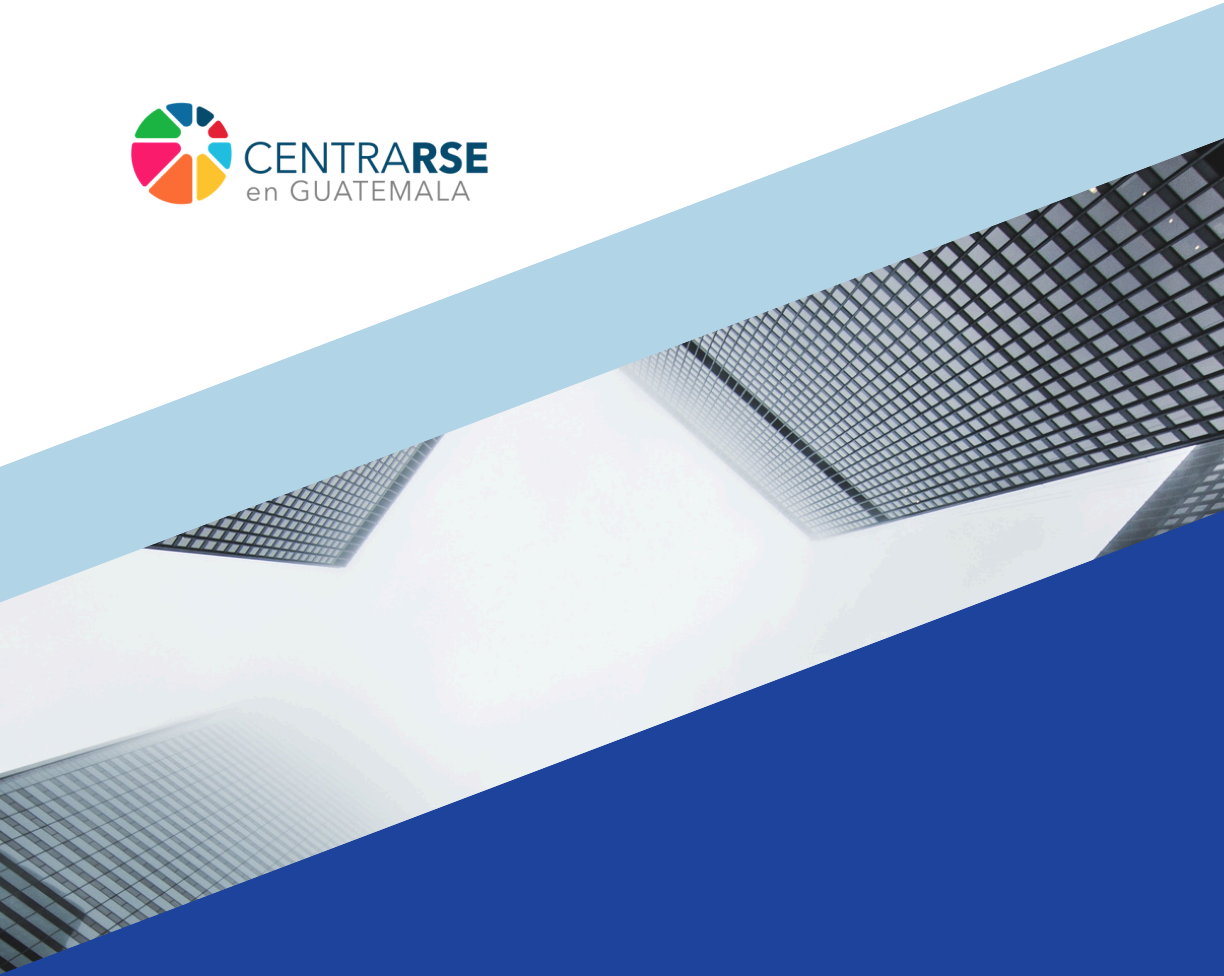
CENTRARSE en GUATEMALA



POLITICAS

Cyberseguridad Mantenimiento y Uso de Equipos

2026

CENTRARSE.ORG

Contenido

Introducción

En el actual ecosistema digital, la ciberseguridad ha dejado de ser una opción técnica para convertirse en un pilar estratégico de la gobernanza y sostenibilidad de CentraRSE. El presente manual responde a la necesidad imperativa de proteger la integridad de nuestra infraestructura, la confidencialidad de nuestros socios y la continuidad de nuestras operaciones frente a amenazas globales como el ransomware y la suplantación de identidad.

A través de este compendio de políticas, la organización adopta un modelo de "Confianza Cero" y modernización tecnológica, donde la responsabilidad individual de cada colaborador, el uso de herramientas licenciadas y el respaldo sistemático de la información constituyen nuestra primera y más sólida línea de defensa para garantizar un entorno de trabajo seguro, eficiente y vanguardista.

Objetivos de la Política

Protección Estratégica de Activos

Garantizar la confidencialidad y disponibilidad de la información mediante controles de acceso estrictos, uso de software con licencia y backups sistemáticos de servidores. El fin es blindar la infraestructura de CentraRSE contra ciberataques y asegurar la continuidad total de nuestras operaciones diarias.

Cultura de Responsabilidad Digital

Capacitar al personal para identificar y reportar amenazas críticas como el phishing y el ransomware. Se busca reducir errores humanos mediante el uso responsable de herramientas digitales, transformando a cada colaborador en una defensa activa y consciente para proteger los datos de la organización.

Sección I

Gestión de Identidades y Acceso Seguro

Sección I: Gestión de Identidades y Acceso Seguro

Esta sección establece los controles mandatorios para la protección de credenciales y sistemas de CentraRSE, bajo los marcos internacionales NIST CSF 2.0 e ISO/IEC 27001:2022.

