



Universidad Cenfotec

Maestría Profesional en Ciberseguridad

Documento Final de Proyecto de Investigación Aplicada 2

**PROPUESTA DE CIBERSEGURIDAD
PARA EL TELETRABAJO BAJO EL
MODELO DE CERO CONFIANZA**

Rodolfo Andrés Villalobos Rodríguez

ABRIL, 2022

Declaratoria de derechos de autor

Se declara que la siguiente investigación fue realizada por el autor único Rodolfo Andrés Villalobos Rodríguez, el investigador ha utilizado diferentes fuentes bibliográficas, con sus debidas referencias bibliográficas y citas en los diferentes capítulos de la investigación, respetando los derechos de autor de estas referencias. Además, se han utilizado diferentes datos recopilados por medio de una entrevista y encuestas, las cuales buscan poner en evidencia datos expertos o del público meta.

Se autoriza el uso total o parcial de esta investigación, para ser utilizada como referencia de investigación en trabajos futuros académicos o científicos, con la única condición de ser referenciado adecuadamente en las referencias.

Agradecimientos

Quisiera agradecer a todas las personas que han hecho posible este trabajo desde antes de empezar el curso y durante el desarrollo de la investigación mencionada:

Para empezar, me gustaría agradecer a mi madre, María de los Ángeles Rodríguez Rodríguez, y a mi abuelo, Carlos Rodríguez Murillo, que me han apoyado durante toda mi vida profesional y mi desarrollo como persona. Sin el apoyo de ninguno de los dos no estaría donde estoy el día de hoy.

A la Universidad Cenfotec y a mi tutor, Luis Alonso Ramírez Jiménez, por todo el proceso formativo, orientación y soporte que ha sido vital para llegar al desarrollo del trabajo de investigación. A mi tutor, por todas las recomendaciones durante el proceso de desarrollo que me han permitido desarrollar la investigación de una manera y exitosa.

Adicionalmente, a Saulo Machado, por su tiempo en la entrevista y por compartir su experiencia en el área de implementación de soluciones de ciberseguridad con clientes internacionales. Esto me permitió entender las necesidades de los diferentes clientes y negocios en la actualidad, además de brindarme una guía inicial para la investigación y sus limitaciones.

Aprobación final del Tribunal



Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad**, requisito para optar por el título de grado de **Maestría**, para el estudiante: **Villalobos Rodríguez Rodolfo**.

**Alonso
Ramírez**

Digitally signed by Alonso
Ramírez
Date: 2022.05.05 19:45:27
-06'00'

M. Sc. Luis A. Ramírez Jiménez
Tutor

M. Sc. Alejandro Bolaños Alpizar
Lector 1

**IGNACIO
TREJOS
ZELAYA
(FIRMA)**

Firmado digitalmente
por IGNACIO TREJOS
ZELAYA (FIRMA)
Fecha: 2022.05.06
08:39:45 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 29 de abril de 2022

Tabla de contenido

Capítulo I. Introducción.....	1
1.1. Generalidades.....	1
1.2. Antecedentes del problema.....	2
1.3. Definición y descripción del problema.....	4
1.4. Justificación	5
1.5. Viabilidad.....	6
1.5.1. Punto de vista técnico.....	6
1.5.2. Punto de vista operativo.....	6
1.5.3. Punto de vista económico.....	6
1.6. Objetivos.....	7
1.6.1. Objetivo general.....	7
1.6.2. Objetivos específicos.....	7
1.7. Alcances y limitaciones	8
1.7.1. Alcances.....	8
1.7.2. Limitaciones.....	8
1.8. Marco de referencia organizacional y socioeconómico.....	9
1.9. Revisión de literatura	9
1.9.1. Revisión sistemática.....	9
1.9.1.1. Formulación de la pregunta.....	9

1.9.1.2. Foco de la pregunta.	9
1.9.1.3. Amplitud y calidad de la pregunta.	9
1.9.1.3.1. Problema.	10
1.9.1.3.2. Pregunta.	10
1.9.1.3.3. Palabras clave y sinónimos.	10
1.9.1.3.4. Intervención.	11
1.9.1.3.5. Control.	11
1.9.1.3.6. Efectos.	11
1.9.1.3.7. Medida de salida.	11
1.9.1.3.8. Población.	11
1.9.1.3.9. Aplicación.	11
1.9.1.3.10. Diseño experimental.	11
1.9.1.4. Selección de fuentes.	11
1.9.1.4.1. Definición del criterio de selección de fuentes.	11
1.9.1.4.2. Lenguaje de estudio.	11
1.9.1.4.3. Identificación de fuentes.	12
1.9.1.4.3.1. Cadenas de búsqueda.	12
1.9.1.4.3.2. Lista de fuentes.	12
1.9.1.4.3.3. Comprobación de las fuentes.	12
1.9.1.4.4. Selección de los estudios.	12

1.9.1.4.4.1. Definición del criterio de inclusión y exclusión de estudios.	13
1.9.1.4.4.2. Procedimiento de selección de estudios.....	13
1.9.1.5. Ejecución de la revisión.	13
1.9.1.5.1. EBSCO.	13
1.9.1.5.2. IEEE Digital Library.....	13
1.9.1.5.3. IET Digital Library.	14
1.9.1.5.4. ACM Digital Library.	14
1.9.1.5.5. Web of Knowledge.	14
1.9.1.5.6. ELibro.	15
1.9.1.5.7. Google Scholar.	15
1.9.1.5.8. Research Gate.	15
1.9.1.5.9. Librarika.	16
1.9.2. Estado de la cuestión.....	16
Capítulo II. Marco conceptual.....	17
2.1. Cero confianza (Zero Trust)	17
2.1.1. Introducción.	17
2.1.2. NIST.....	17
2.1.2.1. Bases de la cero confianza.....	18
2.1.2.1.1. Principios de la cero confianza.	20
2.1.2.2. Componentes lógicos del modelo de cero confianza.	22

2.1.2.3. Variaciones del modelo de cero confianza.....	25
2.1.2.3.1. Cero confianza usando gobernanza de identidad mejorada.....	25
2.1.2.3.2. Cero confianza usando microsegmentación.....	26
2.1.2.3.3. Cero confianza usando la infraestructura de red y perímetros definidos por software.....	26
2.1.2.4. Variaciones de implementación para la arquitectura abstracta.....	26
2.1.2.4.1. Implementación de Agente/Gateway.....	26
2.1.2.4.2. Implementación basada en enclave.....	28
2.1.2.4.3. Implementación basada en el portal de recursos.....	29
2.1.2.4.4. Sandboxing de aplicaciones en dispositivos.....	31
2.1.2.5. Algoritmo de confianza.....	32
2.1.2.6. Escenarios de implementación y casos de uso.....	35
2.1.2.6.1. Empresas con instalaciones satélite.....	35
2.1.2.6.2. Empresas multinube/nube a nube.....	36
2.1.2.6.3. Empresas con servicios contratados o accesos para terceros.....	37
2.1.2.6.4. Colaboración entre límites de empresas.....	38
2.1.2.6.5. Empresas con servicios al públicos o clientes.....	39
2.1.2.7. Amenazas asociadas con el modelo de cero confianza.....	40
2.1.2.7.1. Alteración del proceso de decisión del modelo de cero confianza....	40
2.1.2.7.2. DoS o Interrupción de la red.....	40

2.1.2.7.3. Robo de credenciales/amenaza interna.	41
2.1.2.7.4. Visibilidad en la red.	41
2.1.2.7.5. Almacenamiento de información del sistemas y de la red.	42
2.1.2.7.6. Confianza en soluciones o formatos de datos propietarios.	42
2.1.2.7.7. Uso de entidades no personales (NPE, Non-Personal Entities) en la administración de cero confianza.	42
2.1.2.8. Modelo de cero confianza y posibles interacciones con servicios federados.	43
2.1.2.9. Migración a un modelo de cero confianza.	44
2.1.2.9.1. Modelos cero confianza puro.	44
2.1.2.9.2. Modelo híbrido de cero confianza y basada en perímetro.	45
2.1.2.9.3. Para introducir cero confianza a un modelo de red basado en perímetro.	45
2.1.3. Department of Defense (DoD).	49
2.1.3.1. Modelo de madurez.	50
2.1.3.2. Conceptos y principios de cero confianza.	51
2.1.3.3. Diagramas o flujos de datos.	55
2.2. Teletrabajo	59
2.2.1. NIST: Guía de Seguridad para el teletrabajo, acceso remoto y BYOD en las empresas.	59
2.2.1.1. Descripción de la seguridad del teletrabajo y acceso remoto organizacional.	61

2.2.1.1.1. Vulnerabilidades, amenazas y controles de seguridad.	61
2.2.1.1.2. Métodos de acceso remoto.....	63
2.2.1.1.2.1. Tunneling.	63
2.2.1.1.2.2. Portales de acceso.	64
2.2.1.1.2.3. Acceso por escritorio remoto.	65
2.2.1.1.2.4. Acceso directo a aplicaciones.	66
2.2.1.1.3. Recomendación claves.....	66
2.2.1.2. Seguridad para las soluciones de acceso remoto.	67
2.2.1.2.1. Acceso remoto: autenticación, autorización y control de acceso.	67
2.2.1.2.1.1. Autenticación.	67
2.2.1.2.1.2. Autorización.....	68
2.2.1.2.1.3. Control de acceso para redes de comunicaciones.	68
2.2.1.2.2. Recomendación claves.....	69
2.2.1.3. Seguridad del dispositivo cliente de teletrabajo.	69
2.2.1.3.1. Asegurando computadores personales para el teletrabajo.	70
2.2.1.3.2. Asegurando dispositivos móviles para el teletrabajo.....	71
2.2.1.3.3. Protegiendo información en dispositivos cliente en teletrabajo.	72
2.2.1.3.3.1. Encriptado de datos en reposo.	73
2.2.1.3.3.2. Respaldo de información de los dispositivos en teletrabajo.	73
2.2.1.4. Consideraciones de seguridad para un ciclo de vida de teletrabajo y acceso	

remoto.....	74
2.2.1.5. Recomendación de la NIST para los empleados realizando teletrabajo. ..	77
2.2.1.6. Consideraciones de seguridad para el intercambio de archivos en Internet.	79
2.2.1.6.1. Consideraciones de seguridad para mejorar el intercambio de archivos.....	79
2.2.1.6.2. Posibles soluciones para asegurar el intercambio de archivos.	80
2.2.1.6.3. Soluciones posibles para detectar el intercambio inadecuado de archivos protegidos.....	81
2.3. PCI	82
2.3.1. PCI Estándar de Seguridad de Datos.	83
2.3.1.1. Implementar y mantener sistemas y redes seguras bajo el cumplimiento de la PCI DSS.....	85
2.3.1.2. Como cumplir con la PCI DSS.....	94
2.4. OECD.....	95
2.4.1. Entendimiento de la seguridad digital de los productos: un análisis profundo.	96
2.4.1.1. Información clave para los creadores de políticas de seguridad.	96
2.4.1.2. Recomendaciones de la OECD en relación con la criptografía.	96
2.4.1.2.1. Pautas para políticas de criptografía.	97
2.4.1.3. Riesgo digital de seguridad.	98
2.4.1.3.1. Debilidades, vulnerabilidades y malas configuraciones.....	99

2.4.1.3.2. Amenazas, exploits y AIC (Availability, Integrity and Confidentiality).....	99
2.4.2. Mejorando la seguridad digital en los productos: una discusión de políticas. ..	99
2.4.2.1.1. Principios de las recomendaciones de la OECD en la gestión del riesgo de la seguridad digital.	100
2.5. ISO	100
2.5.1. ISO/IEC 27000:2018.....	100
2.5.1.1. Generalidades.	101
2.5.1.2. Seguridad de la Información.	101
2.5.1.3. ISMS (Information Security Management System).....	101
2.5.1.3.1. Implementando un ISMS.....	102
2.5.2. ISO/IEC 27001:2013.....	102
2.5.2.1. Fases de un SGSI basado en ISO27001.	102
2.5.2.2. Controles de la ISO27001.	103
2.6. GDPR.....	108
2.6.1. Transferencia de datos fuera de la UE.	109
2.6.2. Tratamiento de datos.	109
2.6.3. Violación de datos.....	109
Capítulo III. Marco metodológico.....	110
3.1. Tipo de investigación.....	110
3.2. Alcance investigativo.....	110

3.3. Enfoque de la investigación	110
3.4. Diseño de la investigación	111
3.5. Población y muestreo.....	112
3.6. Instrumentos de recolección	112
3.6.1. Encuesta.	112
3.6.2. Análisis documental.....	112
3.7. Técnicas de análisis de información	113
Capítulo IV. Análisis de resultados	114
4.1. Encuesta	114
4.1.1. Preguntas.....	114
4.1.2. Publicaciones.....	119
4.1.3. Resultados.	119
4.1.4. Conclusión de los resultados.....	129
4.2. Análisis documental.....	131
4.2.1. Estándares internacionales.	134
4.2.1.1. NIST.....	134
4.2.1.1.1. Autenticación.....	134
4.2.1.1.2. Administración de dispositivos.....	137
4.2.1.1.3. Almacenamiento de datos.....	138
4.2.1.2. ISO.....	140

4.2.1.2.1. Autenticación.....	140
4.2.1.2.2. Administración de dispositivos.....	141
4.2.1.2.3. Almacenamiento de datos.....	142
4.2.1.3. PCI.....	143
4.2.1.3.1. Autenticación.....	143
4.2.1.3.2. Administración de dispositivos.....	144
4.2.1.3.3. Almacenamiento de datos.....	145
4.2.1.4. Resultados.	146
4.2.2. Normativas internacionales.....	149
4.2.2.1. OECD.....	150
4.2.2.2. GDPR.....	150
4.2.2.3. Resultados.	151
4.2.3. Conclusión de los resultados.....	152
Capítulo V. Propuesta.....	156
5.1. Fase 1: Evaluación.....	160
5.1.1. Introducción.....	160
5.1.2. Propósito.....	161
5.1.3. Etapas.....	161
5.1.3.1. Inventario de sistemas.....	161
5.1.3.1.1. Introducción.....	161

5.1.3.1.2. Propósito.....	161
5.1.3.1.3. Procedimiento.....	161
5.1.3.2. Inventario de usuarios.	165
5.1.3.2.1. Introducción.....	165
5.1.3.2.2. Propósito.....	165
5.1.3.2.3. Procedimiento.....	165
5.1.3.3. Revisión de procesos de negocio.....	167
5.1.3.3.1. Introducción.....	167
5.1.3.3.2. Propósito.....	167
5.1.3.3.3. Procedimiento.....	168
5.2. Fase 2: Evaluación de riesgos y desarrollo de políticas.....	170
5.2.1. Introducción.	170
5.2.2. Propósito.	170
5.2.3. Etapas.....	170
5.2.3.1. Evaluación de riesgos.....	170
5.2.3.1.1. Introducción.....	170
5.2.3.1.2. Propósito.....	171
5.2.3.1.3. Procedimiento.....	171
5.2.3.2. Selección de controles.	174
5.2.3.2.1. Introducción.....	174

5.2.3.2.2. Propósito.....	174
5.2.3.2.3. Procedimiento.....	175
5.2.3.2.3.1. Identidad.....	175
5.2.3.2.3.2. Administración de dispositivos.....	176
5.2.3.2.3.3. Almacenamiento de datos.....	177
5.2.3.2.3.4. Otros recursos.....	178
5.2.3.2.3.4.1. Microsoft.....	178
5.2.3.3. Desarrollo de políticas.....	179
5.2.3.3.1. Introducción.....	179
5.2.3.3.2. Propósito.....	179
5.2.3.3.3. Procedimiento.....	179
5.3. Fase 3: Despliegue.....	180
5.3.1. Introducción.....	180
5.3.2. Propósito.....	180
5.3.3. Consideraciones.....	180
5.3.4. Etapas.....	181
5.3.4.1. Despliegue.....	181
5.3.4.1.1. Introducción.....	181
5.3.4.1.2. Propósito.....	181
5.3.4.1.3. Procedimiento.....	182

5.3.4.1.3.1. Consideraciones.....	183
5.3.4.1.3.2. Identidad.....	184
5.3.4.1.3.3. Administración de dispositivos.....	185
5.3.4.1.3.4. Almacenamiento de datos.....	187
5.3.4.2. Evaluación.....	188
5.3.4.2.1. Introducción.....	188
5.3.4.2.2. Propósito.....	189
5.3.4.2.3. Procedimiento.....	189
5.4. Fase 4: Operación y monitoreo.....	191
5.4.1. Introducción.....	191
5.4.2. Propósitos.....	192
5.4.3. Etapas.....	192
5.4.3.1. Operación.....	192
5.4.3.1.1. Introducción.....	192
5.4.3.1.2. Propósito.....	192
5.4.3.1.3. Procedimiento.....	192
5.4.3.2. Monitoreo.....	193
5.4.3.2.1. Introducción.....	193
5.4.3.2.2. Propósito.....	193
5.4.3.2.3. Consideraciones.....	194

5.4.3.2.4. Procedimiento.....	194
Capítulo VI. Conclusiones y recomendaciones.....	198
6.1. Expansión del modelo de cero confianza.....	198
6.2. Realidades del mercado.....	198
6.3. Soluciones.....	199
6.3.1. Cisco y Duo.....	200
6.3.2. Palo Alto Networks.....	201
6.3.3. Okta.....	202
6.3.4. Microsoft.....	202
6.3.5. Twingate.....	204
6.3.6. Illumio.....	204
6.3.7. Akamai.....	204
6.3.8. Unisys.....	204
6.3.9. Sysmantec.....	205
6.3.10. AppGate.....	205
6.4. Madurez organizacional.....	205
6.5. Arquitecturas basada en el modelo de cero confianza.....	207
6.6. Factibilidad en Costa Rica.....	208
Capítulo VII. Reflexiones finales.....	210
7.1. Modelo de cero confianza.....	210

7.2. Adopción de cero confianza en el mundo.....	211
Referencias bibliográficas	213
Glosario	222
Apéndices	230
Azure Active Directory, Zero Trust Access Control	230

