UNIVERSIDAD TECNOLÓGICA METROPOLITANA
del Estado de Chile

DEPARTAMENTO DE INFORMÁTICA Y COMPUTACIÓN

FACULTAD DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

TRABAJO DE INVESTIGACIÓN
LA SEGURIDAD DEL TELETRABAJO

Módulo de "TÓPICOS DE SEGURIDAD DE LA INFORMACIÓN"

Alumno : Diego Moya Rivera

Profesor : Camilo Garrido Briones

SANTIAGO DE CHILE
NOVIEMBRE – 2025

ÍNDICE

INTRODUCCIÓN

A día de hoy, el teletrabajo se consolidó como una modalidad habitual en organizaciones públicas y privadas, impulsando transformaciones profundas en la gestión de TI y en los controles de seguridad aplicables a los sistemas de información. En este contexto, la dependencia de servicios en la nube, dispositivos personales (BYOD), aplicaciones colaborativas y conectividad residencial amplifica la superficie de ataque y expone nuevas brechas de gobernanza. Frente a este escenario, no basta con replicar controles perimetrales tradicionales: se requiere un enfoque de gestión de riesgos que incorpore identidad, dispositivos, datos y aplicaciones como ejes de protección, con métricas que evidencien eficacia y mejora continua.

Este ensayo argumenta que el teletrabajo exige evolucionar desde arquitecturas centradas en la red hacia modelos centrados en la identidad y en el dato, apoyados en marcos normativos robustos y buenas prácticas de Zero Trust. Se sostiene que la implementación de controles técnicos debe estar orquestada por políticas, procesos y capacidades de monitoreo continuo, y que la efectividad del programa de seguridad depende de una alineación estratégica entre gestión del riesgo, cumplimiento normativo y experiencia del usuario.

El objetivo es analizar riesgos y desafíos del teletrabajo, discutir controles aplicables y proponer lineamientos de implementación y medición que permitan sostener la postura de seguridad sin sacrificar productividad. Dicho análisis se materializa en una propuesta de implementación por fases, validada por indicadores clave de rendimiento (KPI) que demuestran la eficacia de los controles. El alcance incluye riesgos técnicos y organizacionales (acceso, endpoint, red, datos, nube, cultura), controles alineados a estándares, y métricas de desempeño; se excluyen aspectos laborales o ergonómicos ajenos a la ciberseguridad.(Sahnoune, 2025)

EL TELETRABAJO Y LA SEGURIDAD DE LA INFORMACIÓN

1. RIESGOS Y DESAFÍOS EN ENTORNOS REMOTOS

La transición a este tipo de modelo de trabajos, introduce una gran cantidad de desafíos que atentan contra el perímetro de seguridad tradicional. Analizar cada uno de estos nuevos desafíos es el primer paso para construir una estrategia de defensa resistente y adaptativa.

1.1. IDENTIDAD Y ACCESO

En entornos remotos, donde los usuarios acceden a recursos críticos desde redes no confiables, la identidad se convierte en el principal perímetro de seguridad. El compromiso de cuentas de usuario es uno de los puntos de ataque más críticos y prevalentes. Las tácticas de ingeniería social, como el phishing, se vuelven más efectivas al dirigirse al entorno doméstico, a menudo menos controlado. Un atacante que obtiene una credencial válida puede moverse lateralmente por los sistemas corporativos, escalar privilegios y filtrar datos sensibles con una apariencia de legitimidad.

Para mitigar este riesgo, las buenas prácticas recomiendan la implementación de autenticación multifactor (MFA) de carácter obligatorio. Esta medida añade una capa de protección fundamental al proponer una forma alternativa de verificación además de la contraseña. Sin embargo, la creciente sofisticación de los ataques ha dado lugar a la "fatiga de MFA" (MFA fatigue). Para contrarrestar esto, es crucial implementar controles anti-fatiga, como el number matching, que exige al usuario introducir un número que se muestra en la pantalla de inicio de sesión, asegurando así una aprobación intencionada (Semperis, 2023).

Además, se debe aplicar rigurosamente el principio de menor privilegio y realizar re-certificaciones periódicas de permisos. Estas prácticas se alinean directamente con los dominios de control de normativas como ISO/IEC 27001:2022 (NQA [NQA], 2022), así como con la familia de controles "IA" (Identification and Authentication) del estándar NIST SP 800-53 r5.(National Institute of Standards and Technology, 2020)

1.2. DISPOSITIVOS Y ENDPOINTS

La diversidad de los dispositivos utilizados para el teletrabajo (corporativos y BYOD) incrementa exponencialmente la superficie de ataque. Cada endpoint es una puerta de entrada potencial. Las guías de referencia priorizan la gestión centralizada a través de soluciones de Gestión Unificada de Endpoints (UEM) o Gestión de Dispositivos Móviles (MDM).