1.1 Estándares de Robustez para Contraseñas

Define los requisitos de construcción y ciclo de vida de las credenciales de acceso:

- **Longitud Mínima de 14 Caracteres:** Se exige un mínimo de 14 caracteres por cuenta, priorizando el uso de frases de contraseña (passphrases) largas y memorables para mitigar ataques de fuerza bruta.
- **Gestión con Kaspersky Password Manager:** Se adopta oficialmente este gestor empresarial para el resguardo cifrado de credenciales, prohibiendo el almacenamiento nativo en navegadores (Chrome/Edge) o notas físicas.
- **Modificación Basada en Eventos de Riesgo:** Se elimina la rotación obligatoria temporal para evitar patrones predecibles. El cambio de credenciales se ejecutará de forma reactiva ante alertas de brechas o desvinculación de personal.
- **Prohibición de Reutilización:** Queda restringido el uso de la contraseña corporativa en plataformas de carácter personal o servicios externos a la organización.

- **Mitigación de Fugas por OSINT:** Se prohíbe incluir datos personales expuestos en fuentes abiertas (redes sociales) en las frases de seguridad para evitar ataques dirigidos por ingeniería social.

1.2 Protocolo de PIN y Acceso Local a Equipos

Establece las directrices de seguridad física en los endpoints asignados:

- **Cifrado de Disco Completo:** Es obligatorio el uso de PIN personal inmediato en laptops y la activación de cifrado de hardware (BitLocker en Windows / FileVault en Mac) con llaves custodiadas por TI.
- **Autenticación en Dispositivos Móviles:** Todo smartphone corporativo debe asegurar un PIN de bloqueo de pantalla robusto para restringir el acceso local a los buzones institucionales.
- **Tiempos de Bloqueo por Inactividad:** Se establece el forzado técnico de bloqueo automatizado tras 10 minutos de inactividad en laptops y 2 minutos en smartphones.
- **Bloqueo Manual y Escritorio Limpio:** Es obligatorio ejecutar el comando Windows + L y cerrar la tapa del equipo al retirarse del puesto, manteniendo el área libre de documentos confidenciales expuestos.
- **Gestión de Borrado Remoto:** Los dispositivos móviles se inscribirán en el MDM de Google Workspace Endpoint Management para permitir la destrucción remota de datos ante robo o extravío.

1.3 Autenticación de Múltiples Factores (MFA)

Capas de validación de identidad obligatorias para el ecosistema en la nube:

- **Forzado Centralizado desde Consola:** IT aplicará la política de MFA mandatoria para la totalidad de usuarios directamente desde la consola de Google Workspace.
- **Cobertura Completa de Plataformas:** El uso de MFA es requisito no negociable en Google, Microsoft 365, Monday, SurveyMonkey, Luma, AWS y portales bancarios.
- **Jerarquía de Métodos de Validación:** Se establece el uso prioritario de aplicaciones autenticadoras (Google/Microsoft Authenticator) mediante códigos TOTP; el uso de SMS queda relegado a contingencias.
- **Resguardo de Llaves de Recuperación**: Los códigos de respaldo generados se almacenarán exclusivamente de forma digital y cifrada dentro de Kaspersky Password Manager.
- **Auditoría de Parámetros de Seguridad:** IT ejecutará revisiones mensuales en Google Workspace y Microsoft 365 para validar la persistencia de las directivas globales de Security Defaults.

1.4 Seguridad en WhatsApp Corporativo

Protección del canal de comunicación oficial frente a vectores de suplantación:

- **Verificación de Dos Pasos Independiente:** Es obligatorio activar el PIN interno de 6 dígitos en la aplicación, control que actúa de forma independiente al MFA del dispositivo.

- **Backups con Cifrado de Extremo a Extremo:** Los respaldos automáticos en Google Drive deben configurarse con cifrado activo, resguardando la clave maestra.
- **Autogestión de Sesiones Concurrentes:** El colaborador debe realizar una depuración mensual de dispositivos vinculados en WhatsApp Web/Desktop para revocar accesos inactivos.
- **Restricción de Contenido Financiero:** Queda prohibido el envío de credenciales, fotografías de tarjetas de crédito o datos bancarios por este medio, sustituyéndolo por Teams o Google Drive.
- **Habilitación de Notificaciones de Seguridad:** Deben mantenerse activas las alertas de cambio de códigos de seguridad y de nuevos dispositivos vinculados.

1.5 Higiene Digital en la Navegación Web

Controles en navegadores para mitigar ataques de secuestro de sesión (Session Hijacking):

- **Prohibición de Almacenamiento Local de Claves:** Se restringe el uso de la función nativa "Recordar contraseña" de los navegadores por la vulnerabilidad de extracción de credenciales ante malware.
- **Purga Semanal Obligatoria de Cookies:** Todo usuario debe ejecutar una limpieza de historial, cookies y caché semanalmente para invalidar tokens de sesión activos explotables.
- **Sincronización Corporativa Obligatoria:** Se exige el uso exclusivo de navegadores autorizados (Chrome o Edge) vinculados al perfil y cuenta institucional de CentraRSE.

- **Restricción de Extensiones no Validadas:** Queda prohibida la instalación de extensiones de navegador sin aprobación de IT, especialmente herramientas de IA externas que comprometan la lectura del DOM.
- **Aislamiento de Sesiones Técnicas:** El área de TI empleará Ventanas de Incógnito para el acceso a consolas de administración de infraestructura con el fin de evitar la persistencia de artefactos temporales.

Sección II

Protección de Endpoints y Licenciamiento

Sección II: Protección de Endpoints y Licenciamiento

Esta sección define las capas de defensa técnica en dispositivos finales para la detección y neutralización de código malicioso y amenazas de Ransomware, bajo los marcos ISO/IEC 27001:2022 (A.8.7) y NIST CSF 2.0 (DE.CM-09).

2.1 Protección Antivirus Empresarial

Establece los criterios de despliegue para la monitorización centralizada de amenazas en los endpoints:

- **Migración Obligatoria a KSOS:** Se implementará Kaspersky Small Office Security Premium, habilitando la consola web centralizada Kaspersky Business Hub.
- **Protección Activa y Módulo de Rollback:** El agente local mantendrá activa la detección heurística para bloquear Ransomware y revertir cambios maliciosos automáticamente.
- **Control de Dispositivos por Hardware:** Se ejecutará el bloqueo automatizado de unidades de almacenamiento masivo USB no autorizadas directamente desde la consola.
- **Inviolabilidad de las Directivas locales:** Queda prohibido pausar, desinstalar o modificar el antivirus; cualquier excepción será gestionada por IT.
- **Reporte Automatizado de Cumplimiento:** La consola web emitirá alertas automáticas sobre equipos fuera de línea o con firmas desactualizadas.