Índice de tablas

Tabla 1 Palabras claves.....	10
Tabla 2 Estudios que se encontraron en Web of Knowledge	14
Tabla 3 Estudios encontrados en Google Scholar	15
Tabla 4 Controles NIST 1.....	134
Tabla 5 Controles NIST 2.....	137
Tabla 6 Controles NIST 3.....	138
Tabla 7 Controles ISO 1	140
Tabla 8 Controles ISO 2	141
Tabla 9 Controles ISO 3	142
Tabla 10 Controles PCI 1	143
Tabla 11 Controles PCI 2	144
Tabla 12 Controles PCI 3	145
Tabla 13 Resultados de los estándares internacionales estudiados	146
Tabla 14 Controles OECD.....	150
Tabla 15 Controles GDPR.....	151
Tabla 16 Resultados de las normativas internacionales estudiados	151
Tabla 17 Resultados finales.....	152
Tabla 18 Códigos de inventario de Sistemas.....	162
Tabla 19 Ejemplo de inventario de activos	163
Tabla 20 Ejemplo de inventario de aplicaciones	164
Tabla 21 Relación de aplicaciones y activos	165

Tabla 22 Códigos de inventario de sistemas y usuarios	166
Tabla 23 Información de usuarios	166
Tabla 24 Códigos de inventario de sistemas, usuarios y procesos	168
Tabla 25 Definición de código de departamento.....	169
Tabla 26 Definición de código de proceso	169
Tabla 27 Definición de código de procedimiento	169

Índice de ilustraciones

Ilustración 1 Modelo de acceso, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly).....	20
Ilustración 2 Modelo de componentes de cero confianza, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)	23
Ilustración 3 Implementación de Agente/Gateway, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)	28
Ilustración 4 Implementación basada en enclave, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)	29
Ilustración 5 Implementación basada en el portal de recursos, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)	30
Ilustración 6 Implementación de Sandboxing de aplicaciones en dispositivos, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)	31
Ilustración 7 Entradas del algoritmo de confianza, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)	32
Ilustración 8 Empresa con empleados remotos, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly).....	36
Ilustración 9 Caso de uso de multinube, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly).....	37
Ilustración 10 Empresa con usuario de terceros, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly).....	38
Ilustración 11 Colaboración entre límites de empresas, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)	39
Ilustración 12 Pasos del RFM, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly).....	46

Ilustración 13 Modelo de madurez del modelo de cero confianza, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)	51
Ilustración 14 Pilares de cero confianza, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)	53
Ilustración 15 Modelo Operacional, Etiquetado de datos, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021).....	56
Ilustración 16 Modelo Operacional, Cumplimiento de dispositivos, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)	57
Ilustración 17 Modelo Operacional: Análisis de Usuarios, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021).....	58
Ilustración 18 Modelo Operacional del DRM, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)	59
Ilustración 19 Mapa de Análisis de la información	113
Ilustración 20 Encabezado de encuesta	114
Ilustración 21 Pregunta n.º 1.....	115
Ilustración 22 Pregunta n.º 2.....	116
Ilustración 23 Pregunta n.º 3.....	117
Ilustración 24 Pregunta n.º 4.....	118
Ilustración 25 Pregunta n.º 5.....	119
Ilustración 26 Resultados pregunta n.º 1	122
Ilustración 27 Resultados pregunta n.º 2	124

Ilustración 28 Resultados pregunta n.º 3	125
Ilustración 29 Resultados pregunta n.º 4	127
Ilustración 30 Resultados pregunta n.º 5	129
Ilustración 31 Basado en el documento de la NIST y sus pasos documentados en el RMF	157
Ilustración 32 Ciclo de la mejora continua propuesta	160
Ilustración 33 Cuadrante de cero confianza Q3 2020.....	200
Ilustración 34 Cuadro que se basa en el modelo de madurez del DoD	206
Ilustración 35 Arquitectura basada en el modelo de cero confianza	207
Ilustración 36 Azure Active Directory: Zero Trust Access Control.....	230

Resumen

El COVID-19 ha incrementado la necesidad del teletrabajo, lo que obliga a las organizaciones a implementar este modelo para subsistir y seguir sus operaciones de negocio, de una manera más transparente y con una menor afectación. Además, este modelo permite cuidar a sus colaboradores del contagio. Esta última razón es una de las principales, ya que en muchas metodologías de recuperación de desastres el activo máspreciado de las organizaciones es el empleado y siempre se debe poner la vida humana de primero.

La investigación buscó proponer un diseño de cero confianza para el teletrabajo, ya que este puede incluir muchos escenarios o tecnologías. La propuesta cubre la identidad, la administración de estaciones de trabajo y los datos de usuario, además de considerar algunas de las recomendaciones y estándares internacionales.

Palabras clave: teletrabajo, trabajo remoto, cero confianza, Zero Trust.

Abstract

The COVID-19 has increased the necessity for remote work, which forces the organization to implement this model to subsist and continue their business operations, in the transparent way possible and with least impact. Furthermore, this model helps protecting their workforce of the disease exposure. This last reason is one the most important reasons, because many DR methodologies set the company workforce as the most valuable asset and put first the human life.

This research tries to propose a design of zero trust for the remote work, as it can include many scenarios and technologies. This proposal will cover identity, workstation administration and user data, and will consider some recommendation and international standards.

Keywords: Remote Work, Work from home, Zero Trust.

Capítulo I. Introducción

El trabajo desde casa o teletrabajo es una modalidad que no es nueva, muchas organizaciones no habían incursionado en esta por el apego a las modalidades tradicionales, usualmente por falta de confianza en los empleados o incluso por la falta de infraestructura. Aunque los países de primer mundo llevan varios años usando esta modalidad, en los países de tercer mundo algunas empresas medianas y pequeñas siguen esquemas más tradicionales de trabajo presencial donde, se trabaja por horario y no por objetivos y la confianza depositada en sus trabajadores es limitada.

Durante los últimos 2 años de la pandemia COVID-19 se ha impulsado el teletrabajo en muchas empresas y, de esta manera, adaptarse. Se puede afirmar que la pandemia ha impulsado la transformación digital en muchas empresas y esta ha sido más acelerada y bien recibida.

Esta transformación ha cambiado tabúes de la administración tradicional y ha probado que en muchos casos los empleados pueden trabajar de más. Además, ha traído otros beneficios como el recorte del gasto de alquileres y servicios públicos.

El problema para muchos especialistas con el trabajo desde casa es que la casa está en una zona gris. Muy pocas organizaciones se preocupan por instruir a sus empleados en prácticas seguras y muchos empleados pueden ser muy confiados al no estar conscientes de las consecuencias y riesgos. El ambiente de la casa implica más variables externas que el ambiente seguro o controlado de la oficina, esta nueva flexibilidad permite a los empleados trabajar desde un café u hotel, el teléfono, computadora personal o de trabajo.

1.1. Generalidades

Este documento busca generar una propuesta de ciberseguridad para el teletrabajo aplicable a cualquier organización basada en cero confianza y seguirá los estándares internacionales definidos por NIST, ISO y PCI. La solución pretende ser una guía para resolver algunos de los problemas de seguridad que han aumentado con la acelerada adopción del teletrabajo que impulsa la pandemia de la COVID-19 alrededor del mundo.

1.2. Antecedentes del problema

Se llevó a cabo una búsqueda en Librarika (biblioteca virtual de la Universidad Cenfotec) y no se encontró ninguna propuesta de teletrabajo. Se pudo encontrar propuestas para modelos generales de ciberseguridad en organizaciones, los cuales se amplían en el estado de la cuestión.

Se aplicó una entrevista a un especialista de seguridad de Microsoft, Saulo Machado, que trata con clientes que desean implementar soluciones de seguridad para teletrabajo y comentó que las soluciones que se utilizan actualmente están construidas o pensadas para ambientes On-Prem, algunos han recurrido a la VPN para establecer y asegurar la mayoría de sus comunicaciones entre los recursos de la organización y sus empleados.

Asimismo, comentó (Machado, comunicación personal, 2021) que muchas organizaciones han implementado soluciones AAD para autenticación segura, Intune para administración de dispositivos en Internet, SCCM que es una solución On-Prem, pero cuenta con una solución en la nube para manejar dispositivos Windows en Internet y, finalmente, soluciones DLP. Sin embargo, explica que muchas empresas adquieren estos productos para atacar problemas específicos y no para diseñar una solución integral y muchas veces se debe a desconocimiento de los riesgos, problemas tecnológicos o presupuesto. La mayoría de sus clientes en estos últimos 2 años han enfrentado los siguientes problemas:

- Reuniones en línea.
- Administración de equipos empresariales, BYOD, otros dispositivos móviles y sistemas operativos.
- Conectividad con aplicaciones y datos, de manera segura.
- Identidad y autenticación.

Machado (comunicación personal, 2021) explicó que las empresas del ámbito financiero y de telecomunicaciones son las que han logrado enfrentar estos retos, de una manera más eficiente, ya que muchas han adoptado tecnología avanzadas con anterioridad y han invertido en capacitación de personal. Muchas de estas organizaciones han buscado soluciones de CASB, Azure Information Protection y de DLP de perímetro. Esto se debe al

aumento de ataques cibernéticos durante estos últimos 2 años y que los antivirus tradicionales no sirven para estos ambientes híbridos.

Además, varios profesionales también destacan los problemas al administrar dispositivos remotamente y las grandes adquisiciones que muchas compañías tuvieron que hacer para hacer posible el WFH y, como afirma Meredith (2020), muchos de estos dispositivos no se desplegaron sin antes haber obtenido o haber aplicado las políticas de seguridad de la organización y cuántos de estos dispositivos pueden parchearse desde Internet o de forma remota y, adicionalmente, darle visibilidad a los administradores de los parches aplicados o cuántos empleados saben el proceso que deben seguir para que sus máquinas estén seguras. Meredith (2020) también explica que muchas organizaciones tuvieron que tomar decisiones apresuradas por la falta de equipos o presupuesto y permitieron la política de BYOD si una evaluación o configuración adecuada.

- Almacenamiento en la nube: así como lo explica Meredith (2020), muchas organizaciones han eliminado estas plataformas por problemas en el momento de establecer contraseñas seguras y cómo se comparten muchos de estos archivos y a quiénes.
- Redes de casa: Meredith (2020) también indica que podría ser importante para una organización plantear la posibilidad de proveer a sus empleados con dispositivos seguros y configurados por la organización o con ayuda de un especialista, ya que muchos de estos dispositivos pueden ser obsoletos o pueden tener configuraciones por defecto no seguras.

Para finalizar, los cibercriminales han visto más oportunidades de éxito con estos ambientes desatendidos y sin monitoreo. Thales (2021) analizó una encuesta aplicada por 451 Reseach a 2600 profesionales de seguridad y líderes. Según este artículo un 86 % de los entrevistados está preocupado por los riesgos o amenazas de seguridad de los empleados que trabajan de forma remota. Esto se deriva de un aumento percibido del 53 % en ataques de *ransomware* y 38 % en ataques cibernéticos. Existe una preocupación de dónde están los datos de la organización, solo el 23 % tiene conocimiento de dónde están almacenados sus datos, de los cuales el 20 % cifra sus datos en la nube; ese 20 % posiblemente no cifra todos sus datos por rendimiento y presupuesto. Un 49 % de las personas encuestadas expresó haber

tenido una brecha de seguridad. Si se estudia el Data Threat Report de Latam (Thales, 2021) realizado por la misma compañía expresa que de las personas encuestadas solo el 24 % se siente preparado para manejar los riesgos de seguridad causados por la pandemia. El mismo reporte comparte que el 28 % ha adoptado formalmente una política de cero confianza y el 71 % confía en esta arquitectura de seguridad.

1.3. Definición y descripción del problema

Los cambios sociales y tecnológicos actuales han impulsado el cambio del trabajo tradicional de oficina y los ha transformado en ambientes híbridos de cotrabajo o de teletrabajo, donde los empleados podrían trabajar desde cualquier lugar, no necesariamente desde casa como afirma su nombre en inglés Work From Home. Muchas organizaciones no saben o han fallado al afrontar este reto tecnológico y cultural en su organización.

Los cambios en el modelo de trabajo han aumentado los puntos de ataque para cibercriminales y también han reducido el nivel de control que las organizaciones solían tener sobre sus dispositivos. Esto ha despertado incertidumbre en cuanto al uso y la ubicación de los dispositivos empresariales, su nivel de parcheo para vulnerabilidades conocidas o su cumplimiento con las políticas empresariales de seguridad. También ha despertado otras preocupaciones de seguridad como el uso de la data que reside fuera y dentro de la organización y como se maneja, finalmente, se han visto obligados a confiar en sus empleados por falta de control sobre las acciones de sus empleados en ambientes no seguros.

No solo se han despertado muchas dudas por las organizaciones y sus administradores, también se han materializado muchos de los miedos de estas. Durante estos últimos 2 años de pandemia se ha podido observar un aumento de ciberataques y es que el trabajo desde casa ha ingresado nuevas variables, según la presentación de Cisco en Vancouver del 2020 (CISCO, 2020) el *malware* en IoT ha aumentado en un 300 %, lo que facilita los ataques a red del hogar. No solo nuevas variables son aprovechadas por cibercriminales, las contraseñas débiles son un problema, según el mismo reporte un 81 % de los ataques de cuentas de usuarios se han que se lleva a cabo con contraseñas robadas o débiles. Ambas situaciones dan a entender las posibilidades de robo de información y de contaminación de *malware* en dispositivos, tanto de la organización como ajenos. Otra táctica

que también ha aumentado es el *phishing*, la cual también puede utilizarse para robar información personal, empresarial y credenciales. Este método de ataque ha visto una gran oportunidad en temas que se relacionan con la COVID-19 (Kaspersky Team, 2021).

Adicionalmente, el trabajo desde casa aumenta las posibilidades de robo de activos, ya que pone en riesgo los dispositivos empresariales y la información almacenada en el activo, no solo por redes o dispositivos inseguros. Según Nabe (2020), cerca de un 47 % de los empleados puede ser víctima de un ataque de *phishing* mientras trabaja desde casa, también indica que cerca de 500 000 usuarios han sido afectados por brechas de información en plataformas de videoconferencias. Nabe (2020) indica que durante la pandemia se han incrementado los nuevos ataques, de un 20 % a un 35 % (nuevos vectores o códigos de ataque), además indica que la perspectiva de la ciberseguridad ha cambiado con estos cuatro puntos:

- Los empleados maliciosos que trabajan desde casa con menos supervisión y controles técnicos.
- Los cibercriminales están conscientes de que las medidas de seguridad en la data no son adecuadas o suficiente robustas en la mayoría de las empresas.
- Las actividades de hacktivismo se han incrementado.
- Los *hackers junior* ven la oportunidad de probar habilidades en esta nueva realidad por la falta de controles.

Muchos de los problemas descubiertos durante la investigación preliminar no tienen soluciones aisladas, la propuesta de seguridad, bajo el enfoque de cero confianza, ofrece soluciones para estos problemas.

1.4. Justificación

El teletrabajo puede ser la nueva realidad para muchas organizaciones en el ámbito mundial y muchas podrían no regresar a modelos tradicionales. La necesidad de propuestas aplicables a cualquier organización será grande, ya que no cuentan con especialistas en ciberseguridad o pueden no entender los retos que enfrentan las empresas al trabajar en esta modalidad. La propuesta busca ofrecer una solución aplicable a cualquier organización y

que contemple los problemas capturados durante la investigación. Además, se pretende presentar una propuesta para la implementación del modelo de cero confianza en ambientes de teletrabajo, enfocado principalmente en identificación de usuarios, administración de dispositivos y protección de data de usuarios, asimismo, sigue los estándares internacionales que le permitirán desarrollar una solución aplicable en organizaciones de cualquier ámbito, en proceso de certificación o certificadas.

1.5. Viabilidad

A continuación, se define la viabilidad de esta propuesta.

1.5.1. Punto de vista técnico. Se posee la capacidad técnica profesional para desarrollar la propuesta utilizando la documentación de cero confianza de la NIST y alinearla con los estándares internacionales como la normativa de GDPR, ISO 27000 y PCI, además de seguir las recomendaciones definidas por la OECD. En esta investigación no se realiza una implementación, ya que es solamente una propuesta.

1.5.2. Punto de vista operativo. Esta propuesta consiste en un diseño de seguridad para el teletrabajo bajo la modalidad de cero confianza, solo se precisa de la documentación para desarrollar de la propuesta, la cual en el futuro podrá utilizarse como referencia para una posterior implementación por parte de terceros. Se aclara que es posible llevar a cabo esta propuesta sin alterar el funcionamiento operativo de ninguna empresa durante el desarrollo de la investigación. Se pueden utilizar personas de cualquier empresa o área para obtener datos estadísticos para la investigación.

1.5.3. Punto de vista económico. El desarrollo de esta propuesta no requiere de la compra o alquiler de ningún equipo, licencia, componente o artefacto. La propuesta se desarrolla en horas de consultoría e investigación, bajo un esquema teórico donde el autor asume el costo. Cabe destacar que el desarrollo de la propuesta no representa ningún costo real a una organización, por lo tanto, el costo teórico será asumido por la persona investigadora.

Como referencia del costo potencial del desarrollo, se usa el salario mínimo establecido por el Gobierno de Costa Rica, así se puede definir el costo mínimo de la investigación. Se aclara que el grado académico más alto previsto por el decreto de salarios

mínimos es el de licenciatura como afirma el Decreto 42748-MTSS y 42923-MTSS (MTSS, 2021), publicado en la Gaceta 295 y 119, Alcances 332 y 123, del 17 de diciembre del 2020 y del 22 junio del 2021 respectivamente que entró en vigor el 1 de enero del 2021, el salario bruto correspondiente es de ₡682.607,23 mensuales.

Se estima que la investigación y desarrollo de la propuesta dura 4 meses (1 cuatrimestre) y se invertirán cerca de 20 horas semanales, lo cual da un resultado de 16 semanas (promedio de semanas por mes 4) por 20 (horas destinadas semanales) para un total de 320 horas. Como aproximado al costo por hora, se procede a dividir ₡682.607,23 entre 160 (160 horas; promedio de días trabajados mensuales [20], multiplicado jornadas de 8 horas como establece la ley), cual da un total de ₡4.266,29 por hora. El resultado de 320 horas a un costo de ₡4.266,29 es de ₡1.365.212,8. Se puede afirmar que el desarrollo de la propuesta tendría un costo mínimo de ₡1.365.212,8.