Estas plataformas permiten aplicar políticas consistentes, como la obligatoriedad del cifrado de disco completo, la aplicación de parches de seguridad críticos en un plazo estricto (ejemplo: menor a 7 días) y la capacidad de borrado remoto de la información corporativa en caso de que un dispositivo sea comprometido. Para un control más específico, se debe implementar un control de periféricos basado en la clasificación de los datos y bloquear la sincronización de datos corporativos hacia almacenamientos en la nube personales o dispositivos no gestionados.

1.3. RED Y ACCESO REMOTO

Tradicionalmente, el acceso remoto se ha basado en Redes Privadas Virtuales (VPN). Si bien una VPN crea un túnel cifrado, su modelo a menudo otorga un acceso amplio a toda la red corporativa. Este enfoque de "confianza implícita" crea un riesgo significativo de movimiento lateral para un atacante.

Por ello, la industria se está moviendo hacia un modelo de Zero Trust (Confianza Cero), cuyo principio es "nunca confiar, siempre verificar". En lugar de dar acceso a la red, se otorga acceso fragmentado y por sesión únicamente a las aplicaciones específicas que el usuario necesita, a través de soluciones de Zero Trust Network Access (ZTNA), reduciendo drásticamente la superficie de ataque. Cuando el uso de VPN es inevitable, se deben aplicar controles de segmentación estrictos y políticas "deny-all" por defecto (CCN-CERT, 2020). Adicionalmente, la implementación de DNSSEC (Domain Name System Security Extensions) es crucial para garantizar que los usuarios se conectan al sitio web legítimo, protegiéndolos de ataques de envenenamiento de caché DNS y redirecciones maliciosas (Cloudflare, s. f.; Akamai, 2025).

1.4. PROTECCIÓN DE DATOS Y APLICACIONES(SaaS)

Con el uso intensivo de suites colaborativas en la nube, la probabilidad de fuga de datos se concentra en estas plataformas. Las autoridades de protección de datos recomiendan un enfoque multifacético: clasificación y etiquetado de la información, asegurar el cifrado de datos en tránsito (TLS 1.3), e implementar soluciones de Prevención de Pérdida de Datos (DLP) en el correo, endpoints y aplicaciones SaaS (AEPD, 2020).

Medidas prácticas de alto impacto incluyen: prohibir enlaces de compartición públicos por defecto, establecer una fecha de caducidad automática para los accesos compartidos, revisar mensualmente los permisos en carpetas críticas y configurar alertas para detectar descargas masivas de archivos.

1.5. CULTURA Y CONCIENTIZACIÓN

Los controles técnicos más avanzados pueden ser insuficientes si no van acompañados de hábitos seguros por parte de los usuarios. Fomentar una cultura de seguridad robusta es un control en sí mismo. Se aconseja el desarrollo de campañas de formación breves, recurrentes y prácticas sobre riesgos del entorno doméstico ("hogar digital") y el reconocimiento de phishing.

Es igualmente importante establecer mecanismos sencillos para que los empleados reporten incidentes o correos sospechosos sin temor a represalias (Gobierno Digital de Chile, s. f.). Al transformar a cada empleado en un sensor activo, la organización gana una capacidad de detección temprana invaluable.

2. LINEAMIENTOS DE LA IMPLEMENTACIÓN

Una implementación exitosa es un programa continuo y estructurado. Un enfoque por fases permite gestionar recursos y demostrar valor de manera progresiva.

Fase 1 — Diagnóstico (4–6 semanas).

Para una primera fase de diagnóstico se propone la integración de un inventario de usuarios, dispositivos y aplicaciones para poder clasificar información sensible, además se propone la revisión de políticas de uso aceptable y definición de KPI base.

Una forma eficiente y eficaz para demostrar estos resultados sería la creación de una matriz de riesgos de acuerdo a los datos extraídos, además de un plan de tratamiento priorizado (INCIBE, 2020)

Fase 2 — Controles base (8–12 semanas).

En una segunda fase, la implementación de un MFA universal con anti-fatiga es primordial junto al endurecimiento de VPN o adopción de **acceso por aplicación (ZTNA/Proxy)**, cifrando o etiquetando los accesos a correo y SaaS.

Esto puede ser plasmado mediante una lista de políticas aprobadas, un tablero de cumplimiento o una baseline de configuración (AEPD, 2020; CCN-CERT, 2020)

Fase 3 — Profundización (continuo).

Para una tercera fase se recomienda profundizar o continuar con lo propuesto en la fase anterior, implementando revisiones de comparticiones en los SaaS, además de extender la seguridad para dominios críticos.

Algunos puntos recomendables para mostrar los resultados de esta fase podría ser un reporte de simulaciones con sus métricas de eficacia(Cloudflare, s. f)

Fase 4 — Mejora continua.

Por último, la fase posiblemente más importante, es la de mejora continua, ya que finalmente, ninguna de las implementaciones anteriores tiene sentido si no se busca una mejora continua en los sistemas de seguridad, esto se puede realizar acompañado de constantes revisiones gerenciales, el planteamiento de lecciones aprendidas, la reapreciación de riesgos y la actualización de contenidos de formación alineado con constantes con auditorías internas.