2.2 Optimización y Actualización del Sistema

Garantiza el mantenimiento preventivo y el cierre oportuno de brechas de seguridad por vulnerabilidades técnicas:

- **Despliegue Inmediato de Parches Críticos:** Es obligatorio instalar las actualizaciones de seguridad de Windows/macOS en un plazo máximo de 48 horas en modo automático.
- **Evaluación Automatizada de Vulnerabilidades:** Se programarán reportes automáticos desde la consola de Kaspersky para identificar equipos con parches críticos pendientes.
- **Restricción de Privilegios de Administrador Local:** Los usuarios finales no tendrán permisos de administrador en sus laptops para evitar alteraciones en el sistema.
- **Optimización y Limpieza de Hardware:** Se establece el uso regular de PC Manager para la depuración de archivos temporales y optimización del equipo.
- **Mantenimiento Semanal de Plugins Web:** Se actualizarán mensualmente los plugins críticos de WordPress (Elementor y All In One SEO) para mitigar riesgos en el sitio.

2.3 Monitoreo de Infraestructura y Logs de Seguridad

Implementación de controles de visibilidad inmutable para la detección temprana de anomalías en el ecosistema digital:

- **Centralización en AWS CloudWatch:** Se mantiene la recopilación inmutable de logs del backend de la plataforma Juntos 2.0 para auditoría forense.

- **Auditoría de Comandos Nativos (Living off the Land):** Se supervisará y alertará el uso anómalo de herramientas legítimas del sistema operativo como Powershell o BitsAdmin.
- **Disparadores Automáticos de Alertas Cloud:** Se configuran alertas en Google y Microsoft ante intentos fallidos repetidos o accesos desde ubicaciones inusuales.
- **Retención Mínima Obligatoria de Logs:** Todo registro de auditoría y seguridad en las nubes corporativas mantendrá una retención inalterable de 12 meses.
- **Monitoreo Continuo de Fugas (OSINT):** Se suscribe el dominio institucional a HavelBeenPwned para detectar cuentas corporativas filtradas en brechas públicas.

2.4 Política de Software Legítimo y Licenciamiento

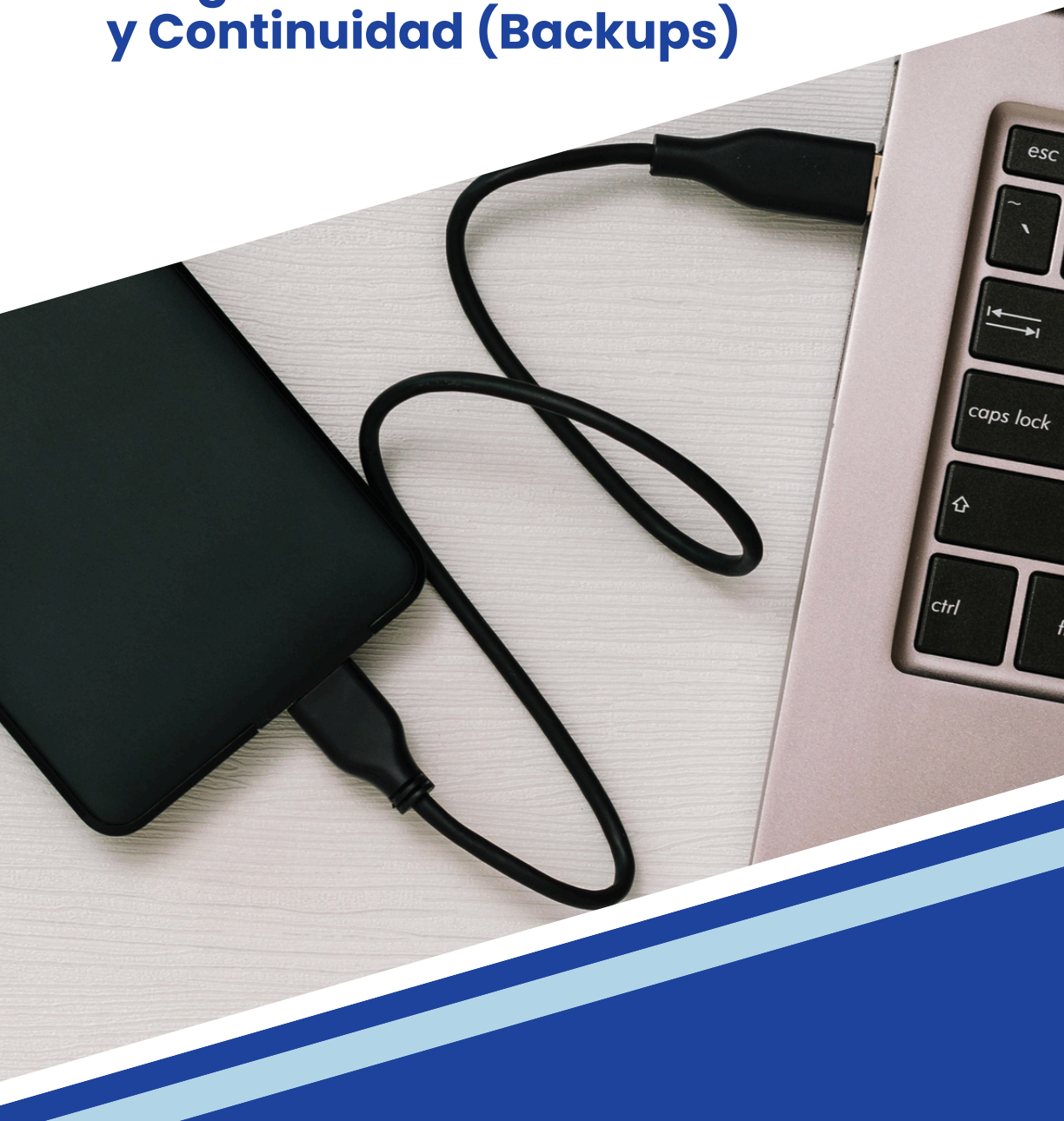
Establece los estándares de cumplimiento técnico y legal para la ejecución de aplicaciones corporativas:

- **Cero Tolerancia a Software Crackeado:** Prohibición absoluta de instalar programas modificados o activadores ilegales, principal vector de entrada de ransomware.
- **Definición de Software Autorizado:** Se permite únicamente el uso de software con licencia válida (comercial, open source u oficial gratuito) aprobado por TI.
- **Validación de Inventario vía Consola:** Se ejecutará una auditoría mensual automática del software instalado en cada endpoint desde Kaspersky Business Hub.