1.6. Objetivos

Este trabajo de investigación define sus objetivos utilizando la Taxonomía de Bloom creada en 1956, se utiliza esta taxonomía, ya que cuenta con respaldo internacional y, aunque existen nuevas versiones de esta, la original es la más aceptada. Entre sus beneficios está la facilidad de dar congruencia a los objetivos, además de dar una idea clara de la intensidad y alcance en la investigación, ya que permite definir objetivos específicos claros para cumplir el objetivo general.

1.6.1. Objetivo general. Diseñar una propuesta de ciberseguridad para el teletrabajo basada en el modelo de cero confianza limitada a identificación de usuarios, administración de dispositivos y protección de data de usuarios, que sea aplicable para cualquier organización en Costa Rica, sin importar su índole comercial, sector productivo y si es una organización pública o privada.

1.6.2. Objetivos específicos. A continuación, se definen los objetivos específicos:

1. Reconocer los puntos importantes de ciberseguridad para esta propuesta bajo el modelo de cero confianza de los estándares internacionales de la NIST, ISO y PCI.

2. Revisar las normativas de GDPR y OECD en el contexto de ciberseguridad con el enfoque de cero confianza.
3. Identificar los problemas, necesidades y retos de ciberseguridad que muchas organizaciones y sus colaboradores enfrentan en sus actividades diarias con una metodología de teletrabajo o trabajo remoto.
4. Elegir los controles técnicos necesarios para resolver los problemas que se identifican durante la investigación siguiendo los estándares y normativas internacionales, a partir del modelo cero confianza.
5. Justificar los controles seleccionados y la aplicación del modelo de cero confianza con el desarrollo de esta investigación.

1.7. Alcances y limitaciones

A continuación, se definen los alcances y limitaciones.

1.7.1. Alcances. El trabajo de investigación busca proponer el modelo de cero confianza como solución de ciberseguridad para el teletrabajo, el cual comprende los siguientes ámbitos, identidad, administración de dispositivos remotos y data de usuarios. La propuesta está dentro del contexto nacional (Costa Rica) sigue los estándares y normativas internacionales.

1.7.2. Limitaciones. A continuación, se definen las limitaciones del proyecto:

1. La investigación no se implementa en ninguna organización ni entrega un manual para su implementación debido a la complejidad de la infraestructura de cada organización, se limita a seleccionar los controles necesarios dentro del modelo de cero confianza y alinearlos con las estándares y normativas internacionales.
2. Se limitará a los problemas que se identifican durante la investigación en las áreas Identidad, administración de dispositivos y data de usuarios. Aceptando la realidad tecnológica y rápido cambio, así como el surgimiento de nuevas tendencias en ciberseguridad y cibercrimen.

3. La investigación se enfoca en computadoras empresariales (estaciones de trabajo móviles) y no en dispositivos móviles como teléfonos inteligentes o similares, ya que esta propuesta está pensada para una nueva adopción y no para empresas donde ya existen plataformas de acceso externo o servicios móviles.

1.8. Marco de referencia organizacional y socioeconómico

Como se detalló, el trabajo de investigación entrega una propuesta aplicable para cualquier organización de Costa Rica, por lo que no existe una referencia organizacional o socioeconómica que considerar como parte de la investigación.

1.9. Revisión de literatura

El término cero confianza no es nuevo, su primera mención fue el 2010 (Cloudflare, s. f.), desde entonces ha sido aplicado en diferentes ámbitos tecnológicos, por lo que cabe destacar que la selección de documentos técnicos se lleva a cabo solo para los cuales sean relevantes para el desarrollo de la investigación, utilizando de base los alcances y limitaciones definidos anteriormente.

1.9.1. Revisión sistemática. Para la revisión sistemática se utiliza la metodología sugerida por la universidad, la cual establece un esquema para revisión sistemática con un enfoque a la ingeniería de *software* (Pedreira, Piattini, Luaces y Brisaboa, 2007).

1.9.1.1. Formulación de la pregunta. Se procederá a formular la pregunta para delimitar exitosamente los resultados. Se sabe que cero confianza puede nombrarse Zero Trust en inglés y que se utiliza ampliamente en tecnología, por lo que teletrabajo, trabajo remoto, Work From Home y similares son palabras clave para delimitar la búsqueda.

1.9.1.2. Foco de la pregunta. Se requieren documentos técnicos de modelos de cero confianza implementados en ambientes de teletrabajo. También se consideran casos de éxito o experiencias, ya que pueden ser beneficiosas para la investigación y entender sus beneficios y deficiencias.

1.9.1.3. Amplitud y calidad de la pregunta. En esta sección se listan los términos clave para llevar a cabo una búsqueda asertiva y pertinente. Esta pregunta debe responder el problema definido en la definición del problema de la investigación.

1.9.1.3.1. *Problema.* La poca preparación de las organizaciones al enfrentar los retos tecnológicos que ha presentado la pandemia de la COVID-19 con referencia a la seguridad en el teletrabajo. El trabajo de investigación está enfocado en el uso del modelo de cero confianza para resolver estos problemas y, específicamente, en términos de identidad, administración de dispositivos móviles y data de usuarios.

1.9.1.3.2. *Pregunta.* Con el problema anterior sintetizado, se construye la siguiente pregunta:

- ¿Qué propuestas se han llevado a cabo con el modelo de cero confianza para el teletrabajo?

1.9.1.3.3. *Palabras clave y sinónimos.* A continuación, se listan las palabras identificadas como clave para llevar a cabo la búsqueda de libros, tesis, documentos y artículos, con alguna relación con la investigación y que puedan considerarse. Se utilizarán palabras en inglés debido a que es un modelo utilizado ampliamente en Estados Unidos. Se utiliza la Tabla 1 para listar las palabras clave y sus traducciones en inglés:

Tabla 1

Palabras claves

Palabra clave sinónimo	Traducción en inglés
Cero confianza	Zero Trust
Propuesta	Proposal
Implementación	Deployment
Diseño	Design
Teletrabajo	Work from home (WFH)
Teletrabajo	Work from home (WFH)

Trabajo desde casa

Work from home (WFH)

Trabajo remoto

Work from home (WFH)

1.9.1.3.4. Intervención. Leer y considerar los resultados en el marco del uso del modelo de cero confianza y los alcances de la investigación, así como si la información adicional en estos documentos se considera pertinente a criterio del investigador. Esto con el fin de extraer los documentos de relevancia para el desarrollo del proyecto.

1.9.1.3.5. Control. Se aclara que no se cuenta con ninguna base de datos y la búsqueda empieza desde cero.

1.9.1.3.6. Efectos. Se espera encontrar casos de uso del modelo de cero confianza, mas no propuestas específicas del modelo para el teletrabajo. Lo cual puede brindar una idea de la adopción para estos problemas en particular.

1.9.1.3.7. Medida de salida. Se utilizan medios conocidos y se evita el uso de motores de búsqueda para obtener documentos serios de carácter investigativo o técnico y la revisión de su contenido se hace por parte de la persona investigadora.

1.9.1.3.8. Población. La población meta son organizaciones de cualquier carácter en Costa Rica, pero para la revisión bibliográfica se utilizan documentos de carácter global.

1.9.1.3.9. Aplicación. Esta investigación puede ser puesta en práctica por administradores en sistemas o especialistas en seguridad.

1.9.1.3.10. Diseño experimental. Se realiza un análisis de los documentos obtenidos durante la búsqueda sistemática y se clasifican con base en su relevancia para la investigación.

1.9.1.4. Selección de fuentes. *Definición del criterio de selección de fuentes.* Se toman en cuenta repositorios conocidos de tecnología, gracias a su respaldo global. Algunos podrían necesitar contraseñas o ser repositorios privados de organizaciones globales con acceso a partir del modelo de suscripción.

1.9.1.4.2. Lenguaje de estudio. Como se detalló, se utilizan palabras en español e

inglés.

1.9.1.4.3. Identificación de fuentes. Cadenas de búsqueda. Las cadenas de búsqueda utilizan las palabras reservadas que utilizan la mayoría de los motores de búsqueda *and* y *or*, también búsquedas sin estas, ya que muchos motores de búsqueda funcionan mejor sin esas palabras clave o ya no utilizan estas palabras reservadas. Cadenas de búsqueda:

1. (“Propuesta” OR “Implementación” OR “Diseño”) AND “Cero Confianza” AND (“Tele trabajo” OR “Teletrabajo” OR “Trabajo desde casa” OR “Trabajo remoto”).
2. (“Proposal” OR “Deployment” OR “Design”) AND “Zero Trust” AND (“Work from home” OR “WFH”).

1.9.1.4.3.2. Lista de fuentes. Debido a su credibilidad y trayectoria se han considerado como fuentes válidas y profesionales las siguientes:

1. EBSCO, <https://www.ebsco.com/es/bibliotecas-academicas>
2. IEEE Digital Library, <https://ieeexplore.ieee.org/document/6461145>
3. IET Digital Library, <https://digital-library.theiet.org/>
4. ACM Digital Library, <https://dl.acm.org/>
5. Web of Knowledge, <https://login.webofknowledge.com/>
6. eLibro, <https://elibro.com/>
7. Google Scholar, <https://scholar.google.com/>
8. Research Gate, <https://www.researchgate.net/>
9. Librabrika, <https://ucenfotec.librarika.com/>

1.9.1.4.3.3. Comprobación de las fuentes. Se toman en cuenta los documentos que estén bien documentados y con fuentes externas creíbles. Investigaciones con fuentes colaborativas como Wikipedia y similares se desechan.

1.9.1.4.4. Selección de los estudios. A continuación, se define la selección de estudios

para este proyecto.

1.9.1.4.4.1. Definición del criterio de inclusión y exclusión de estudios. Todos los documentos que se encontraron deben estar relacionados con la aplicación del modelo de *cero confianza* con el *teletrabajo*, los trabajos no que se relacionan con los dos temas se excluyen. Se puede considerar aplicaciones del modelo, investigación, implementación y propuestas.

1.9.1.4.4.2. Procedimiento de selección de estudios. Se siguen los siguientes pasos para llevar a cabo una búsqueda eficaz:

1. Se utiliza la búsqueda avanzada si está disponible y filtros adicionales que cada motor puede ofrecer.
2. Se utilizan las cadenas de búsqueda, con o sin las palabras reservadas.
3. Si se obtuvieran más de 30 resultados se puede limitar más la búsqueda de ser necesario.
4. Se rescatan y evalúan los resultados. Finalmente, se repite este proceso en cada una de las fuentes listadas anteriormente.

1.9.1.5. Ejecución de la revisión. A continuación, el proceso que se lleva a cabo en cada fuente listada.

1.9.1.5.1. EBSCO. EBSCO no cuenta con búsqueda avanzada, se procedió primero a busca el modelo en discusión, no se obtuvieron resultados utilizando *cero confianza* o *Zero Trust*, por lo cual se descarta esta fuente.

1.9.1.5.2. IEEE Digital Library. IEEE tiene la opción de búsqueda avanzada y del uso de las palabras reservadas de búsqueda. Se procede primero a llevar a cabo la búsqueda en español y, posteriormente, en inglés. Ambas búsquedas retornaron 31 resultados.

Se analizaron los documentos y, aunque mucho son interesantes y *teletrabajo* o el modelo de *cero confianza* se enfocan o aplican en otros ámbitos, también se encuentran ensayos del teletrabajo en tiempos de COVID-19, pero de manera muy general, por lo que los resultados quedan excluidos según el criterio definido.

1.9.1.5.3. *IET Digital Library*. Se procede a realizar la búsqueda avanzada, las opciones son muy limitadas, por cual se empieza con *cero confianza* y *Zero Trust*, lo cual solo genera cuatro resultados.

Se revisaron los resultados, pero ninguno está relacionado con el modelo de cero confianza por lo que se descartan todos los resultados de esta fuente.

1.9.1.5.4. *ACM Digital Library*. Se utilizaron las cadenas de búsqueda en español primero y después en inglés, el sitio *web* no permite la cláusula *Or* se optó por combinar las palabras y hacer búsquedas independientes por cada *Or*. Se obtuvieron 41 resultados individuales en total.

Los cuales todos se descartaron en su totalidad, ya que ninguno estaba utilizando la metodología de cero confianza y solo dos documentos hablaban de dispositivos móviles, pero no tenían el enfoque deseado para esta investigación.

1.9.1.5.5. *Web of Knowledge*. Se utilizó la búsqueda avanzada, pero no tiene la capacidad de utilizar varias palabras en la cadena de búsqueda. *Cero confianza* no devolvió ningún resultado, pero *Zero Trust* devolvió 24,000+ resultados, se utilizaron más palabras de la cadena de búsqueda, lo cual redujo los resultados a 3,000+ y se procedió a revisar los primeros 50 resultados.

De los 50 primeros resultados solo uno se seleccionó, según lo definido en el criterio de selección. En la Tabla 2 se Detalla su información:

Tabla 2

Estudios que se encontraron en Web of Knowledge

#	Título	Autores	Año	URL
1	Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home	Sudakshina Mandal; Danish Ali Khan; Sarika Jain	2021	https://publons.com/publon/47951129/

1.9.1.5.6. *ELibro*. Esta fuente no posee la opción de búsqueda avanzada, por lo que se empezó con *cero confianza* y *Zero Trust*, posteriormente se agregó un filtro para temas que se relacionan con informática y afines. No obstante, no se pudo encontrar nada relacionado con el modelo de cero confianza. Esta fuente ha sido descartada, ya que ningún resultado cumple el criterio.

1.9.1.5.7. *Google Scholar*. Esta fuente no cuenta con búsqueda avanzada y no entiende las palabras reservadas, por lo que se procedió a realizar búsquedas independientes por cada *Or*, ya que los resultados de *cero confianza* y *Zero Trust* eran muchos y no se contaba con filtros adicionales, de igual manera, se obtuvieron más de 30 resultados, por lo que se optó por revisar los primeros 50. Durante la revisión se pudieron observar documentos consultados, adicionalmente uno encontrado en Web of Knowledge, el cual fue el único resultado válido según los criterios de selección.

Tabla 3

Estudios encontrados en Google Scholar

#	Título	Autores	Año	URL
1	Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic	Sudakshina Mandal; Danish Ali Khan; Sarika Jain	2021	https://link.springer.com/content/pdf/10.1007/s00354-021-00130-6.pdf

1.9.1.5.8. *Research Gate*. Esta fuente no tiene búsqueda avanzada, pero permite el uso de las palabras reservadas, se procedió a ingresar las cadenas de búsqueda creadas. Hubo cuatro resultados una vez ejecutadas ambas búsquedas; ninguno de los resultados se relaciona

con el criterio de búsqueda establecido.

1.9.1.5.9. Librarika. Finalmente, se hizo la búsqueda en el catálogo de la universidad. No tiene búsqueda avanzada y no permite el uso de operadores de búsqueda. No hubo resultados en *Zero Trust* o *cero confianza*. Por esto, esta fuente se descartó.

1.9.2. Estado de la cuestión. Después de la revisión del documento se descartó, el Abstrac y el título parecían indicar que era aplicable para la investigación, pero no cubre ninguno de los temas seleccionados y solo se enfoca en la configuración de la red de una organización en términos generales.

Capítulo II. Marco conceptual

2.1. Cero confianza (Zero Trust)

A continuación, define el modelo de cero confianza o Zero Trust.

2.1.1. Introducción. El modelo de cero confianza no es una idea nueva, ha existido por mucho más tiempo del que se podría suponer. La Agencia de Defensa en Sistemas de Información (DISA) había publicado parte de una estrategia para moverse de la seguridad basada en perímetro de red a un modelo de transacciones individuales, le dieron el nombre de BCORE (Black Core). Posteriormente, en 2004 en un foro de Jericho se empezó hablar de este tema y darle forma (Gartner, 2021) para obtener su nombre en 2010 por John Kindervag analista de Forrester Research Inc. quien nombró el modelo por primera vez (Cloudflare, s. f.). Posteriormente, en 2014 Google anunció la adopción de este modelo en la seguridad de su red y desde entonces desarrollo BeyondCorp su solución de cero confianza para redes (Google, s. f.). En 2019 Gartner lo enlistó como componente clave para varias soluciones de seguridad en tecnología.

El trabajo de investigación se enfoca en la aplicación de cero confianza para el teletrabajo, con énfasis en identidad de usuarios, manejo de dispositivos y seguridad de data de usuarios. Se utiliza la documentación desarrollada por la NIST y el Departamento de Defensa de los Estados Unidos, por lo que el marco teórico está basado principalmente en la publicación de la NIST 800-207 (Rose, Borchert, Mitchell y Connelly, s. f.) y el documento de Referencia del Modelo de Cero Confianza (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021) y otras fuentes que se consideren importantes.

2.1.2. NIST. La NIST define el modelo de cero confianza como una estrategia de seguridad que mueve el foco de la seguridad basada en perímetros de red a un enfoque basado en usuarios, activos y recursos. Las organizaciones han crecido en complejidad, ya no hay una sola red, ahora las organizaciones tienen su infraestructura local, trabajadores remotos, otras oficinas con sus propias redes y servicios en la nube, lo cual hace que la seguridad basada en un perímetro de red sea un reto, ya que no es fácil identificar todos los perímetros.

Cero confianza se basa en el principio de asumir que no hay confianza implícitamente dada a cuentas de usuarios y activos por su ubicación física o su ubicación en la red organizacional, por ejemplo, dispositivos en la red interna o Internet o dispositivos empresariales o propios del usuario. El proceso de autenticación y autorización, a nivel de usuario o dispositivo, debe suceder antes de dar el acceso a los recursos empresariales sin importar estas condiciones, sin dar confianza adicional a ninguno. Cero confianza se creó como respuesta a nuevas tendencias empresariales, como usuarios remotos, BYOD o dispositivos en la nube que no se encuentran dentro de esta red empresarial. Cero confianza asume que un atacante está presente en el ambiente y que el ambiente empresarial no es diferente, por lo tanto, no merece confianza adicional. Además, reutiliza algunos conceptos como Least Privilege, la cual busca asegurar que los usuarios tienen los accesos necesarios y no más de los que necesitan para su trabajo, además de establecer un análisis continuo para asegurar lo mismo, combinado con continua autenticación y autorización.

Cero confianza busca establecer principios en los que no se confía en la red interna y busca bloquear el acceso indebido a la información y limitar el movimiento lateral. El uso del modelo de cero confianza no es simplemente una solución de mercadotecnia es un modelo de principios, procesos y soluciones tecnológicas enfocadas en un caso de uso.