La creación de actas de revisión y cierres de hallazgos es primordial para llevar un seguimiento de estos puntos anteriores (Gobierno Digital de Chile, s. f.)

3. INDICADORES OPERATIVOS (KPI)

Para asegurar que los controles implementados no sean meramente teóricos, sino que contribuyan activamente a la reducción del riesgo, es imperativo establecer Indicadores Clave de Desempeño (KPI). Estos permiten una gestión basada en evidencia, demuestran el retorno de la inversión en seguridad y facilitan la mejora continua. La siguiente tabla propone un conjunto de indicadores de referencia para un entorno de teletrabajo seguro.

Dominio	Indicador	Meta de referencia	Observación
Identidad	Cuentas con MFA	≥ 98 %	Activar *number matching*
Endpoints	Equipos cifrados	100 %	Verificación por MDM/UEM
Parches	Tiempo medio parche crítico	≤ 7 días	Medir por SO
Acceso	Sesiones vía ZTNA (vs. VPN)	+20 pp trimestral	Migración por aplicación
Datos	Incidentes DLP bloqueados	Tendencia ascendente	Normalizar por volumen
DNS	Dominios propios con DNSSEC	100 %	Auditoría semestral
Cultura	Reporte vs. clic en phishing	> 1,5	Entrenamiento dirigido
Incidentes	MTTD / MTTR	Tendencia disminuible	Casos de uso remotos

CONCLUSIÓN

La seguridad en el teletrabajo mejora sustancialmente cuando la organización transita de un paradigma de defensa perimetral a uno que prioriza la identidad, el dispositivo y los datos, sustentado por políticas específicas, controles medibles y una ejecución por fases. El verdadero valor no reside en acumular recomendaciones, sino en operacionalizarlas a través de un programa estructurado, cuyos resultados sean validados con indicadores que demuestren la eficacia en la reducción del riesgo sin sacrificar la productividad.

Las guías en español de organismos como INCIBE, la AEPD y entidades públicas de Chile, ofrecen una base clara y sólida para implantar controles fundamentales. Con este enfoque integral, el teletrabajo deja de ser una excepción operativa y se consolida como un servicio gestionado, auditable y sostenible, permitiendo a la organización aprovechar sus beneficios de manera segura.

BIBLIOGRAFÍA

- Agencia Española de Protección de Datos. (2020). *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo* [PDF]. https://www.aepd.es/guias/nota-tecnica-proteger-datos-teletrabajo.pdf aepd.es

- Agencia Española de Protección de Datos. (2021, 19 julio). *Teletrabajo y protección de datos en el ámbito digital* (blog). https://www.aepd.es/prensa-y-comunicacion/blog/teletrabajo-y-pd-en-el-ambito-digital aepd.es

- Cloudflare. (s. f.). *¿Cómo funciona DNSSEC?* Recuperado el 4 de noviembre de 2025, de https://www.cloudflare.com/es-es/learning/dns/dnssec/how-dnssec-works/ cloudflare.com

- Gobierno Digital de Chile. (s. f.). *Guía Técnica de Seguridad de la Información y Ciberseguridad (GUI-CIBER-001)*. Recuperado el 4 de noviembre de 2025, de https://wikiguias.digital.gob.cl/guias/GU-CIBER-001 wikiguias.digital.gob.cl

- Semperis. (2023). *Cómo defenderse de los ataques de fatiga MFA* (es-ES). https://www.semperis.com/es/blog/active-directory-security/how-to-defend-against-mfa-fatigue-attacks/ Semperis

- Akamai. (2025, 11 abril). *¿Qué es DNSSEC y cómo funciona?* (es-ES). https://www.akamai.com/es/blog/trends/dnssec-how-it-works-key-considerations akamai.com

- Sahnoune, Z. S. (2025, 3 marzo). ISO 27001 frente a NIST 800-53: diferencias y similitudes clave. Security Compass. Recuperado 3 de noviembre de 2025, de https://www.securitycompass.com/blog/iso-27001-vs-nist-800-53/

- NQA [NQA]. (2022). ISO 27001:2022 GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. NQA. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

- National Institute of Standards and Technology. (2020). SP 800-53 Rev.5: Security and Privacy Controls… https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

- INCIBE. (2020, 15 de julio). Ciberseguridad en el teletrabajo: una guía de aproximación para el empresario. https://www.incibe.es/empresas/guias/ciberseguridad-en-el-teletrabajo-una-guia-de-aproximacion-para-el-empresario

- CCN-CERT. (2020, 30 de marzo). Teletrabajo: recomendaciones de seguridad y refuerzo de vigilancia. https://www.ccn-cert.cni.es/es/comunicacion-eventos/cibercovid19/teletrabajo.html