- **Bloqueo Preventivo de Binarios:** Se restringe localmente la ejecución de archivos de riesgo (.exe, .bat) provenientes de fuentes externas no autorizadas.
- **Tramitación Formal de Licencias:** Toda nueva herramienta digital requerida por el personal debe ser solicitada formalmente a Administración y IT para su compra.

Sección III

Resguardo de Información y Continuidad (Backups)



Sección III: Resguardo de Información y Continuidad (Backups)

Esta sección define las directrices obligatorias para la replicación, almacenamiento y disponibilidad de los datos institucionales, bajo los estándares internacionales ISO/IEC 27001:2022 (A.8.13) y NIST SP 800-34

3.1 Sincronización Automática de Usuario

Establece los mecanismos de respaldo en tiempo real para mitigar pérdidas por fallos físicos o sustracción de endpoints:

- **Uso Exclusivo de Repositorios Cloud:** Todo documento de trabajo debe almacenarse en las carpetas institucionales sincronizadas con Google Drive o OneDrive vinculadas a la cuenta @centrarse.org.
- **Alcance de los Directorios Locales:** La sincronización automática debe cubrir obligatoriamente los directorios locales de "Mis Documentos", "Escritorio" y archivos vinculados a proyectos activos.
- **Prohibición de Almacenamiento Local Aislado:** Queda estrictamente prohibido el guardado exclusivo de datos en el disco local sin su debido respaldo y réplica en la nube.
- **Validación de Drive/OneDrive al Onboarding:** Se integra en el checklist de ingreso de personal la verificación física de que los agentes cloud estén activos y sincronizando antes de entregar el equipo.

- **Adopción de la Estrategia Operativa 3-2-1:** Se promueve la resiliencia de datos mediante el almacenamiento de 3 copias de seguridad en 2 medios distintos (Cloud/Local) y 1 de ellos fuera del entorno principal.

3.2 Resguardo de Infraestructura y Plataformas

Garantiza la continuidad operativa de los entornos web y las consolas estratégicas de la organización:

- **Resguardos Sistemáticos de WordPress:** Se mantiene la ejecución automatizada de backups diarios del sitio web oficial de CentraRSE y la plataforma Juntos 2.0 utilizando el plugin All In One SEO/AIOS.
- **Trazabilidad en Herramientas de Productividad:** Se configurarán respaldos periódicos de la información alojada en Monday.com, Luma y Google Drive corporativo para proteger la memoria histórica de los proyectos.
- **Mantenimiento Técnico de Plugins:** Las actualizaciones semanales de Elementor y AIOS se ejecutarán de forma mandatoria para evitar fallas lógicas o brechas durante los procesos de respaldo.
- **Pruebas Semestrales de Restauración (Test de Restore):** El área de TI realizará simulacros de recuperación cada 6 meses para verificar que los respaldos de infraestructura sean íntegros, legibles y funcionales.

3.3 Continuidad en Dispositivos Móviles

Asegura la preservación de los canales de comunicación institucionales frente al extravío de terminales móviles:

- **Cifrado de Copias de WhatsApp:** Es obligatorio vincular el backup diario de WhatsApp Business a la cuenta de Google institucional, activando el cifrado de extremo a extremo.
- **Custodia de Claves de Cifrado Móvil:** Las contraseñas maestras generadas para los respaldos cifrados de WhatsApp se almacenarán exclusivamente en el gestor de contraseñas de TI.
- **Sincronización Centralizada de Agendas:** Toda la información de contactos corporativos y calendarios debe sincronizarse únicamente con el ecosistema de la cuenta @centrarse.org.
- **Restricción de Almacenamiento SIM/Local:** Se prohíbe guardar contactos institucionales o agendas de socios directamente en la memoria local del teléfono o en la tarjeta SIM.
- **Horario Homologado de Respaldos:** Las aplicaciones móviles se configurarán técnicamente para ejecutar sus backups en la nube diariamente a las 2:00 AM para optimizar el ancho de banda.

3.4 Protocolo de Cifrado y Archivo Histórico

Establece las medidas de mitigación contra fallos físicos, borrado accidental y robo en el repositorio histórico principal:

- **Cifrado Mandatorio BitLocker To Go:** El disco duro físico de 8 TB que concentra el archivo histórico institucional debe estar cifrado obligatoriamente con BitLocker To Go.

- **Custodia de la Clave Maestra de Recuperación:** La clave de descifrado del repositorio histórico será resguardada únicamente por el área de TI dentro de la carpeta compartida de continuidad.
- **Duplicación Homóloga de Contingencia:** Se establece la creación de un segundo disco espejo de 8 TB, igualmente cifrado, esguardado en una ubicación física externa y segura.
- **Configuración Forzada de Solo Lectura:** El disco físico que se preste a los colaboradores para consultas de información se entregará configurado estrictamente en modo de solo lectura.
- **Exclusión como Mecanismo de Continuidad:** Se determina que el disco de 8 TB actúa como archivo histórico complementario y no sustituye los respaldos automáticos en la nube.

Sección IV

Conectividad y Seguridad Física

Sección IV: Conectividad y Seguridad Física

Esta sección establece las directrices lógicas y físicas para mitigar la interceptación de tráfico de datos y la sustracción de activos de CentraRSE, bajo las normas ISO/IEC 27001:2022 (A.8.20 / A.8.22) y NIST SP 800-46 Rev. 2.