2.1.2.1. Bases de la cero confianza. Cero confianza es un conjunto de conceptos e ideas diseñados para minimizar la poca certeza que pueda existir en cualquier situación y siempre aplicando los mismos procedimientos para reforzar la certeza de una transacción. Esto lo logra utilizando una política de mínimo acceso por solicitud de acceso en sistemas de información y servicios, asumiendo que se trabaja en una red comprometida. El modelo utiliza conceptos de cero confianza para relación de componentes, planificación de los flujos de trabajo y políticas de acceso, además, se puede afirmar que es un grupo de controles y políticas operacionales.

Parte fundamental de una implementación exitosa en una organización para minimizar las incertezas es enfocarse en autenticación y autorización, además de minimizar las zonas de confianza implícita y minimizar retrasos en los mecanismos de autenticación. Otra clave es crear reglas de acceso lo más granular posible, esto permite reforzar las políticas

de acceso mínimo. La NIST brinda el siguiente diagrama donde se usa un PDP (Policy Decision Point) o un PEP (Policy Enforcement Point), donde el acceso es dado por ambos.

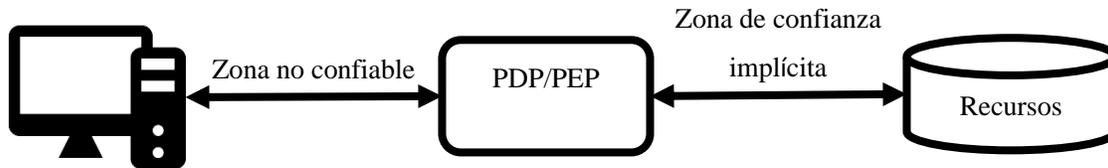


Ilustración 1

Modelo de acceso, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

Los sistemas deben asegurar que el sujeto es auténtico y que la solicitud es válida. El PDP y PEP utilizan las políticas de acceso para juzgar si el sujeto puede acceder los recursos que solicita. Esto debe asegurar que cero confianza cumple las dos áreas básicas de autenticación y Autorización. Las políticas de acceso deben evaluar el nivel de confianza sobre un sujeto, como su nivel de confianza, factores por considerar para cambiar su nivel de confianza (hora, ubicación, estatus, etc.), esto obliga a muchas organizaciones a mantener y desarrollar políticas dinámicas, lo cual asegura que se adapten al ambiente actual y a los recursos. Asimismo, ayuda a no confiar en sujetos que han pasado la autenticación base (Logging). Existe una Implicit Trust Zone o zona de confianza implícita que representa todas las entidades que son confiables a cierto nivel por el PDP o PEP, lo que quiere decir que todo aquel que puede pasar el PDP o PEP tiene el mismo nivel de confianza, esta zona debe ser lo más pequeña posible.

2.1.2.1.1. Principios de la cero confianza. La NIST menciona que hay mucha discusión sobre si la cero confianza debería remover los conceptos de seguridad perimetral (como *firewall*) o trabajar en conjunto y define los siguientes principios basados en los consensos internacionales. Se aclara que no todos estos principios deben aplicarse completamente, pero deben existir en un ambiente de cero confianza y dependen de la estrategia de la empresa.

1. Todas las fuentes de información y de servicios informáticos se consideran recursos, una red está compuesta de muchos tipos de dispositivos que envían y reciben información, servicios de *software* y otras funciones. Se deben incluir dispositivos personales que tienen algún nivel de acceso a los recursos de la organización.

2. Toda comunicación debe asegurarse sin importar su ubicación en la red, la ubicación de la red no implica confianza y los dispositivos dentro de la red empresarial deben cumplir con los mismos requerimientos de seguridad que dispositivos fuera de esta.
3. El acceso a recursos empresariales individuales es dado por sesión, se debe evaluar el nivel de confianza en el sujeto antes de brindar acceso, por lo que se debería autenticar y autorizar nuevamente. El acceso debe darse utilizando la política del mínimo privilegio y no debería dar acceso a otro recurso o por un tiempo superior al deseado.
4. El acceso a los recursos lo determina una política dinámica que puede incluir el comportamiento del sujeto o atributos del ambiente, las organizaciones protegen recursos definiendo qué recursos tienen y cuáles sujetos pueden acceder a ellos y qué nivel de acceso requieren estos sujetos para esos recursos. En cero confianza la identidad del cliente puede incluir la cuenta de usuario y otros atributos asignados por la empresa, entre ellos puede estar el estado del dispositivo como versiones de *software* instalado, ubicación de la red, fecha, comportamientos anteriores y credenciales; también se pueden capturar atributos de comportamiento como desviaciones de uso, análisis del dispositivo, análisis del sujeto y otros. Las políticas pueden basarse en todos o algunos de estos atributos y se definen, finalmente, por las necesidades de negocio y el nivel de riesgo aceptable definido.
5. La empresa monitorea y mide la integridad o postura de seguridad de todos los dispositivos de la empresa y asociados con la red, ningún activo tiene confianza heredada. La organización evalúa la postura de seguridad de los dispositivos cuando este hace una solicitud a un recurso. Las empresas que han implementado cero confianza deben establecer un Sistema de Diagnóstico y Mitigación Continuo (CDM) o sistemas similares de monitoreo que den detalles del estado de dispositivos y aplicaciones, además de que permita aplicar parches cuando sea necesario. Esto permite detectar dispositivos que no sigan las políticas empresariales o tengan vulnerabilidades conocidas o que simplemente no se

manejen por la organización, incluso se puede tratar a estos dispositivos de manera diferente cuando tratan de acceder a la red organizacional. Esto también ayudaría a detectar los dispositivos ajenos a la organización y cómo deben tratarse.

6. Toda autenticación y autorización de recursos es dinámica y estrictamente obligatoria antes de permitir el acceso a los recursos, esto debe establecer un ciclo de solicitudes de acceso constantes, escaneos, evaluación de amenazas, adaptaciones y evaluación constante de confianza en una comunicación activa. Una organización que está implementando cero confianza debería tener manejo de identidad, credenciales y administración de accesos (ICAM), además de tener administración de activos. Esto debería incluir MFA (Multifactor Authentication, autenticación de factores múltiples) para el acceso de algunos o todos los recursos empresariales. Es clave tener monitoreo continuo con una posible reautenticación y reautorización, como lo defina la política obligatoria de la organización.
7. La organización deberá recolectar toda la información posible acerca del estado actual de los activos, la red y las comunicaciones para utilizarla al generar la postura de seguridad del activo. La organización deberá capturar información del activo, así como su postura de seguridad, tráfico de red, solicitudes de accesos, data procesada o cualquier otra información necesaria para mejorar la creación y cumplimiento de las políticas establecidas. Además, puede utilizarla para permitir acceso a recursos.

2.1.2.2. Componentes lógicos del modelo de cero confianza. La documentación de la NIST muestra un modelo conceptual y sus relaciones, debajo de la ilustración la descripción de cada uno:

- Componentes adicionales: estos componentes pueden informar y dar políticas adicionales que pueden utilizarse por parte del PE al tomar decisiones.
 - Continuous Diagnostics and Mitigation (CDM) System: el CDM o Sistema de Diagnóstico y Mitigación Continuo obtiene información acerca de los dispositivos de la organización como su estado, además, ayuda con la actualización de su configuración y *software*. Ayuda brindando información al PE acerca del sistema operativo de la máquina, su integridad, así como que esté ejecutando *software* aprobado por la organización y que no tenga ninguna vulnerabilidad conocida. El CDM es el encargado de aplicar las políticas en dispositivos no empresariales y que se encuentran activos en la red de organización.
 - Sistema de cumplimiento industrial: este componente pretende evaluar que la organización este en cumplimiento regulatorio con el régimen industrial al cual pertenece. Esto debe incluir todas las políticas que la organización haya desarrollado para asegurar su cumplimiento.
 - Feed de inteligencia de amenazas: provee información de fuentes internas o externas que ayudan al PE a tomar decisiones. Esto puede representarse por muchos servicios que obtienen información de muchas fuentes y revelen datos de nuevos ataques y vulnerabilidades, así como fallas de *software* o nuevo *malware*. Todo esto también debería utilizarse por parte del PE para lograr una evaluación correcta.
 - Registros de actividad de red y sistemas: este sistema debería agregar entradas de registro para cada activo, acciones de acceso a recursos y otros eventos que den un estado en tiempo real de la postura organización en seguridad.
 - Políticas de acceso a datos (Data Access Policies): estos son atributos, reglas y políticas para el acceso a los recursos empresariales. Estos recursos pueden administrarse con una interfaz de administración o generadas dinámicamente por el PE. Estas políticas pueden utilizarse como el punto inicial para autorizar

acceso a recursos. Estas políticas deben ser definidas bajo la misión de cada role y necesidades de la organización.

- Enterprise Public Key Infrastructure (PKI): PKI o la infraestructura de llave pública soporta la creación y generación de certificados, además de registrar los certificados creados a recursos, sujetos, servicios y aplicaciones. Esto incluye no solo a la empresa también puede incluir una autoridad de certificados globales o federada.
- Sistema de administración de ID (ID Management System): este sistema es responsable de crear, guardar y mantener las cuentas de usuarios y los registros de identidad de la organización (usualmente un servidor LDAP o de Active Directory). Este sistema contiene la información necesaria de un sujeto y otras características empresariales como el rol, accesos, correo electrónico, certificados, etc.
- Security Information and Event Management (SIEM) System: el SIEM o sistema de gestión de eventos e información de seguridad recolecta información de seguridad, de manera centralizada, para un análisis posterior. Esta información se utiliza para refinar las políticas y advertir a la organización de posibles ataques a organización.

2.1.2.3. Variaciones del modelo de cero confianza. Según la NIST todas las organizaciones deben aplicar los principios establecidos anteriormente, pero puede utilizar uno o dos para definir sus políticas o modelo de cero confianza. Las soluciones completas de cero confianza deberán incluir elementos de los tres enfoques que se explican a continuación, a saber, la gobernanza de identidad mejorada, microsegmentación y segmentación basada en la red.

2.1.2.3.1. Cero confianza usando gobernanza de identidad mejorada. Este enfoque utiliza la identidad de los actores como el componente principal para la creación de las políticas, se puede afirmar que si no hay más solicitudes de acceso a recursos no habría necesidad de políticas. Las políticas de acceso se basan en la identidad y los tributos asignados y el requerimiento primario para acceder a los recursos se basa en los privilegios

de acceso dados a un sujeto, utilizar otros factores pueden afectar el nivel de confianza o restringirlo y modificar su nivel de acceso.

Este modelo por lo general se utiliza junto con modelos de redes abiertas o redes empresariales con acceso a visitantes y similares. Esto significa que, de alguna forma, el acceso a la red se da inicialmente a todos los dispositivos, pero el acceso a los recursos empresariales es restringido solo para las identidades con los niveles acceso apropiados. Una desventaja de dar acceso a la red es que actores maliciosos podrían intentar un ataque, lo cual implica que las organizaciones necesitarán de monitoreo y respuesta para esos incidentes.

2.1.2.3.2. Cero confianza usando microsegmentación. Una organización podría implementar cero confianza con base en la ubicación de recursos individuales o grupos en un segmento de red protegido por algún componente de seguridad como un *gateway*. En este enfoque las organizaciones ponen dispositivos como *switches* inteligentes, *firewalls* o algún *gateway* que actúa como un PEP y protege este grupo de recursos. Además, la organización puede utilizar agentes de *software* o agentes de *firewall*.

Este enfoque necesita que los componentes del PEP sean administrados y capaces de reaccionar o reconfigurarse como sea necesario al responder contra una amenaza. Una de sus desventajas son las complicaciones de implementar muchos o varios *gateways* u otros dispositivos, además de los altos costos de administración.

2.1.2.3.3. Cero confianza usando la infraestructura de red y perímetros definidos por software. Este último enfoque usa la infraestructura de red para implementar el modelo de cero confianza. Utilizan SDN (Software Defined Networks, redes definidas por *software*) e IBN (Intent-based Networking). El PA actúa como un controlador de red que se instala o reconfigura basada en decisiones hechas por el PE. El cliente sigue pidiendo acceso por medio del PEP, el cual se maneja por el PA.

2.1.2.4. Variaciones de implementación para la arquitectura abstracta. Implementación de Agente/Gateway. En este modelo de implementación el PEP está dividido en dos componentes que están en el cliente o antes del cliente. Por ejemplo, un cliente puede tener un cliente que direcciona el tráfico al PEP y el Gateway puede ser el responsable de las comunicaciones con el PA sigue las rutas de comunicación configuradas.

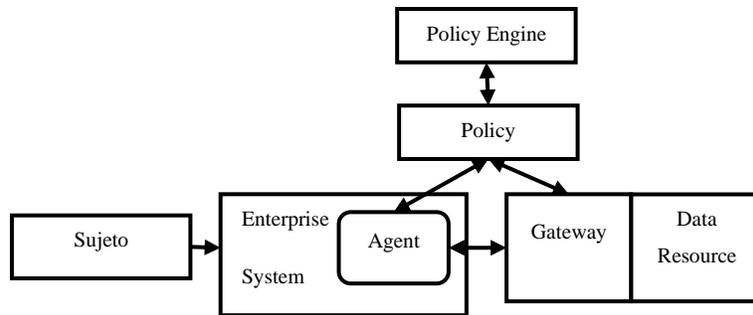


Ilustración 3

Implementación de Agente/Gateway, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

Típicamente, en un escenario donde un sujeto con una *laptop* de la organización y que desee conectarse empezará con una solicitud de acceso que es tomada por el agente local en la máquina, este reenviará esta solicitud al PA. El PA y el PE que puede ser un componente empresarial local o un servicio hospedado en la red, el PA enviará esta solicitud al PE para evaluación. Finalmente, si la solicitud es autorizada el PA configurará el canal de comunicación entre el agente del dispositivo y el *gateway* del recurso en solicitud. Este canal o sesión puede incluir información como la IP, información de puertos, llave de sesión o artefactos similares. Una vez establecida la sesión entre el dispositivo y el *gateway* ambos se conectan y se encripta la transmisión de datos. Esta sesión posteriormente terminará cuando lo indique por el flujo de trabajo o por ejecución del PA en caso de algún problema de seguridad o política.

Este modelo es generalmente utilizado en empresas donde se tiene una administración de dispositivos robusta y también para empresas con servicios en la nube. Lo más importante para esta investigación es que este modelo no se utiliza con BYOD, ya que el acceso solo es posible por medio del agente, el cual debe estar solo en dispositivos organizacionales.

2.1.2.4.2. Implementación basada en enclave. Este modelo de implementación es una variación del modelo de agente/*gateway*. Una de las diferencias es que en este el *gateway* no está en el dispositivo, sino en el límite del grupo (enclave) del recurso, un buen ejemplo puede ser el centro de datos de la organización.

Por lo general en este modelo los recursos tienen una sola función de negocio o no pueden contactarse directamente por el *gateway*. Este modelo de implementación puede ser útil para empresas que utilicen microservicios hospedados en la nube para un solo proceso de negocio. En este modelo usualmente toda la nube privada se localiza detrás del *gateway*.

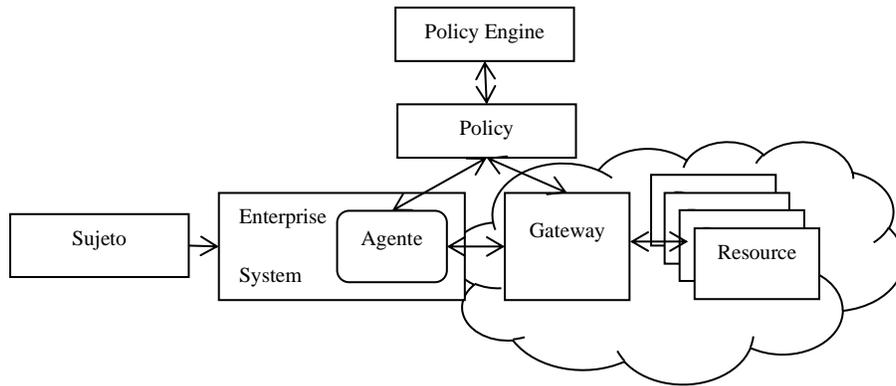


Ilustración 4

Implementación basada en enclave, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

Es posible encontrar implementaciones híbridas de este modelo junto con el modelo de agente/*gateway*. En este modelo de implementación los activos empresariales tienen un agente que se utiliza para conectarse con el *gateway* del enclave y las conexiones se crean de la misma manera que en el modelo de implementación de agente/*gateway*.

Este modelo es útil para organizaciones que tienen aplicaciones viejas (también conocidas como Legacy) o centros de datos locales (también conocidos como On-Premises) que no puede tener *gateways* individuales. Se necesita un programa de administración de activos y configuración para instalar y configurar los agentes. El lado negativo es que el *gateway* protege una colección de recursos y no puede proteger a los recursos individualmente y podría permitir accesos no deseados.

2.1.2.4.3. Implementación basada en el portal de recursos. En este modelo de implementación el PEP es un solo componente que actúa como *gateway* para la solicitud de un sujeto. El portal del *gateway* puede ser para un recurso individual o para asegurar a un enclave para una colección de recursos que se utilizan para alguna función de negocio. Un ejemplo es el uso de un Portal de *gateway* en una nube privada o Centro de Datos con

aplicaciones viejas (Legacy).

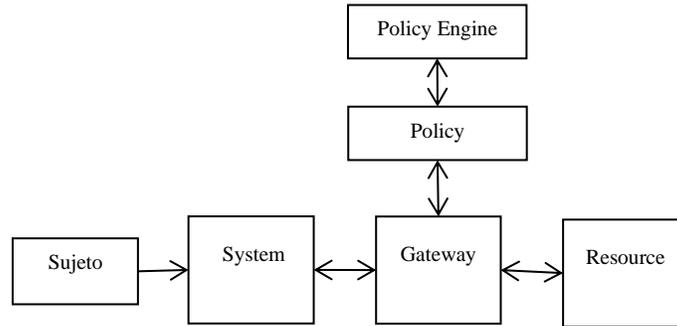


Ilustración 5

Implementación basada en el portal de recursos, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

El beneficio primario de este modelo sobre los expuestos es que el componente de *software* no necesita estar instalado en todos los dispositivos empresariales o no empresariales. Por esto, este modelo es suficientemente flexible para ambientes donde se utiliza el modelo BYOD o políticas interorganizacionales (empresas terceras). Por esto, los administradores organizacionales no tienen ninguna necesidad de asegurar que todas las máquinas tienen este agente para poder comunicarse con el PA o un *gateway*, lo cual también limitará la información que es posible solicitar de los dispositivos. Este modelo solo puede analizar y escanear activos y dispositivos una vez que están conectados al portal del PEP y es posible que no pueda monitorearlos continuamente u obtener información como si está infectada, si tiene alguna vulnerabilidad, si necesita alguna actualización o si tiene la configuración adecuada.