4.1 Uso Seguro de Redes y Conectividad

Define los estándares técnicos para la transmisión de datos fuera y dentro de las instalaciones institucionales:

- **Prohibición Absoluta de Redes Públicas:** Queda restringido conectar cualquier equipo corporativo a redes Wi-Fi abiertas o públicas sin seguridad robusta (aeropuertos, cafés o coworkings) por el riesgo crítico de ataques de Man-in-the-Middle.
- **Uso Obligatorio de Hotspot Corporativo:** Ante la necesidad de conectividad externa, el colaborador utilizará de forma exclusiva la función de "Compartir Internet" desde su smartphone asignado por la organización.
- **Activación Mandatoria de VPN Institucional:** Se establece el uso obligatorio de Kaspersky VPN Secure Connection (incluida en el plan KSOS) para encriptar el tráfico de forma ilimitada en cualquier conexión externa.
- **Rotación de Credenciales de Red Local:** La contraseña del Wi-Fi de la oficina de CentraRSE se actualizará anualmente de forma preventiva, y de manera inmediata ante la desvinculación de cualquier colaborador para revocar el acceso físico-radial.

- **Segregación de Tráfico para Invitados:** Se mantendrá configurada de forma permanente una red Wi-Fi aislada y exclusiva para visitantes, socios o consultores, impidiendo su acceso al segmento de la red corporativa.

4.2 Protocolo de Bloqueo y Custodia de Equipos

Establece las obligaciones operativas para salvaguardar la integridad de los endpoints durante la jornada laboral:

- **Comando Forzado de Bloqueo Local:** Al retirarse momentáneamente de su puesto, el colaborador debe ejecutar el atajo Windows + L (PC) o Ctrl + Cmd + Q (Mac), procediendo inmediatamente a cerrar la tapa de la laptop.

- **Prevención de Accesos No Supervisados:** La aplicación del bloqueo local es obligatoria para impedir la visualización o manipulación de información confidencial por parte de terceros mientras el equipo no esté bajo supervisión directa.

- **Cumplimiento de Escritorio Limpio:** Queda prohibido dejar documentos físicos sensibles (contratos, facturas, listados de socios) o contraseñas anotadas expuestas en el área de trabajo al finalizar la jornada laboral.

- **Resguardo Nocturno y de Fin de Semana:** Los activos (laptops y smartphones) deben permanecer resguardados bajo llave en la oficina o en el domicilio del colaborador en un espacio seguro y fuera de la vista de terceros.

- **Prohibición de Almacenamiento en Vehículos:** Queda estrictamente prohibido dejar equipos de cómputo o celulares dentro de vehículos corporativos o personales, sin importar si estos se encuentran cerrados o en parqueos públicos.

4.3 Viajes, Desplazamientos y Gestión de Incidentes

Regula la seguridad física de los activos durante traslados institucionales, viajes internacionales y protocolos de emergencia:

- **Transporte Seguro de Activos:** Los equipos informáticos deben movilizarse exclusivamente dentro de las mochilas asignadas por la organización, mitigando impactos físicos o detecciones visuales externas.

- **Uso Exclusivo de Parqueos Supervisados:** Si es estrictamente necesario transportar el equipo en vehículo, el colaborador está obligado a utilizar únicamente parqueos pagados que cuenten con seguridad privada e infraestructura de vigilancia.

- **Restricción de Equipos en Viajes Personales:** En viajes de carácter estrictamente personal al extranjero, los equipos de CentraRSE deben permanecer obligatoriamente en territorio nacional, apagados y bajo resguardo seguro.

- **Autorización para Viajes Oficiales:** La salida de laptops o smartphones fuera de las fronteras nacionales se limitará única y exclusivamente a misiones de trabajo oficiales debidamente aprobadas por la Dirección Ejecutiva.

- **Reporte Inmediato de Pérdida o Robo:** Ante el extravío o robo de un activo físico, el colaborador debe notificar a IT y a Administración en un plazo máximo e improrrogable de 2 horas para ejecutar el bloqueo remoto y coordinar la denuncia legal.

Sección V

Eventos Virtuales y Uso Ético de IA

Sección V: Eventos Virtuales y Uso Ético de IA

Esta sección establece las directrices lógicas para el desarrollo seguro de eventos digitales y la gobernanza en el uso de herramientas de Inteligencia Artificial en CentraRSE, bajo las normas ISO/IEC 27001:2022 (A.8.12) y NIST CSF 2.0 (PR.DS-01/02).

5.1 Seguridad en Eventos Virtuales y Plataformas de Transmisión

Regula los controles de acceso y mitigación de intrusiones en sesiones digitales institucionales:

- **Uso Exclusivo de Microsoft Teams:** Se establece Teams como la única plataforma oficial para reuniones y eventos; Zoom queda prohibido operativamente por brechas de seguridad.
- **Configuración del Protocolo en 3 Vías:** Todo evento masivo requiere la asignación obligatoria de roles técnicos en sala: (1) Anfitrión, (2) Moderador de chat y (3) Administrador de señales.
- **Control de Acceso y Salas de Espera:** Es obligatorio activar la función de Sala de Espera y el registro previo para validar la identidad de los asistentes externos.
- **Restricción de Permisos para Invitados:** Se configurará por defecto el bloqueo de compartición de pantalla, uso de micrófonos y encendido de cámaras para participantes ajenos.
- **Gestión de Enlaces de Acceso Masivo:** Queda prohibido publicar enlaces directos de moderación o contraseñas de eventos en canales públicos o redes sociales abiertas.

5.2 Uso Ético y Seguro de Inteligencia Artificial (IA)

Establece el marco de gobernanza para la introducción de tecnologías de automatización cognitiva:

- **Restricción de Herramientas de IA Gratuitas:** Queda prohibido el uso de versiones de IA públicas o gratuitas (ChatGPT libre, DeepSeek) para procesar información de la organización.
- **Prohibición de Ingesta de Datos Sensibles (PII/SPII):** Se prohíbe introducir nombres de socios, registros financieros, estrategias de negocio o salarios en motores de IA externos.
- **Uso Obligatorio de Gemini Workspace Licenciado:** Todo análisis corporativo con IA debe ejecutarse exclusivamente en Gemini con licencia empresarial para evitar la fuga de datos.
- **Validación Humana de Entregables (Anti-Alucinación):** Todo informe o material generado o asistido por IA debe pasar por una revisión técnico-humana para verificar su veracidad.
- **Declaración de Contenido Asistido:** Los documentos públicos de CentraRSE que utilicen IA de forma mayoritaria en su redacción deben incluir una nota de transparencia institucional.

5.3 Ecosistema Autorizado y Control de Extensiones

Define el perímetro de software permitido y la mitigación de fuga de datos en navegadores:

- **Catálogo Corporativo Cerrado:** El software se restringe a:
    - **Ejecución General**: Google Workspace, Microsoft 365, Teams, Monday, SurveyMonkey y Mentimeter.
    - **Comunicación:** Adobe CC, Canva, Brevo y Elementor.
    - **Administración:** Odoo como sistema contable oficial.
- **Bloqueo de Extensiones Espías en Navegadores:** Se prohíbe la instalación de extensiones no autorizadas con privilegios técnicos para leer el DOM y capturar credenciales de sesión.
- **Restricción de Plugins Automatizados en WordPress:** La instalación de complementos adicionales en el sitio web institucional queda centralizada y sujeta a auditoría de IT.
- **Uso de Cuentas Institucionales Unificadas:** Todo acceso a las plataformas del ecosistema autorizado se realizará exclusivamente mediante el correo @centrarse.org con MFA activo.
- **Auditoría de Extensiones vía MDM:** El área de IT ejecutará revisiones lógicas remotas para identificar y remover complementos de terceros no aprobados en los navegadores corporativos.

Sección VI

Cultura Preventiva y Respuesta a Incidentes

Sección VI: Cultura Preventiva y Respuesta a Incidentes

Esta sección define las directrices de concientización y los protocolos operativos de reacción ante vectores de ataque que comprometan los activos de CentraRSE, bajo los estándares ISO/IEC 27001:2022 (A.6.3 / A.5.24) y NIST SP 800-50 Rev. 1.

6.1 Los 3 Puntos Vitales de Concientización Institucional

Establece los criterios de identificación de amenazas críticas orientados a reducir la superficie de ataque derivada del factor humano:

- **Malware (Software Malicioso):** Identificación de programas encubiertos diseñados para infiltrarse o interrumpir sistemas; se mitiga bajo la prohibición estricta de ejecutar archivos sin firma o licencias.
- **Ransomware (Secuestro de Datos):** Código malicioso orientado al cifrado ininterrumpido de archivos masivos con fines de extorsión económica; se establece que la replicación sistemática es la única defensa operativa real.
- **Phishing (Suplantación de Identidad):** Técnicas de ingeniería social mediante correos o dominios simulados (ej: support@banco-bi.net) para la sustracción de credenciales de acceso o tokens.
- **Análisis de Vectores por OSINT:** Concientización sobre la fase de reconocimiento del atacante, restringiendo la publicación visual de lanyards, planos o credenciales corporativas en perfiles de redes sociales.

- **Detección del Eslabón Técnico de Entrada:** Capacitación al personal para verificar extensiones sospechosas (como archivos .exe camuflados como currículums), impidiendo la ejecución de payloads en los endpoints.

6.2 Protocolo de Reacción Inmediata D.C.A.R.

Define el flujo secuencial y obligatorio que debe ejecutar el colaborador ante la sospecha o confirmación de un compromiso de seguridad:

- **Desconectar (Aislamiento Inmediato):** El usuario debe cortar de forma instantánea la conexión Wi-Fi o cable de red física del equipo afectado para contener la propagación radial del malware.
- **Cambiar (Protección de Identidad):** Modificar de forma inmediata la totalidad de las contraseñas institucionales expuestas, ejecutando la acción estrictamente desde un dispositivo alterno seguro.
- **Analizar (Mitigación Lógica):** Notificar de forma mandatoria al área de TI para proceder con el aislamiento lógico del endpoint, auditoría de logs y ejecución de escaneos profundos antivirus.
- **Reporte y Documentación Formal:** Es obligatorio reportar el evento de forma inmediata llenando el Formulario de Anomalías oficial de la organización a través del siguiente enlace institucional, https://wkf.ms/4dltldm.

- **Erradicación y Cuarentena Remota:** El área de IT mantendrá el dispositivo en aislamiento de red e implementará la eliminación forzada de artefactos maliciosos antes de reincorporar el hardware a la red interna.

6.3 Programa de Capacitación Técnica y Simulación

Establece la frecuencia, alcance y métricas de control para el fortalecimiento de las capacidades defensivas de la organización:

- **Frecuencia Semestral Obligatoria:** Se reestructura el ciclo de capacitación, fijando sesiones técnicas obligatorias semestrales para todo el personal junto con el envío mensual de micropíldoras informativas.
- **Segmentación de Contenidos por Roles:** Se definen tres niveles formativos: (a) General: ingeniería social y phishing; (b) Operativo: MFA y gestor de claves; (c) Directivo/Finanzas: fraudes de transferencia y suplantación ejecutiva.
- **Simulacros Trimestrales de Phishing:** El área de TI coordinará de forma obligatoria simulacros de ataques simulados trimestrales utilizando plataformas especializadas (GoPhish, KnowBe4 o herramientas controladas).
- **Métricas de Control de Superficie:** Se establecen la tasa de clics y la tasa de reporte oportuno como indicadores clave de cumplimiento de los simulacros para medir el nivel de riesgo real.
- **Coordinación y Registro Oficial:** Se nombra formalmente a Pablo Cabrera como responsable y coordinador del programa, quedando obligado a archivar las bitácoras de asistencia como evidencia de auditoría.

Sección VII

Manejo Financiero, Cumplimiento y Compromiso

Sección VII: Manejo Financiero, Cumplimiento y Compromiso

Esta sección define las directrices obligatorias para salvaguardar los activos financieros, la clasificación de datos sensibles y las responsabilidades legales de cumplimiento en CentraRSE, bajo las normas internacionales ISO/IEC 27001:2022 (A.5.14 / A.5.36) y el marco NIST CSF 2.0 (GV.OV-01).