La diferencia principal con este modelo es que no hay un agente local, entonces no puede manejar las solicitudes locales y la organización solo puede tener información de ellas cuando estas se conectan al PEP, justamente como sucede en los ambientes de trabajo remoto. Este modelo también podría permitir ataques al portal del PEP si es descubierto, por lo tanto, lo hace vulnerable a ataques de DoS (Denial of Service). Esto implica que la organización necesita proteger el portal del PEP en contra de ataques DoS o proveerle la suficiente disponibilidad para que no se vea afectado y tener un plan de contingencia para cualquier problema con el servicio de red.

2.1.2.4.4. *Sandboxing de aplicaciones en dispositivos*. Es otra variable del modelo de implementación de agente/*gateway* y trata de mantener las aplicaciones examinadas (o aplicaciones confiables) en procesos virtualizados dentro de la máquina (Sandbox), lo cual evita que los procesos tengan acceso directo a la máquina. Esto se puede llevar a cabo de muchas maneras, por ejemplo, máquinas virtuales, *containers*, entre otros. No importa el método de Sandbox, el objetivo debe ser siempre el mismo y es proteger a la aplicación o a las instancias de esta de un *host* que pueden estar comprometidas.

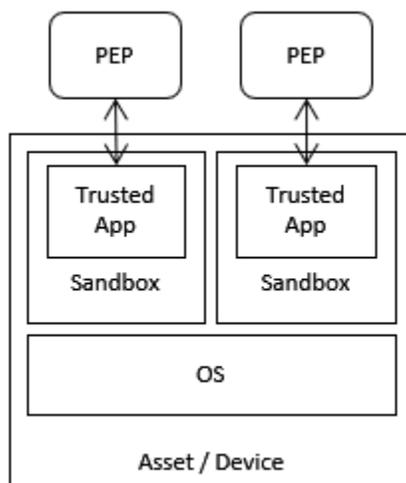


Ilustración 6

Implementación de Sandboxing de aplicaciones en dispositivos, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

En la Ilustración 6 se muestra un escenario donde un dispositivo está ejecutando aplicaciones confiables en un Sandbox, las aplicaciones pueden comunicarse con el PEP, pero otras aplicaciones se rechazan al tratar de negociar con este. El PEP podría ser local o estar en la nube.

La ventaja principal de este modelo de implementación es que las aplicaciones están separadas del dispositivo, por lo que el no escanear vulnerabilidades del dispositivo no debería ser un problema, ya que deberían estar protegidas de un potencial *malware* en el activo. Una de las desventajas es que la organización debe mantener todas estas aplicaciones para todos los activos, adicionalmente, no tendrán visibilidad completa sobre las máquinas clientes. Otro punto que se puede mencionar es que la organización no solo tiene que

mantener y soportar las aplicaciones también debe garantizar que son seguras, lo cual requiere más esfuerzo que solo monitorear.

2.1.2.5. Algoritmo de confianza. Para un modelo de cero confianza el algoritmo de confianza representa el proceso de validación que ejecuta el PE. El PE utiliza este algoritmo para aprobar o denegar el acceso a un recurso empresarial. El PE utiliza información de muchas fuentes como la base de datos de los sujetos, ahí podrá obtener información de los atributos y roles del sujeto, patrones históricos de comportamiento, estas fuentes pueden incluir datos de amenazas actuales, entre otras.

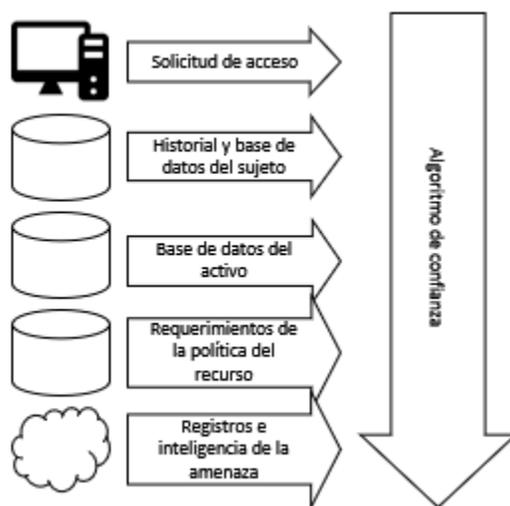


Ilustración 7

Entradas del algoritmo de confianza, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

Como se puede ver en la Ilustración 7 las categorías podrían dividirse de la siguiente manera con base en la información que dan:

- Access Request (Solicitudes de acceso): es la solicitud de acceso del sujeto, podría contener información principal del solicitante como la versión de sistema operativo, *software* utilizado, el nivel de actualización, entre otros. Por lo general con esta información, la postura de seguridad del dispositivo y otros datos podrían permitir o denegarle el acceso al dispositivo.

- Subject Database (información del sujeto en la base de datos): es la información del sujeto que solicita acceso a los recursos (Puede ser humano, físico o virtual), esto podría incluir otros atributos del sujeto. La identidad del usuario puede ser una combinación de datos lógicos y otros resultados de autenticación realizados por el PEP. Los atributos pueden utilizarse para determinar el nivel de confianza e incluir tiempo y ubicación para determinarla. Los atributos tienen información de los privilegios y roles del sujeto en un momento dado. Toda esta información debe estar disponible en el sistema de administración de ID y la base de datos de políticas. Algunas veces se puede almacenar información del comportamiento de un sujeto o variaciones.
- Asset Database (Información del Activo en la Base de datos): esta base de datos contiene la información conocida del activo y su estatus. Esto podría incluir información como versión del sistema operativo, *software* instalado, integridad, locación (geográfica y en la red) y nivel de actualización. Esta información se puede utilizar para comparar los cambios de información de un activo y restringir o denegar el acceso de ser necesario.
- Resource Requirements (requerimientos del recurso): los requerimientos pueden ser representados por un grupo de políticas y estas políticas también pueden complementar la información con el ID de usuario y los atributos en la base de datos del sujeto, el objetivo principal de este grupo de políticas es definir un grupo de requerimientos mínimos para acceder un recurso. Estos requerimientos pueden utilizarse para definir el nivel mínimo de autenticación para acceder un recurso, por ejemplo, solicitar MFA (autenticación de multifactor) para acceder algunos recursos o cuando algunos sujetos se encuentren en ciertas ubicaciones. Estos requerimientos deberían ser desarrollados por el custodio de los datos y el responsable del proceso que utilice los datos.
- Threat Intelligence (Información de inteligencia de Amenazas): se representa por lo general con un *feed* o una lista viva de información general y específica de amenazas y *malware*. Esta información se puede utilizar por muchos otros servicios y puede mostrar información externa e interna, esto podría incluir

descubrimientos nuevos o data de información anterior, así como firmas de ataques, vectores de ataques y pasos de mitigación. Usualmente, es información generada por fuentes externas y no por la organización.

La importancia de cada fuente de información la determina o configura la organización. El PE y el PA utiliza esta información para evaluar la solicitud y el PA configura el PEP para habilitar las comunicaciones con estas políticas. Existen dos maneras de manejar la evaluación o administración la TA, el primer punto se basa en la evaluación de factores y el segundo es cómo la solicitud se evalúa con base en otras evaluaciones del mismo sujeto.

- Criterios *versus* basado en evaluación: la evaluación basada en los criterios asume un conjunto de atributos que deben cumplirse antes de dar acceso a un recurso o permitir una acción determinada. Estos criterios de evaluación los configura la empresa y deben ser configurados independientemente para cada recurso. El acceso es dado a un recurso solo si todos los criterios se cumplen. Cuando se utiliza la Evaluación el TA calcula el nivel de confianza con base en los valores para cada fuente de datos y la importancia asignada por la organización a cada una de estas fuentes. Si la calificación es mayor que la configurada por la empresa para el recurso se permite el acceso o la acción deseada que el sujeto solicita, de otra manera, la solicitud se rechaza o el nivel de acceso se reduce.
- Singular *versus* contextual: el método de evaluación singular hace que la TA trate cada solicitud de manera individual y no tome en consideración el historial del sujeto antes de hacer la evaluación. Este método permite que la evaluación suceda de manera rápida, pero existe una probabilidad de que algún ataque pase desapercibido en caso de que suceda desde algún sujeto que ha sido permitido. Un TA con evaluación contextual toma la información histórica de un sujeto en contexto cuando se lleva a cabo la evaluación de una solicitud de acceso. Con este segundo método el PE debe mantener información del estado de todos los sujetos y aplicaciones, pero tiene más probabilidades de detectar a un atacante cuando utiliza credenciales comprometidas, por medio de detecciones atípicas de comportamiento. Esto también significa que el PE debe ser informado por el PA

y PEP desde comportamiento e interacciones del sujeto al haber algún tipo de comunicación. Este modelo de análisis del comportamiento de los sujetos puede crear un modelo aceptable de uso e identificar desviaciones para llevar a cabo algún control adicional o denegar el acceso.

Ambos puntos pueden utilizarse de maneras diferentes y estos deben ser definidos por la organización y por los datos que la organización posea para soportar las decisiones. Idealmente el TA debe ser contextual, ya que es el que mitiga la mayoría de las amenazas, pero muchas organizaciones pueden usar metodologías mixtas para equilibrar seguridad, usabilidad y costo-eficacia. Desarrollar los criterios o definir la importancia de las fuentes de información requiere planificación y testeo y este proceso por lo general es difícil y puede generar muchos problemas adicionales cuando se empieza la implementación de cero confianza.

2.1.2.6. Escenarios de implementación y casos de uso. Cualquier organización puede diseñar un ambiente con los principios de cero confianza en mente y es posible que muchas ya tengan elemento de cero confianza en la infraestructura de la organización, ya que muchos de estos se alinean con prácticas de seguridad de la información y políticas de resiliencia. Cualquier organización se puede beneficiar de estos principios, las raíces de cero confianza se enfocan en organización geográficamente distribuidas o con una fuerza de trabajo móvil.

2.1.2.6.1. Empresas con instalaciones satélite. El escenario más común involucra una ubicación principal y una o más locaciones geográficas que no están conectadas físicamente por una misma red empresarial y algunos empleados pueden no estar en esa red y necesitan acceder a algunos de los recursos empresariales. Estas organizaciones pueden tener algún tipo de *link* entre las ubicaciones principales y las demás locaciones, pero puede que no tenga la capacidad de manejar todo el ancho de banda, pueden tener empleados teletrabajando fuera de estas locaciones con equipos empresariales o propios, lo cual implica que la compañía debe poner a disposición algunos recursos en Internet o fuera de la red empresarial principal.

En este caso de uso el PE/PA generalmente se hospeda como un servicio en la nube y los clientes por lo general tienen un cliente instalado o por medio de portal de recursos. Por lo general el PE/PA no se hospeda localmente para evitar que el tráfico sature la red.

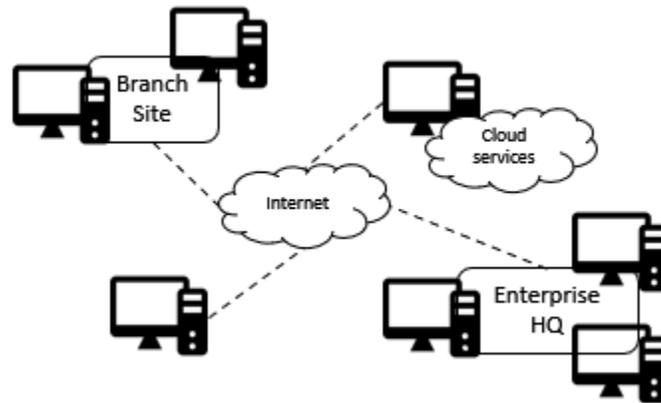


Ilustración 8

Empresa con empleados remotos, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

2.1.2.6.2. *Empresas multinube/nube a nube.* Este es un modelo en aumento y es donde las organizaciones utilizan nubes de proveedores múltiples. La organización tiene una red local y utiliza al menos dos proveedores de servicios en la nube para hospedar aplicaciones, servicios o datos, en otros casos puede que datos y aplicaciones estén en proveedores independientes y ambas deban conectarse directamente.

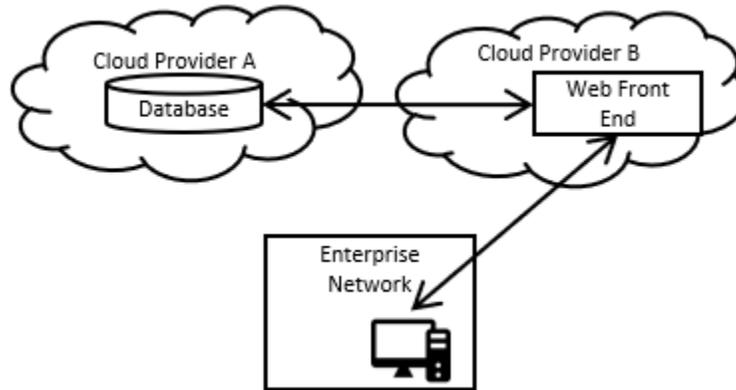


Ilustración 9

Caso de uso de multinube, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

Este caso de uso es una implementación de servidor a servidor en proveedores de nube distintos, como es posible ver en la Ilustración 9 ambos se encuentran fuera del perímetro de seguridad, lo cual puede ser un problema para metodologías de seguridad tradicionales. La solución de cero confianza para estos escenarios es colocar el PEP en el punto de acceso para cada aplicación/servicio y fuente de datos. El PE/PA puede ser un servicio en alguna de ambas nubes o en una tercera nube. El cliente (sea por portal o agente) puede acceder al PEP directamente. Algo posiblemente negativo es que los diferentes proveedores tienen distintas maneras de implementar funcionalidades similares, por lo que requiere que el arquitecto organizacional conozca estas diferencias y cómo se pueden implementar.

2.1.2.6.3. Empresas con servicios contratados o accesos para terceros. Este es un escenario común donde una empresa tiene visitas en sitio u otros servicios subcontratados que requieren acceso a algunos recursos empresariales para llevar a cabo su trabajo. Esto significa que el modelo de cero confianza debe proveer acceso a dispositivos no empresariales cuando visitan las instalaciones y limitar el acceso solo a los recursos que estos necesitan.

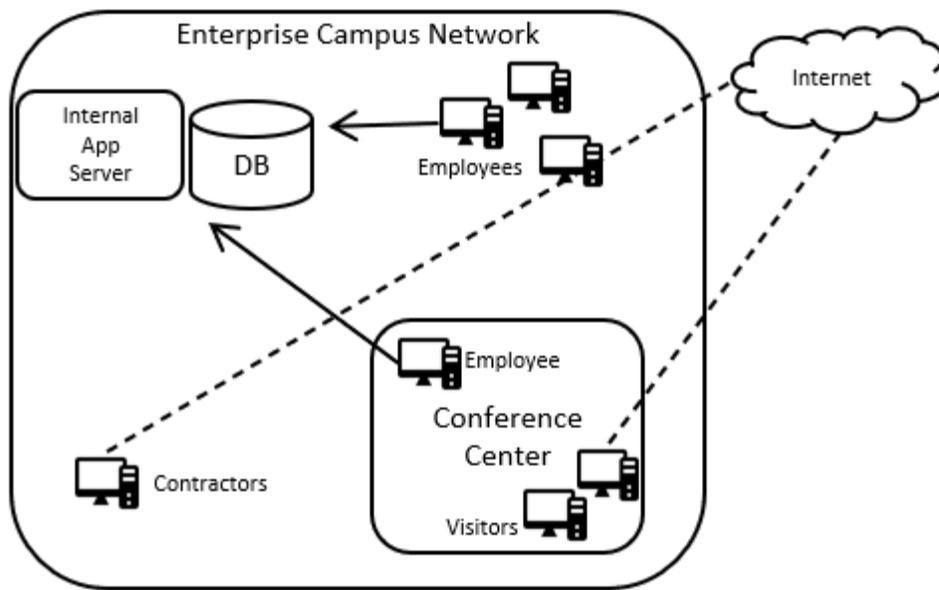


Ilustración 10

Empresa con usuario de terceros, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

En la Ilustración 10 se pueden observar empleados de otras empresas y visitantes que podrán tener acceso a Internet y tal vez a algunos de los recursos empresariales. Si fuera necesario, los empleados que se ubiquen en una misma ubicación que los visitantes podrán tener una experiencia transparente sobre los recursos empresariales que ocupen.

Para este caso, la PE/PA puede estar en la nube o en la LAN (en caso de no tener o poseer pocos recursos en la nube), la organización puede tener agentes o portales de acceso para los sujetos y, finalmente, la PA/PE se asegura de que todos los activos ajenos a la empresa no puedan acceder a los recursos locales, también puede limitarlos y solo permitir el acceso al Internet.

2.1.2.6.4. Colaboración entre límites de empresas. Este caso de uso es para la comunicación entre empresas, aplica para dos empresas independientes o federadas y los recursos de la empresa A solo pueden ser utilizados por un grupo de usuarios de la empresa B. La empresa A en algunos casos debe crear cuentas para los empleados de la empresa B para acceder a la data o denegar el acceso a los otros recursos. Este caso de uso es difícil de manejar si son dos empresas federadas, al ser federadas será más fácil establecer estas

relaciones entre las organizaciones y el PEP podrá autenticar los sujetos con su ID federado.

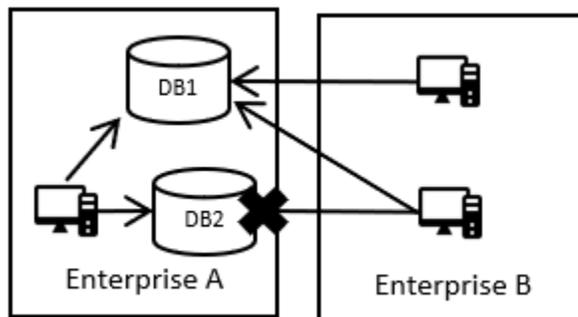


Ilustración 11

Colaboración entre límites de empresas, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

En este caso el PE/PA está hospedado como un servicio en la nube para que pueda dar la disponibilidad necesaria entre ambas empresas sin tener que configurar una VPN o similar. En algunos casos se puede utilizar un agente en la empresa B para acceder al *gateway* de la empresa A.