7.1 Protección de Activos Financieros

Establece los controles lógicos mandatorios para mitigar riesgos de fraude bancario o robo de identidad financiera:

- **Confidencialidad Absoluta de Tarjetas:** Queda prohibido compartir fotografías, números, fechas de vencimiento o códigos CVV de tarjetas institucionales por WhatsApp, Teams o correo electrónico.
- **Uso Restringido de Credenciales de Pago:** La tarjeta empresarial de CentraRSE solo podrá ser portada y utilizada por el personal expresamente autorizado por la Dirección Ejecutiva y Administración.
- **Transacciones en Entornos Seguros:** Todo pago o ingreso de credenciales bancarias debe realizarse exclusivamente desde equipos corporativos protegidos y redes cableadas o Wi-Fi seguras.
- **Doble Aprobación de Transferencias:** Se implementa el principio de segregación de funciones en los portales bancarios, requiriendo un usuario preparador (Administración) y un usuario autorizador (Dirección).

- **Bloqueo Inmediato por Sospecha:** Ante cualquier alerta de consumo no reconocido o sospecha de phishing financiero, el portador de la tarjeta está obligado a reportarlo a TI para coordinar el bloqueo bancario inmediato.

7.2 Clasificación y Manejo de Información

Define los niveles de criticidad de los activos de información para garantizar su correcto tratamiento y privacidad:

- **Clasificación de Información Pública:** Datos, memorias de sostenibilidad o materiales de eventos destinados a la libre difusión abierta y sin restricciones de acceso.
- **Clasificación de Información Interna:** Comunicaciones operativas, minutas de trabajo agendas y correos cotidianos de uso exclusivo para el personal de la organización.
- **Tratamiento de Datos Confidenciales (PII):** Datos críticos (registros financieros, planillas o salarios) que exigen cifrado obligatorio debido al alto riesgo de seguridad en caso de exposición.
- **Procesamiento Exclusivo con Gemini:** Toda información clasificada como Confidencial (PII) o Sensible ($SPII$) debe procesarse obligatoriamente utilizando Gemini con licencia empresarial para evitar fugas.

7.3 Cumplimiento, Monitoreo y Auditoría

Establece las consecuencias administrativas y los mecanismos técnicos para garantizar la obligatoriedad de este manual:

- **Obligatoriedad de los Estándares:** El cumplimiento de la totalidad de las secciones de este manual es mandatorio para todo el personal, consultores externos y terceros vinculados.
- **Supervisión Técnica vía Kaspersky Hub:** El área de TI utilizará la consola centralizada de Kaspersky Business Hub para monitorear el estado del antivirus, actualizaciones pendientes y bloqueos de USB.
- **Auditoría Externa Independiente Anual:** Se establece una cláusula de revisión anual obligatoria del cumplimiento de estas políticas por parte de un consultor de ciberseguridad externo e independiente.
- **Gobernanza BYOD (Dispositivos Personales):** Se autoriza el acceso a Monday o correo desde teléfonos propios, exigiendo obligatoriamente un PIN de pantalla robusto, cifrado activo del sistema y autorización de borrado remoto selectivo de la cuenta institucional ante robo.
- **Checklist de Egreso Obligatorio (Offboarding):** Ante la baja de cualquier colaborador, IT y Administración ejecutarán la revocación inmediata de accesos a Google/Microsoft y el cambio mandatorio de contraseñas compartidas para mitigar fugas.
- **Consecuencias por Incumplimiento Deliberado:** La desactivación intencional de sistemas de seguridad o el uso de software crackeado será reportado a Administración, dando lugar a medidas administrativas.

Preguntas Frecuentes

1. ¿Por qué ya no es obligatorio cambiar mi contraseña cada 3 meses si antes era una regla estricta?

Porque los estudios técnicos demostraron que la rotación forzada hace que los usuarios creen patrones predecibles y fáciles de adivinar (como cambiar Clave2026! por Clave2026.). Ahora exigimos una contraseña inicial mucho más larga (mínimo 14 caracteres), la cual solo se cambiará si existe una sospecha real de que fue filtrada o comprometida.

2. ¿Puedo conectar la laptop de la oficina al Wi-Fi de un centro comercial o cafetería si es una emergencia de trabajo?

No, queda estrictamente prohibido conectar los equipos institucionales a redes Wi-Fi públicas o abiertas debido al alto riesgo de que un atacante intercepte tu tráfico y robe tus credenciales (ataques de Hombre en el Medio). Ante emergencias fuera de la oficina, debes usar exclusivamente la función de "Compartir Internet" (Hotspot) de tu celular corporativo.

3. Si descargo un archivo adjunto que parece un PDF pero tiene extensión ".exe", ¿qué debo hacer?

No debes abrirlo ni ejecutarlo bajo ninguna circunstancia, ya que los archivos con extensión .exe son programas ejecutables y constituyen el principal vector de entrada de virus y Ransomware. Debes aislar tu equipo de la red y reportar la anomalía inmediatamente a TI a través del formulario oficial.

4. ¿Por qué debo borrar las cookies y el historial de mi navegador web todas las semanas?

Porque al navegar en internet se almacenan pequeños archivos llamados "tokens de sesión" que te permiten entrar a tus cuentas sin pedirte clave. Si un virus infecta tu computadora, lo primero que hace es robarse esos tokens (Session Hijacking) para entrar a tus plataformas evadiendo la doble verificación; la limpieza semanal destruye esos archivos viejos.

Preguntas Frecuentes

5. ¿Qué pasa si dejo mi laptop encendida en mi escritorio mientras voy a una reunión rápida en la oficina?

Incumples la política de Escritorio Limpio y Custodia de Activos. Al retirarte de tu puesto por cualquier motivo, estás obligado a presionar las teclas Windows + L (o Ctrl + Cmd + Q en Mac) y cerrar físicamente la tapa de la laptop para prevenir accesos no autorizados a información confidencial de socios.

6. ¿Por qué está prohibido usar Zoom para los webinars o reuniones con socios si es la plataforma más común?

Zoom quedó descontinuado operativamente a nivel institucional debido a las recurrentes fallas críticas de seguridad y privacidad que presenta la herramienta. La plataforma oficial aprobada y licenciada por la organización para garantizar la confidencialidad de las transmisiones es Microsoft Teams.