2.1.2.6.5. Empresas con servicios al públicos o clientes. Una característica en muchas empresas en la actualidad son los servicios públicos que pueden o no necesitar registro (usuarios creados o credenciales generadas por la organización). Como es claro en todos los casos los usuarios o los activos solicitando acceso a los recursos empresariales son ajenos a la organización y esta tiene que confiar en las políticas de ciberseguridad para mantener todos estos recursos seguros.

Para un servicio general que no requiere credenciales o inicio de sesión los principios de cero confianza no aplican directamente, ya que la empresa no puede controlar o solicitar el control de activos ajenos o sujetos que se autentican anónimamente. La organización puede establecer políticas para usuarios registrados (como se haría con clientes u otras empresas de servicios), estas políticas pueden ser el tamaño de la contraseña, tiempo de validez y otros factores como MFA. Estas políticas son limitadas, ya que solo manejarán información de sesión del usuario y no del dispositivo que este utiliza, si se puede generar un perfil del usuario como horas de trabajo, solicitudes usuales al servicio, ubicación, buscador que utiliza

para acceder el servicio *web* y cualquier desviación puede verse como un posible ataque. En estos casos las organizaciones deben saber qué información pueden recolectar según lo que dictan las regulaciones del país o países.

2.1.2.7. Amenazas asociadas con el modelo de cero confianza. Ninguna empresa puede eliminar los riesgos de ciberseguridad.

2.1.2.7.1. Alteración del proceso de decisión del modelo de cero confianza. El PE y el PA son componentes clave de toda la empresa, ninguna comunicación entre recursos debe suceder sin que lo aprueben ambos componentes y su canal de comunicación se configure con el PEP. Esto indica que es crítico que ambos componentes estén configurados y mantenidos correctamente.

Las políticas del PE/PA las genera la organización, pero cualquier administrado con acceso a la configuración del PE puede llevar a cabo cambios indeseados, sea maliciosamente o por error y puede generar una interrupción de las operaciones. Si los cambios se realizan en el PA pueden generar accesos a sujetos que normalmente no serían aceptados. Muchas veces ambos componentes se representan como uno solo, Por esto, deben configurarse correctamente y monitorearse para evitar cambios indeseados, adicionalmente, es importante tener registros activos.

2.1.2.7.2. DoS o Interrupción de la red. En el modelo de cero confianza el PA es clave para dar acceso a los recursos, por lo que una organización no puede conectar recursos sin permiso de la PA. Lo mismo sucede con los demás componentes que trabajan en la toma de decisiones, si un atacante interrumpe el servicio del PEP, PE o PA, la empresa está comprometida. Esto se puede evitar si la organización tiene redundancia de servicios o mecanismos/políticas de seguridad que protejan estos servicios de ataques.

Este escenario igual que cualquier otro solo se puede mitigar, pueden desarrollarse ataques de DoS suficientemente grandes para afectar un proveedor de servicio de la nube grande. Otra posibilidad es que un atacante puede interceptar o bloquear tráfico del proceso de autenticación y autorización, pero este escenario no es propio del modelo de cero confianza. Asimismo, dentro de este escenario también se puede presentar una equivocación

por parte del proveedor de servicio en la nube, donde alguno de los componentes se inhabilite accidentalmente.

2.1.2.7.3. Robo de credenciales/amenaza interna. Cero confianza, las políticas de seguridad y resiliencia y buenas prácticas disminuyen las posibilidades de un ataque con credenciales robadas o incluso un atacante dentro de la organización. Por la forma en la que cero confianza se maneja, el atacante necesita comprometer una cuenta existente o un dispositivo para acceder a la organización, incluso así un modelo de cero confianza correctamente implementado debe prevenir que un usuario o activo acceda un recurso que no necesite normalmente o que no sea parte de su comportamiento usual sin pedir algún tipo de autenticación y autorización nuevamente. Esto implica que un atacante debe buscar cuentas que cedan a la información que le interesa para no despertar sospechas.

Los atacantes pueden utilizar métodos de ataque como *phishing*, ingeniería social o ambas para conseguir credenciales de cuenta valiosas. La implementación de MFA puede reducir el riesgo de robo de información por el uso de cuentas comprometidas, incluso así, un atacante puede tener acceso a recursos a los que ya este usuario obtuvo acceso, pues esto depende de las políticas empresariales.

Cero confianza reduce el riesgo o previene que cuentas o dispositivos comprometidos puedan utilizarse para movimiento laterales a través de la red. El TA debe detectar comportamientos inusuales y detener un ataque de este tipo y denegar el acceso a la cuenta o activo.

2.1.2.7.4. Visibilidad en la red. Como se ha mencionado, las recomendaciones de la NIST dicen que es necesario inspeccionar y registrar en una bitácora el tráfico de red para analizar posteriormente los datos en función de identificar y actuar ante un posible ataque. Es posible que parte del tráfico generado por dispositivos no empresariales, aplicaciones y servicios no sean visibles por herramientas de monitoreo y análisis en la capa 3 de la red. Las organizaciones no pueden llevar a cabo inspecciones profundas en el tráfico de red o destinar recursos para examinar tráfico encriptado, por lo que es posible que deba utilizar otros métodos para evaluar ataques en la red. La empresa puede recolectar metadatos del tráfico encriptado como la fuente, ubicación, entre otros. Algunas técnicas de Machine Learning pueden utilizarse para analizar el tráfico.

2.1.2.7.5. Almacenamiento de información del sistemas y de la red. Una amenaza del monitoreo y análisis de tráfico de red y de sistemas es el componente de monitoreo, si se utiliza algún componente de monitoreo para contextualizar políticas, información forense o para otros análisis, esa información puede convertirse en un objetivo para algún atacante. Esto puede incluir diagramas de red, archivos de configuración, información de arquitectura y esto implica que estos recursos deben protegerse. Si esta información se compromete le puede dar al atacante una herramienta valiosa de la arquitectura de la empresa y la identidad de los activos.

Otra fuente de información en un modelo de cero confianza es la herramienta de administración utilizada para codificar las políticas de acceso y esto puede darle información de qué cuentas pueden acceder que recursos e identificar cuentas importantes para llevar a cabo un ataque exitoso. Como todos estos recursos son valiosos para la organización, es importante prevenir accesos no autorizados o intentos de acceso, así como establecer las políticas más restrictivas y que se puedan acceder solo desde lugares designados o que utilicen cuentas de administración dedicadas.

2.1.2.7.6. Confianza en soluciones o formatos de datos propietarios. Cero confianza confía en diferentes fuentes de datos para llevar a cabo las decisiones necesarias para permitir o denegar acceso a recursos empresariales, así como información de sujeto, activo utilizado, empresa e inteligencia externa y en algunos casos incluso información relacionada con el análisis de amenazas. Muchas veces estas fuentes de información no tienen un estándar de almacenamiento o para relacionar, compartir o interactuar con la información almacenada y puede que la organización se quede encerrada con pocos o algunos proveedores por problemas de interoperabilidad, lo que significa que cambio o migración a nuevos sistemas puede ser imposible o de alto costo, sin hablar de muchas horas de trabajo para completar la migración. Esta amenaza no es propia de cero confianza, pero cabe destacar la importancia de considerar proveedores holísticos, con mejores controles de seguridad, fácil migración, rendimiento, estabilidad, etc.

2.1.2.7.7. Uso de entidades no personales (NPE, Non-Personal Entities) en la administración de cero confianza. Las entidades de inteligencia artificial o agentes de *software* son los que se utilizan para manejar problemas de seguridad en las redes

empresariales y estos componentes requieren interactuar con los componentes de administración de cero confianza en lugar de un humano y cómo estos componentes autentican con la organización es un problema, ya que utilizan API propietarios para autenticar. Esto puede abrir puerta a problemas de configuración o de aplicación de políticas, que podrían dar falsos positivos o falsos negativos, lo que impacta la postura de seguridad de la empresa. Esto requiere análisis continuo y corrección de los procesos de decisión, configuración o políticas para estos dispositivos.

El riesgo es que un atacante puede inducir o boicotear un NPE para llevar a cabo acciones invasivas. Cuando se habla de un agente hay otro riesgo en el que puede obtener las credenciales del sujeto de la máquina comprometida.

2.1.2.8. Modelo de cero confianza y posibles interacciones con servicios federados.

Si varias políticas y pautas federales existen podrían cruzarse con la planificación, implementación y operación de un modelo de cero confianza. Una empresa federada puede implementar un modelo orientado a cero confianza pero puede influir en el desarrollo de su estrategia. Esto se debe a que es necesario complementar las directivas, políticas de seguridad existentes, ICAM (Identity, Credential, and Access Management; identidad, credenciales y administración de acceso) y monitoreo continuo.

La planificación e implementación de cero confianza puede cambiar los límites definidos para autorización y esto sucede por los nuevos componentes y la reducción de confianza en la red. Adicionalmente, la protección de la privacidad de los usuarios y de la información privada es una preocupación principal para las organizaciones, muchos estándares internacionales como FISMA, HIPAA y PCI producen un marco de referencia para describir los riesgos y definir estrategias de mitigación, además, definen un proceso para que la empresa identifique, mida y mitigue el riesgo de la privacidad de los usuarios y la información privada que almacena y procesa la organización. Esto puede incluir información que se utiliza para soportar la toma de decisiones del modelo de cero confianza como se ha mencionado.

Parte del núcleo de cero confianza es la habilidad de crear un *token* o llave de acceso, por lo que el PE necesitara tener la información necesaria para autorizar la conexión de los recursos. Se puede necesitar definir un grupo claro de atributos y políticas que se utilizan

para evaluar el acceso, junto con las políticas de autenticación necesarias antes de implementar cero confianza. Parte importante de la implementación de cero confianza es entender el ambiente y esto se puede llevar a cabo por medio de las siguientes preguntas:

- **¿Qué está conectado?** Qué dispositivos, aplicaciones y servicios se utilizan en la organización, esto incluye la observación y mejoramiento de la postura de seguridad de los artefactos, así como las vulnerabilidades y amenazas descubiertas.
- **¿Quién está utilizando la red?** Qué usuarios son parte de la organización o externos y a qué recursos se les tiene permitido acceder. Esto puede incluir NPE.
- **¿Qué sucede en la red?** Una empresa necesita conocer los patrones de tráfico y los mensajes conocidos entre sistemas.
- **¿Cómo están protegidos los datos?** La empresa necesita un grupo de políticas sobre cómo se protege la información cuando está en reposo, en tránsito y en uso.

Después de llevar a cabo estas preguntas queda claro la necesidad de un CDM y por qué es importante tener un registro de los activos de la organización.

2.1.2.9. Migración a un modelo de cero confianza. La implementación según la NIST es más un viaje que un reemplazo de la infraestructura o de los procesos internos de la organización. Por lo general se hace gradualmente donde se implementan los principios, cambios de procesos y soluciones tecnológicas, protegiendo primero los activos o recursos más valiosos. Muchas organizaciones optan por permanecer en un modelo híbrido y precisan de una base que incluya componentes necesarios para empezar una implementación o adopción del modelo de cero confianza. Esta base debe inventariar los activos, sujetos, procesos de negocio, flujos de tráfico y dependencias, una vez que la organización tiene este inventario puede desarrollar una lista de los procesos candidatos juntos con los sujetos y activos involucrados en el proceso.

2.1.2.9.1. Modelos cero confianza puro. En una nueva implementación donde es posible empezar desde cero y asumiendo que la organización conoce las aplicaciones, servicios y flujos de trabajo que requiere o quiere utilizar para sus operaciones, puede

implementar los principios de cero confianza para esos flujos de trabajo. Una vez que estos flujos de trabajo se identifican la empresa solo necesita descubrir los componentes necesarios y diagramar las interacciones individuales de los componentes. Este ejercicio debe ser desarrollado por toda la organización o al menos los entes que se relacionan con el proceso, no solo el área de Ingeniería, para llevar a cabo una construcción y configuración correcta de los componentes necesarios para sus procesos. Además, puede incluir algunos cambios organizacionales según cómo opere la organización en ese momento.

Esto en la práctica es raro, ya que muchas organizaciones están federadas o tienen redes ya construidas, pero se puede observar cuando algunas organizaciones necesitan construir su propia infraestructura para una nueva responsabilidad o procesos organizacionales. Por lo tanto, toda esta nueva implementación puede seguir en cierto grado los principios de cero confianza; se puede llamar a estas implementaciones como microperímetros de cero confianza y el nivel de éxito puede determinarse por cuán dependiente es la nueva infraestructura de la anterior.

2.1.2.9.2. Modelo híbrido de cero confianza y basada en perímetro. Es difícil que las organizaciones puedan migrar a cero confianza en un solo ciclo de actualización tecnológica y puede que requiera de muchos ciclos de trabajo para que el modelo pueda coexistir exitosamente con el flujo de trabajo de los procesos que no son de cero confianza. Por eso, lo más común es lo que se mencionó, se migran los procesos uno por uno para llevar a cabo los ajustes y pruebas necesarias. La organización necesita saber que los elementos comunes como el sistema de administración de ID, administración de dispositivos, el registro de eventos, entre otros, son lo suficientemente flexibles para operar con el modelo de cero confianza y perímetro a la vez. Es necesario que la organización pueda determinar cuáles procesos no pueden ser candidatos de una implementación de cero confianza antes de empezar una implementación fallida. La migración de un flujo de trabajo a cero confianza requiere al menos un rediseño parcial y esto es una oportunidad para implementar y revisar otros estándares o recomendaciones de seguridad.

2.1.2.9.3. Para introducir cero confianza a un modelo de red basado en perímetro. Como se explicó, la migración a cero confianza requiere que la organización tenga un conocimiento detallado de los activos, sujetos y procesos de negocio, esta información la

utiliza el PE cuando evalúa las solicitudes de acceso. El conocimiento incompleto puede producir un fallo en los procesos de negocio si se deniega el acceso a un sujeto o activos críticos.

Antes de considerar el modelo de cero confianza se debe alcanzar un estado donde la infraestructura pueda funcionar con los cambios requeridos para que el despliegue del modelo sea exitoso. Para entender el estado de la organización y de los procesos se pueden aplicar encuestas de los procesos y los sujetos involucrados. La NIST recomienda utilizar su estándar SP800-37 RFM (Risk Management Framework for Information Systems and Organizations o en español marco de administración de riesgos para sistemas de información y organizaciones), el cual no se desarrolla en este trabajo porque no se estudia el proceso de organización específica, más adelante se puede apreciar el ciclo que se sigue en este marco que puede dar el contexto necesario para este trabajo de investigación.

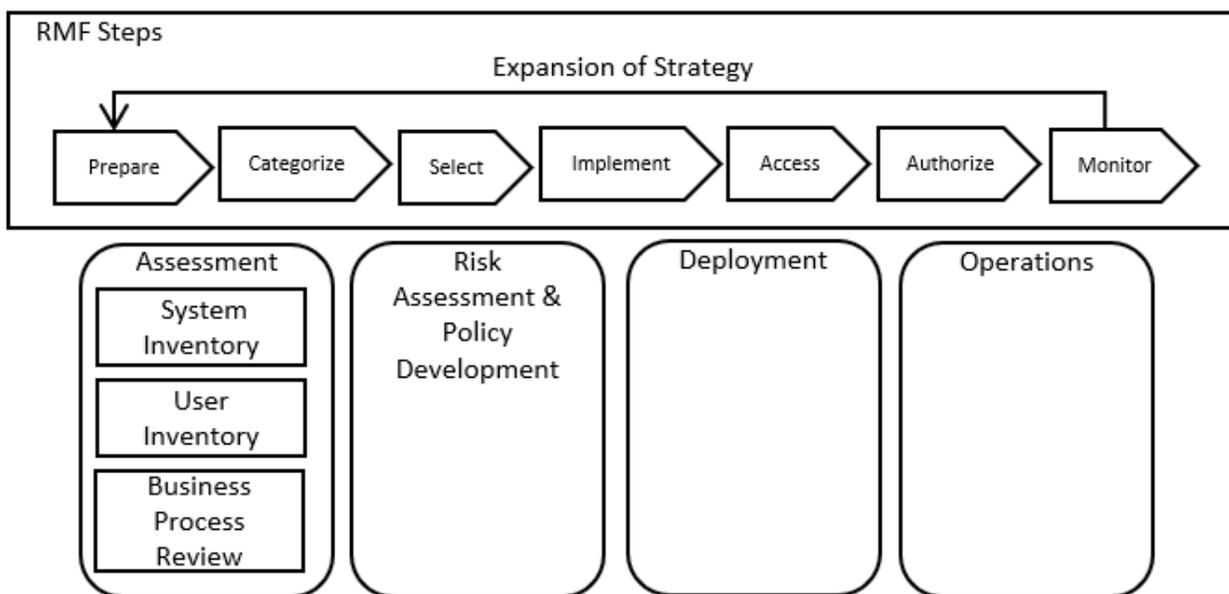


Ilustración 12

Pasos del RFM, basado en el documento de la NIST (Rose, Borchert, Mitchell y Connelly)

Una vez que el inventario ha sido creado, tiene que haber un ciclo de mantenimiento y actualización, el cual puede cambiar el proceso de negocio o impactarlo. Los pasos se explican a continuación:

1. Identificar los actores en la organización: en cero confianza el PE necesita conocer los sujetos de la organización, estos pueden ser físicos o virtuales. Las cuentas con permisos especiales o privilegios deben revisarse y evaluarse para evitar atributos o roles incorrectos, ninguna de estas cuentas debe acceder a todos los recursos empresariales, deben tener flexibilidad para cumplir con sus requerimientos de negocio y debe existir trazabilidad, se puede incluso utilizar políticas más rígidas para estos usuarios.
2. Identificar los activos poseídos por la organización: como se mencionó, la administración de dispositivos es uno de los requerimientos base de la cero confianza y debe soportar la administración e identificación de estos. Esto se refiere a cualquier componente de *hardware* (portátiles, teléfonos, IoT, etc.) o artefacto digital (cuentas de usuario, aplicaciones, certificados digitales, etc.). No es solo la identificación es también la administración de su configuración y el monitoreo se debe conocer su estado e informar al PE de toda esta información. Los dispositivos no empresariales o dispositivos fantasma (aquellos que no deben aparecer en inventarios por algún proceso interno) deben registrar información en la red como la dirección MAC, ubicación y otros datos y podrá utilizarla para la toma de decisiones o análisis forenses.
3. Identificar los procesos clave y evaluar los riesgos asociados con la ejecución de procesos: este tercer inventario debe identificar y categorizar en importancia los procesos de la empresa, los flujos de datos y su relación con la misión de la empresa. En este inventario se deben detallar los procesos de negocio y las circunstancias donde se debe permitir o denegar el acceso. Para el dominio de la migración muchas empresas desean empezar con procesos de negocio de bajo impacto, ya que se pueden presentar interrupciones en el servicio y la curva de aprendizaje depende del personal en el proceso de migración y una vez que se ha obtenido más experiencia se pueden migrar procesos más críticos.
4. Formulación de políticas de cero confianza para un proceso candidato: los factores que se pueden considerar para identificar un candidato son la importancia de los procesos, grupo de sujetos afectados y el estado actual de los recursos

utilizados por el flujo de trabajo. Se debe evaluar el riesgo de activo o del flujo de trabajo, la NIST sugiere el uso del NIST SP800-37 (Risk Management Framework, cuadro de administración de riesgos). Después de identificar los activos y flujo de trabajo, se deben identificar todos los recursos arriba (sistema de administración de ID, bases de datos, microservicios, etc.), abajo (registros o bitácoras, monitoreos, etc.) y todas las entidades (sujetos, cuentas de servicio, etc.) relacionadas o afectadas por el flujo de trabajo. Una vez que se han descubierto todos los actores del proceso el administrador de la organización debe determinar un grupo de criterios y el peso de las fuentes de información para construir el nivel de confianza que un recurso ocupa para el proceso candidato de negocio. Este proceso puede requerir ajustes o afinación para lograr políticas que aseguren un acceso al recurso, de manera segura.