7. Para diseñar materiales rápidos, ¿puedo usar herramientas de Inteligencia Artificial gratuitas como ChatGPT o DeepSeek?

Sí, se permite el uso de ChatGPT o DeepSeek únicamente para la generación de borradores, ideas creativas o textos generales que no involucren datos confidenciales. Queda terminantemente prohibido subir a esas plataformas gratuitas listas de socios, nombres, correos o estrategias internas, ya que sus términos no garantizan la privacidad de los datos.

8. ¿Puedo instalar una extensión de IA en Chrome (como Grammarly o Copilot personal) para redactar correos más rápido?

No, queda prohibida la instalación de extensiones de navegador sin la aprobación explícita de IT. Estos complementos tienen permisos técnicos profundos para leer todo el contenido de la pantalla corporativa, lo que representa un riesgo crítico de fuga de información institucional y datos de socios.

Preguntas Frecuentes

9. Si publicamos fotos de eventos o de las oficinas en las redes sociales de CentraRSE, ¿qué precaución debemos tomar?

Deben realizar una inspección visual estricta antes de publicar para asegurar que en las fotografías no se filtren de forma visible acreditaciones (lanyards), planos de las oficinas, pantallas con sistemas abiertos o contraseñas anotadas. Los atacantes utilizan estas imágenes públicas en internet (OSINT) para planificar intrusiones físicas o virtuales.

10. ¿Por qué las herramientas de diseño como Canva o Adobe Creative Cloud están restringidas solo al departamento de Comunicación?

Porque forman parte de la política de Catálogo Corporativo Cerrado por Roles, la cual busca reducir el software innecesario en los endpoints de la organización. Al limitar las licencias de diseño exclusivamente al personal de Comunicación, IT mantiene un control estricto de los accesos y reduce la superficie de ataque.

11. ¿Por qué está prohibido pasar una foto o los datos de la tarjeta de crédito institucional por el grupo de WhatsApp del trabajo?

Porque WhatsApp, a pesar de estar cifrado en el celular, es un canal altamente vulnerable a la clonación de cuentas o al acceso visual por descuidos físicos. Compartir datos financieros o códigos CVV por chats o correos expone a la organización a fraudes electrónicos masivos o robo de identidad financiera.

12. ¿Qué control extra implementamos en los portales bancarios para evitar transferencias erróneas o fraudes?

Se implementa de forma obligatoria el principio técnico de Doble Aprobación o segregación de funciones. Esto significa que el equipo de Administración actúa exclusivamente como el usuario "preparador" de la transacción, y la Dirección Ejecutiva debe actuar como el usuario "autorizador" final para validar su legitimidad.

Preguntas Frecuentes

13. ¿Qué es el sistema Odoo y quiénes están autorizados para acceder a esta plataforma?

Odoo es el sistema contable y administrativo oficial de CentraRSE. Su acceso está estrictamente restringido al personal del departamento de Administración y Finanzas que cuente con credenciales corporativas autorizadas y tenga activa de forma mandatoria la doble verificación (MFA).

14. Si un proveedor o consultor me pide que le instale un programa en mi laptop para ver un reporte, ¿puedo hacerlo?

No, el personal de Finanzas y Administración no posee permisos de administrador local en las laptops por directriz de seguridad. Queda prohibida la instalación de cualquier software que no esté aprobado en el catálogo oficial; si se requiere una herramienta, debe solicitarse formalmente a Desarrollo Institucional y IT para su compra legal.

15. ¿Qué tipo de información financiera de los socios se considera "Dato Sensible" (SPII) y cómo debe manejarse?

Se consideran Datos Sensibles (SPII) las planillas de salarios, los estados de cuenta, registros de pago de cuotas y números bancarios de los socios. Esta información requiere cifrado obligatorio y, en caso de necesitar algún análisis gráfico o procesamiento masivo, debe utilizarse exclusivamente la consola licenciada de Gemini empresarial.

16. ¿Qué obligaciones legales tiene CentraRSE si sufrimos un ataque informático y se filtran datos de nuestros socios?

Bajo el marco del Reglamento General de Protección de Datos (RGPD), la organización está obligada por ley a reportar formalmente cualquier brecha de seguridad grave que afecte datos personales de los usuarios a la autoridad competente en un plazo menor a 72 horas. El incumplimiento de este plazo puede acarrear severas sanciones administrativas y legales.

Preguntas Frecuentes

17. ¿Por qué es obligatorio que la Dirección Ejecutiva autorice y revise las bitácoras del programa de concientización?

Porque las normativas internacionales (ISO 27001 / NIST) exigen que la alta dirección ejerza una gobernanza activa sobre el programa de ciberseguridad. Los registros de asistencia a las capacitaciones semestrales y los resultados de los simulacros trimestrales de phishing actúan como evidencia de cumplimiento legal ante auditorías externas.

18. Si un gerente viaja de vacaciones al extranjero, ¿puede llevar su laptop corporativa por si surge una emergencia?

No, las políticas de resguardo físico de la Dirección dictan que los activos institucionales deben permanecer estrictamente en territorio nacional, apagados y resguardados de forma segura durante los viajes personales del colaborador. La salida de equipos fuera de las fronteras del país se restringe exclusivamente a misiones de trabajo oficiales aprobadas.

19. ¿Puedo revisar mi correo institucional o el tablero de Monday desde mi celular o computadora personal?

Sí, pero el dispositivo personal queda sujeto estrictamente a las directrices de control de la organización. Es obligatorio configurar un PIN de pantalla, mantener el cifrado activo del sistema y aceptar la vinculación a la consola de TI para permitir un borrado remoto selectivo (account wipe) de la cuenta institucional en caso de pérdida.

20. ¿Qué implicaciones o consecuencias administrativas existen si un colaborador desactiva deliberadamente el antivirus?

El cumplimiento de todas las secciones de este manual es estrictamente obligatorio para todo el personal. El incumplimiento deliberado de estas normas, la desactivación intencional de las soluciones de seguridad (Kaspersky) o la instalación de software sin licencia válida será reportado inmediatamente a Administración para la aplicación de medidas administrativas.

CENTRARSE en GUATEMALA

Contacto

pcabrera@centrarse.org

5066-4246