5. Identificar soluciones candidatas: una vez que la lista de procesos candidatos se ha desarrollado el arquitecto de la organización puede crear una lista de posibles soluciones. El mejor modelo del mercado puede no ser el mejor para la organización y sus necesidades, a continuación, algunos factores para considerar:
 - a. ¿La solución requiere que los componentes se instalen en los activos empresariales? Esto puede limitar procesos de negocio a máquina organizacionales o administradas, denegando el acceso a los recursos no administrados o no empresariales.
 - b. ¿La solución funciona donde los procesos empresariales existen completamente en el centro de datos local? Algunas soluciones asumen que los recursos estarán en la nube y no dentro del perímetro empresarial.
 - c. ¿La solución provee medios para analizar los registros? Uno de los componentes clave de cero confianza es recolectar la información, usarla y relacionarla en el PE cuando se llevan a cabo las decisiones.
 - d. ¿La solución provee soporte a diferentes aplicaciones, servicios y protocolos? Algunas soluciones pueden tener un soporte muy pequeño para integración o

las fuentes, esto puede limitar la complejidad de la implementación o las fuentes de datos que se utilizan para soportar la toma de decisiones.

- e. ¿La solución requiere cambios en el comportamiento del sujeto? Algunas soluciones podrían requerir pasos adicionales para llevar a cabo un flujo de trabajo deseado.
6. Despliegue inicial y monitoreo: una vez que el flujo de trabajo candidato y los componentes de cero confianza han sido elegidos, se puede iniciar el despliegue inicial. Los administradores empresariales deben implementar las políticas desarrolladas en los componentes seleccionados, lo cual requerirá de observación y monitoreo, puede que se necesite alto monitoreo en las primeras semanas, hasta asegurarse de que las políticas son efectivas y permiten que el proceso funcione como se espera, este proceso debe darle a la organización las bases de los activos y recursos con sus solicitudes, comportamientos y patrones de comunicación. Algunos componentes pueden funcionar con un modo conocido como solo reporte, esto permite el acceso a la mayoría de las solicitudes con la finalidad de entender y registrar todas las conexiones y transacciones antes de la implementación o para utilizar este comportamiento como base cuando se implemente la solución. Estos monitoreos base pueden utilizarse para construir patrones de comportamiento y detectar comportamientos anómalos.
 7. Expandiendo el modelo de cero confianza: cuando la confianza de los administradores y de la organización es alta después de utilizar procesos no críticos como prueba, la organización puede entrar en una fase operacional donde los activos todavía se monitorean y el tráfico incluso se registra, pero cualquier actualización en la política se revisa y evalúa, es importante que en esta etapa ninguna modificación afecte severamente el servicio. Se puede seguir aplicando este ciclo de implementación en otros procesos candidatos.

2.1.3. Department of Defense (DoD). El Departamento de Defensa de los Estados Unidos ha creado un documento de referencia para el modelo de cero confianza junto con la Agencia de Seguridad Nacional (NSA) y la Agencia de Defensa de Sistemas de Información (DISA). A continuación, se detallan los puntos pertinentes del documento (Defense

Information Systems Agency [DISA] and National Security Agency [NSA], 2021).

El DoD menciona cinco conceptos que se pueden tomar en cuenta en una implementación de cero confianza, algunos muy similares a los mencionados por la NIST, pero con pequeñas diferencias:

- Definición de los resultados de la misión: La implementación de cero confianza se relaciona con la misión organizacional y el análisis de las superficies críticas de interacción (datos/activos/aplicaciones/servicios, DAAS).
- Arquitectura de adentro hacia afuera: la prioridad y lo primero que se debe pensar es en la protección de DAAS y, de forma secundaria, el camino para llegar a ellos.
- Definir los grupos de alto nivel: para conocer los grupos importantes de usuarios, dispositivos y aplicaciones.
- Determinar quién o qué necesita acceso: estos son críticos para aplicar las políticas consistentemente en todos los ambientes.
- Inspeccionar y registrar todo el tráfico y los eventos necesarios para responder un posible CCIR (Commanders Critical Information Requirements, requisitos de información crítica de los comandantes) con el análisis derivado de la misión organizacional: Esto es necesario para dar visibilidad completa en todas las capas de la organización.

2.1.3.1. Modelo de madurez. El documento del DoD se basa en el documento del NIST anteriormente expuesto, pero expone un modelo de madurez que puede utilizarse como referencia. Según el documento de la NIST, es necesario llevar a cabo un proceso de descubrimiento y evaluación de las tareas involucradas, así como sus relaciones. El DoD destaca que antes del diseño de un modelo de cero confianza se debe tener una base de protección que siga políticas de seguridad y estándares de TI.

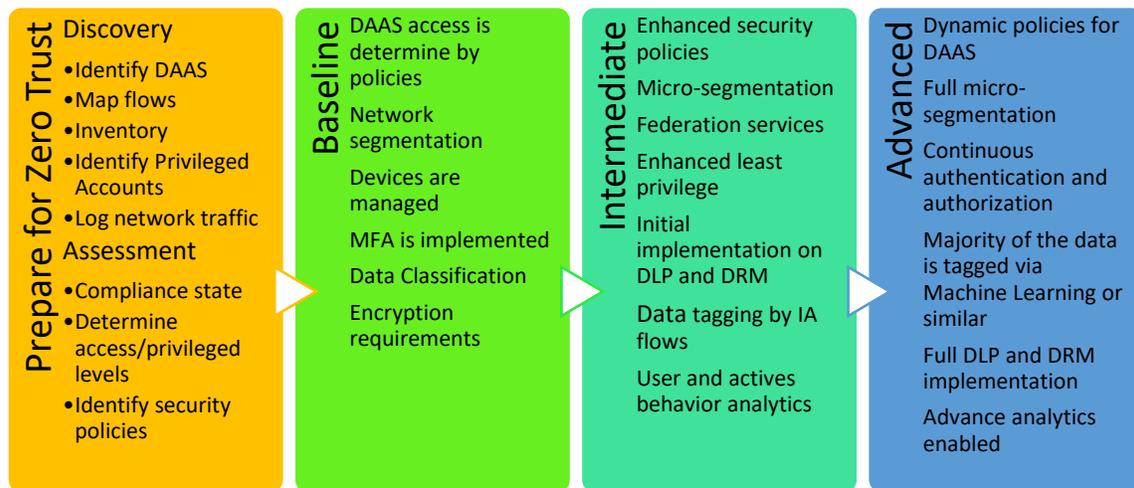


Ilustración 13

Modelo de madurez del modelo de cero confianza, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)

Este modelo de confianza define una etapa donde se puede considerar la organización como lista para un diseño o una implementación de un modelo de cero confianza.

2.1.3.2. Conceptos y principios de cero confianza. Los conceptos o principios listados por el DoD son bastante similares a los expuestos por la NIST, pero tienen diferencias a los citados y se pueden considerar para la investigación:

1. Asumir que todos los ambientes son hostiles: se presume que hay sujetos maliciosos fuera y dentro de la red. todos los usuarios, dispositivos y redes/ambientes se tratan como no confiables.
2. Asumir que hay una brecha: hay miles de ataques contra redes informáticas todos los días, por lo que es importante asumir que el atacante tiene algún tipo de presencia en el ambiente organizacional.
3. Nunca confiar, siempre verificar: por defecto se debe denegar el acceso. Todo dispositivo, usuario, aplicación y datos se autentican y autorizan explícitamente

utilizando las políticas del mínimo privilegio, atributos múltiples para decisión y políticas dinámicas de ciberseguridad.

4. Escrutinio explícito: todos los recursos deben ser accedidos, de manera segura, utilizando múltiples atributos para derivar el nivel de confianza necesario para acceder a los recursos. El acceso a los recursos es condicional y puede cambiar dinámicamente según las acciones o nivel de confianza mencionadas.
5. Aplicar un análisis unificado: es importante utilizar un análisis unificado de datos, aplicaciones, activos y servicios (DAAS) e incluir el comportamiento de estos sujetos, así como registrar cualquier transacción.

Además de los principios y conceptos, el DoD también presenta un diagrama de pilares y capacidades de cada sujeto en un modelo de cero confianza.

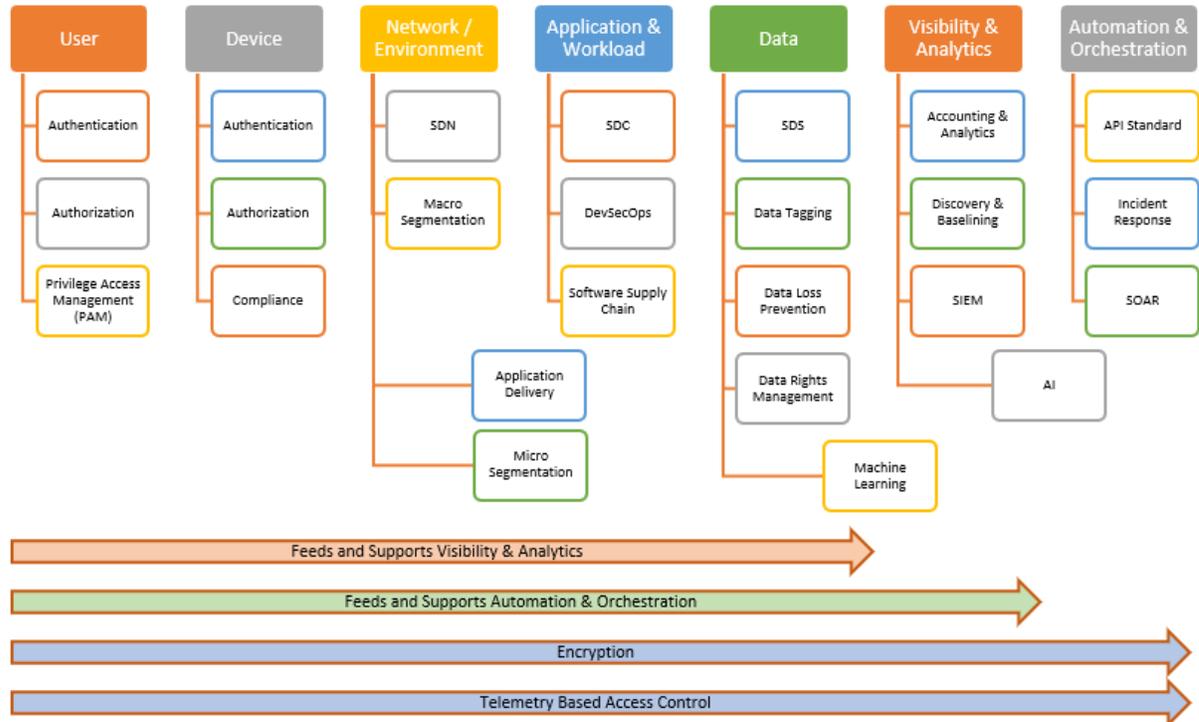


Ilustración 14

Pilares de cero confianza, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)

A continuación, se detalla lo que cada pilar debe incluir para cada uno de los sujetos según el DoD:

- Usuarios: asegurar, limitar y reforzar el acceso de personas, no personas y otras entidades federadas a los DAAS, esto puede abarcar el uso de MFA y CMFA (MFA continuo). Las organizaciones requieren tener la habilidad de autenticar continuamente, autoriza y monitorear la actividad de patrones para gobernar el acceso y los privilegios mientras protege y asegura todas las interacciones. El uso de RBAC (Role Base Access Control o en español control de acceso basado en roles) y ABAC (Attribute Based Access Control o en español control de acceso basado en atributos) entra en este pilar, incluso se aplica para aplicaciones o datos.
- Dispositivos: Se debe tener la habilidad de identificar, autenticar, autorizar, inventariar, aislar, asegurar, solucionar y controlar todos los dispositivos

esenciales para el modelo de cero confianza. Se debe conocer el estado en tiempo real de los dispositivos críticos y su nivel de actualización.

- Red/Ambiente: se debe controlar el acceso y las políticas de restricción a la red o el ambiente; la microsegmentación del perímetro debe permitir más control y protección de DAAS. Es crítico controlar los accesos privilegiados, administrar los flujos de datos externos e internos y prevenir, finalmente, los movimientos laterales por parte de los atacantes.
- Aplicaciones y cargas de trabajo: esto puede incluir tareas en sistemas y servicios, asegurar esta capa de la organización es importante para la cero confianza.
- Datos: La organización precisa categorizar sus DAAS en términos de criticidad y el uso de la información/recursos empresariales para construir una estrategia de administración. Esto se puede lograr por medio de la categorización de los datos, esquemas de desarrollo y data encriptada, sea en tránsito o en reposo. Algunas soluciones como DRM (Documents Rights Management o en español administración de derechos de documentos), DLP (Data Loss Prevention o en español prevención de pérdida de datos) u otras soluciones de *software* pueden ayudar a etiquetar la información o protegerla.
- Visibilidad y análisis: Es vital para el modelo de cero confianza tener detalles contextuales que pueden ayudar a entender el rendimiento, comportamiento y actividad base de la organización. Esta visibilidad debe mejorar la detección de comportamientos anómalos y permite hacer cambios dinámicos sobre las políticas de seguridad y decisiones en tiempo real. Una organización con un modelo de cero confianza debe capturar e inspeccionar el tráfico de red, analizar más allá de la telemetría de los sujetos debe ver en los paquetes y descubrir tráfico que represente una amenaza.
- Automatización y orquestación: una meta de toda organización es automatizar el proceso manual de seguridad para reaccionar con políticas eficientes en la organización de manera rápida y escalable. El uso de, por ejemplo, SOAR (Security Orchestration, Automation and Response o en español orquestación de

seguridad, automatización y respuesta) puede mejorar la seguridad y disminuir el tiempo de respuesta. El uso de un SIEM, por ejemplo, debe permitir el manejo de la información de seguridad y de evento o registros, así como automatizar procesos manuales y asistir en la administración de sistemas de seguridad.

2.1.3.3. Diagramas o flujos de datos. DoD define algunos flujos de trabajo para algunos de los procesos que se llevan a cabo durante el modelo de cero confianza propuesto. Cabe destacar que todos estos flujos de trabajo registran la actividad de sus componentes en un SIEM o similar. El primero está relacionado con el proceso del etiquetado de documentos, el cual permite saber la sensibilidad de la información contenida en el documento por medio de procesos automatizados o un *software* de análisis.

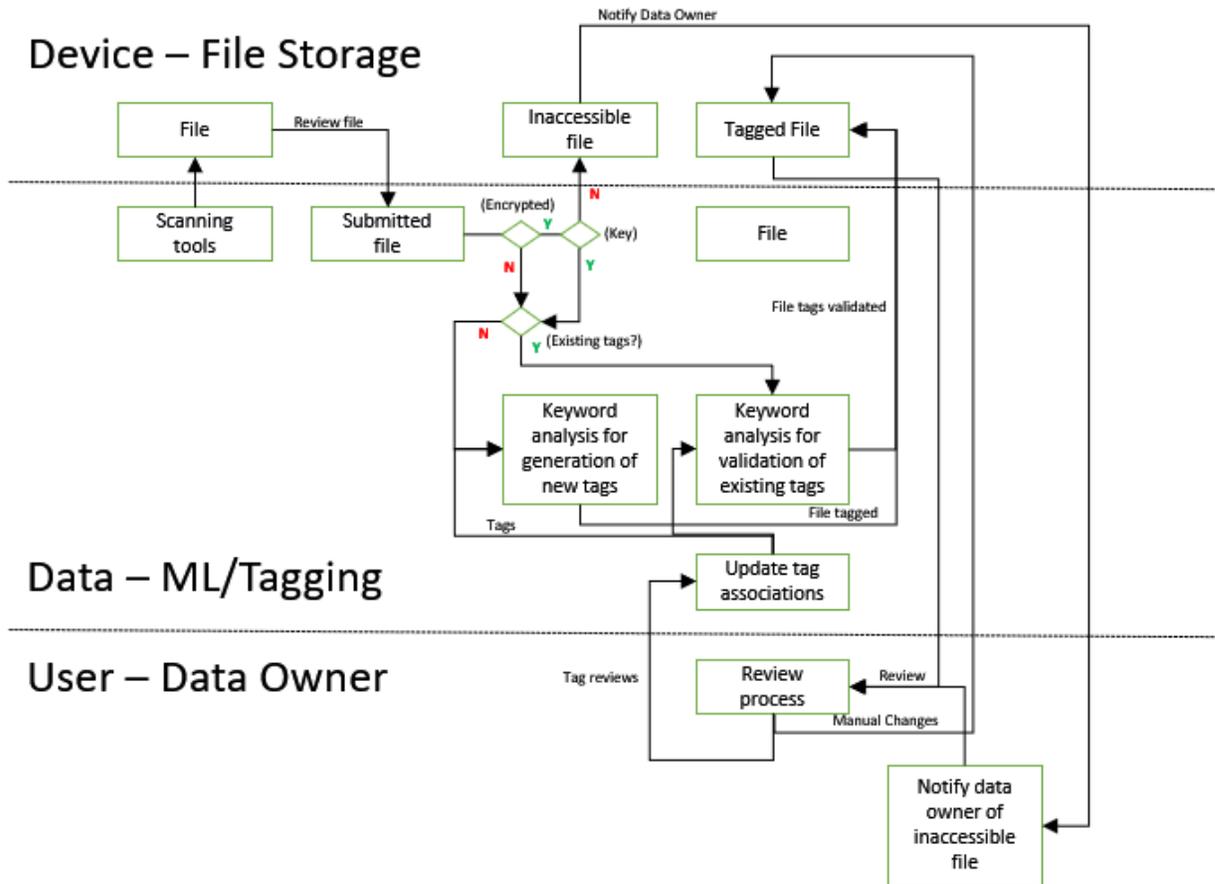


Ilustración 15

Modelo Operacional, Etiquetado de datos, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)

Este segundo flujo de trabajo se relaciona con el cumplimiento de dispositivos donde un agente local ayuda a realizar una comprobación de cumplimiento y su estado se revisa y remedia, de ser posible, se lleva a cabo una revisión adicional después de remediarse. Si no fuera posible remediarlo, según la falla el dispositivo, puede removerse de la red o se le puede denegar el acceso a algunos recursos.

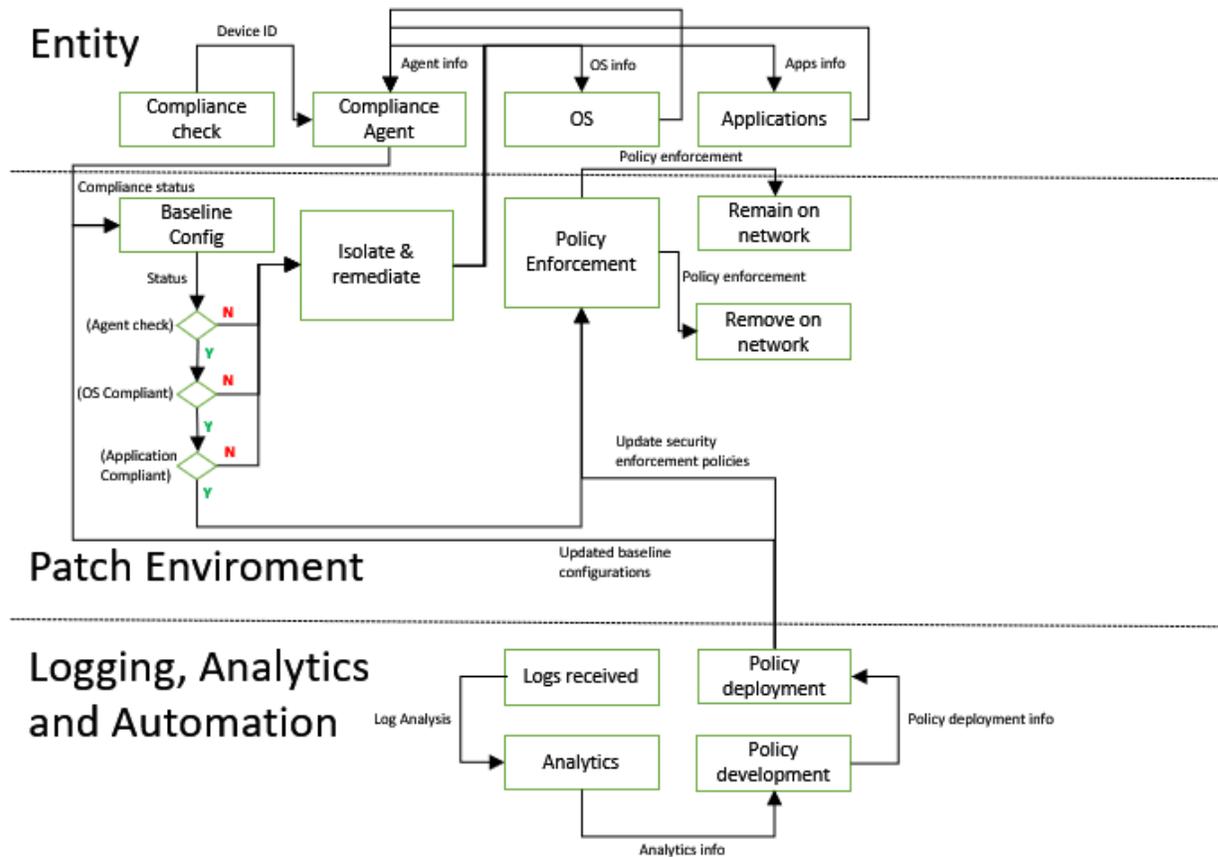


Ilustración 16

Modelo Operacional, Cumplimiento de dispositivos, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)

El tercer diagrama es el de análisis de usuarios donde se toma en cuenta la información histórica de comportamiento del sujeto (cabe destacar que esta información también se puede generar para activos) y el estado o acciones actuales del usuario y se analizan con un motor de análisis. Esta información puede utilizarla para evaluarla contra el comportamiento base global o indicadores de actividad irregular, usualmente tareas que realizaría un atacante o conocidas por ataques documentados. Mucha de esta información viene de investigación interna o publicaciones de terceros. El resultado de este análisis debe darnos el nivel de confianza sobre el comportamiento del usuario (la NIST obtiene esto con la aplicación del TA) y esta calificación de confianza se asocia con el usuario y se comparte en la red, es necesario el monitoreo continuo y el análisis para evaluar y actualizar el valor

de confianza sobre el usuario. Si el nivel de confianza baja se le puede informar al usuario y denegar el acceso a ciertos recursos o a la red.

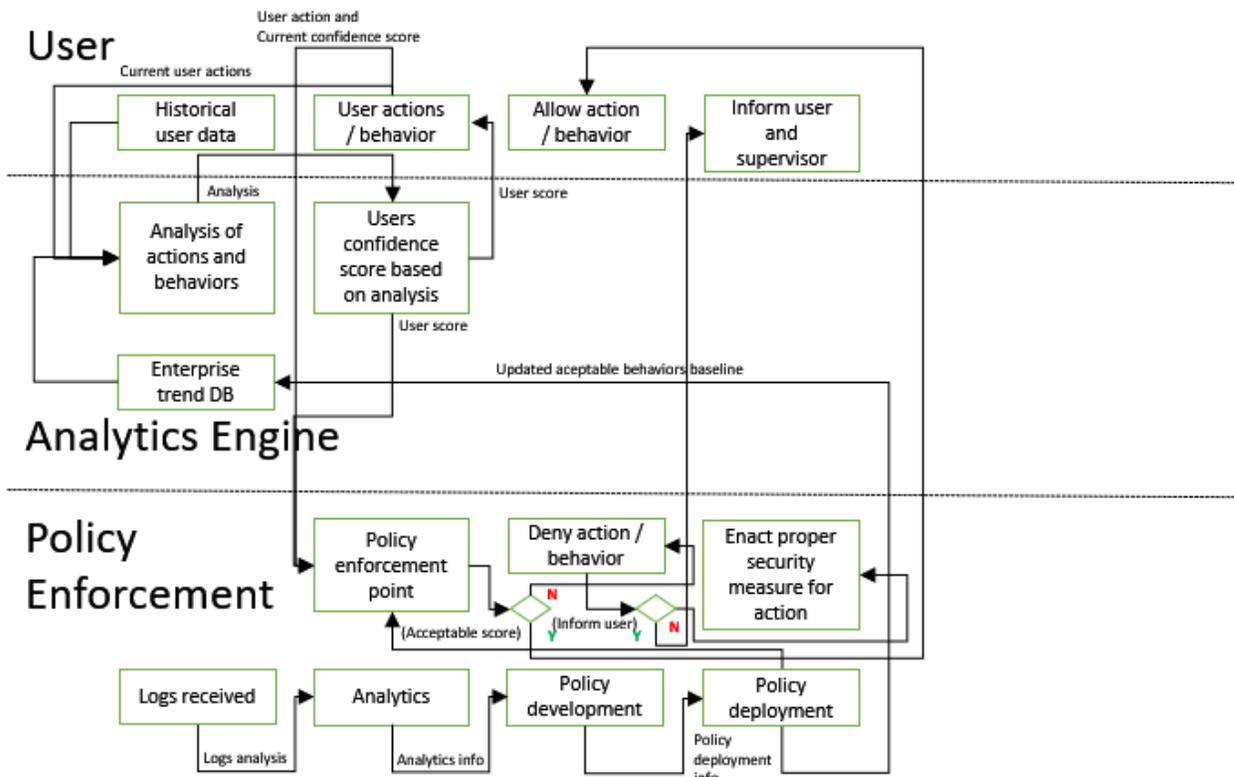


Ilustración 17

Modelo Operacional: Análisis de Usuarios, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)

El cuarto diagrama es de la Administración de Derechos de Documentos o DRM, en este caso un usuario puede solicitar acceso a un documento encriptado, el DRM local de la máquina cliente revisaría si existe la llave para abrir el documento encriptado y si todavía es válida. Si la llave no existiría o ya no es válida puede solicitar una nueva, el administrador del DRM evaluaría si el usuario debe tener acceso a la llave necesaria para acceder al documento. Una vez que el usuario tiene una llave válida puede abrir el documento.

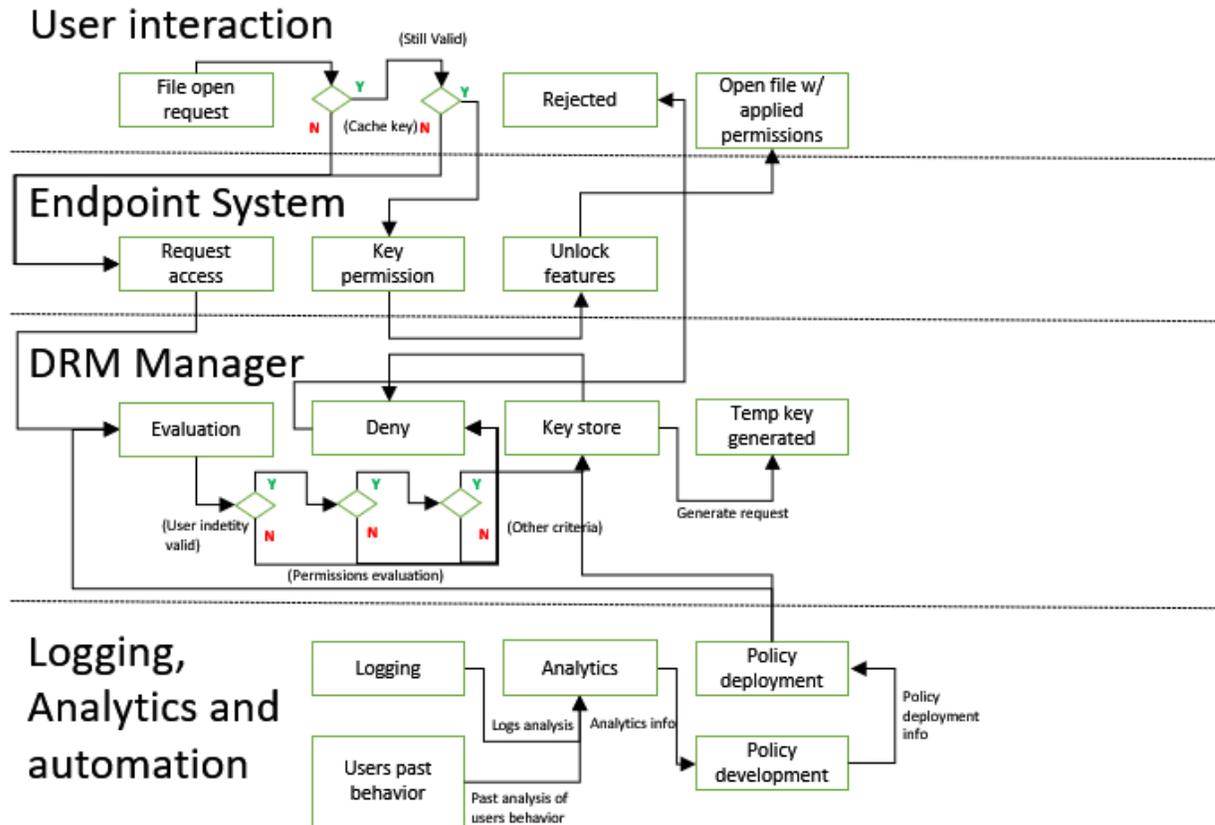


Ilustración 18

Modelo Operacional del DRM, basado en el documento del DoD (Defense Information Systems Agency (DISA) and National Security Agency (NSA), 2021)

Como se mencionó estos modelos pueden tomarse en consideración para la construcción de la propuesta, ya que están alineados o se relacionan con los alcances del trabajo.

2.2. Teletrabajo

En esta sección se hablará de las recomendaciones del teletrabajo dada por la NIST en la sección de Telework: Working Anytime, Anywhere (Teletrabajo trabajando a cualquier hora, en cualquier lugar) empezando con la publicación 800-46 (Souppaya y Scarfone, 2016) que es una guía para empresas que quieren utilizar el teletrabajo, el acceso remoto y la política de BYOD.

2.2.1. NIST: Guía de Seguridad para el teletrabajo, acceso remoto y BYOD en

las empresas. Cabe destacar que el enfoque de este documento no es la cero confianza pero se puede usar como marco de referencia para la seguridad y otras consideraciones relacionadas con el teletrabajo y la investigación. El teletrabajo o acceso remoto les da mayor flexibilidad a las organizaciones, pero implica riesgos de seguridad como la falta de seguridad física o controles en redes externas y posiblemente no seguras, o la conexión de dispositivos infectados ajenos a la organización en una red donde se ubica un recurso organizacional o la conexión directa a la red de la organización, lo que deja de lado la seguridad, otra preocupación es la disponibilidad de los recursos a estos sujetos externos. Estos sujetos externos pueden ser servicios contratados, compañeros de negocios, dispositivos de terceros, BYOD, teléfonos inteligentes, tabletas, entre otros; muchas organizaciones solicitan a compañías de terceros o a sus empleados asegurar sus dispositivos o actualizarlos, pero por lo general no se puede tener control sobre su estado. El plan de teletrabajo de la NIST establece políticas y controles basados en que los ambientes externos tienen amenazas hostiles. La NIST asume la siguiente lista de amenazas:

1. Las redes externas tienen amenazas hostiles que tratarán de hacerse con el control de la data y los recursos de la organización.
2. La organización debe asumir que los dispositivos se encuentran en diferentes tipos de ubicaciones y pueden ser perdidos o robados. Además, pueden comprometer la información en ellos o el acceso a la organización.
3. La organización debe asumir que en las redes externas la comunicación puede leerse, intervenir o modificarse.
4. Siempre se debe asumir que los dispositivos en teletrabajo pueden infectarse de *malware*.

Entre las opciones para mitigar muchas de estas amenazas está la encriptación de los dispositivos y sus comunicaciones, además del uso de una autenticación fuerte, preferiblemente el uso de MFA. Finalmente, es importante el uso de tecnologías de detección de *malware* y la valoración de la postura de seguridad del cliente para entender ha sido comprometido.

Además, es importante la definición de una política de seguridad que defina los requerimientos del teletrabajo, acceso remoto y BYOD, debe limitar que formas de acceso remoto se permiten y el nivel/tipo de acceso del sujeto. Adicionalmente, debe detallar cómo administrar los servidores que soportan estos accesos remotos y cómo actualizar sus políticas. Definir estos niveles de acceso permite a la organización limitar el riesgo en los dispositivos con acceso remoto y debe alinearse con la política del mínimo privilegio.

Parte fundamental del teletrabajo con dispositivos en la organización es mantener y actualizar los clientes contra las amenazas conocidas, así como actualizarlas. Esto se puede lograr con políticas de endurecimiento o políticas de actualización de aplicación o sistemas operativos. Adicionalmente, el uso de *software antimalware* o *firewall* personales que puedan proteger estos dispositivos en redes donde no existe ningún control de seguridad organizacional, la importancia de estas políticas o de estos *software* de protección son la falta de seguridad en los ambientes externos, las máquinas tienen que ser seguras por su propia cuenta. Es importante que la organización pueda tener cierto nivel de certeza en cuanto a la seguridad de los dispositivos conectado en su red.

Si se utilizan dispositivos externos a la organización se puede considerar la implementación de un red dedicada o separada, ya que la falta de control sobre estos los hace generalmente más susceptibles a los ataques y agregan un riesgo considerable a la red de la organización. De la misma manera que la red interna de la organización este segmento debe asegurarse y monitorearse, de manera consistente.

2.2.1.1. Descripción de la seguridad del teletrabajo y acceso remoto organizacional.

Teletrabajo se define en el documento como la habilidad que tienen algunas organizaciones de permitir que sus empleados, servicios contratados, compañeros de negocio o cualquier otro usuario puedan trabajar con los recursos de la organización desde cualquier otra ubicación, con diferentes tipos de dispositivos y puedan responder correos, acceder sitios *web*, revisar o editar documentos, entre otros.

2.2.1.1.1. Vulnerabilidades, amenazas y controles de seguridad. NIST establece como los objetivos más comunes en ambientes de teletrabajo que no difieren mucho de los objetivos generales de seguridad:

1. **Confidencialidad:** se debe asegurar que las comunicaciones de acceso remoto y los datos almacenados por los usuarios no sean autorizados por sujetos no autorizados.
2. **Integridad:** se debe detectar cualquier cambio con o sin intención de una comunicación remota en tránsito.
3. **Disponibilidad:** se debe asegurar que el acceso a los recursos por medio remotos suceda cuando se necesite y cómo se necesite.

Es importante que cualquier organización pueda desarrollar un modelo de Sistemas de Amenazas (Se puede utilizar el NIST 800-154 como guía, este no será ampliado en la investigación) antes de diseñar o implementar un modelo de teletrabajo. El proceso del modelo de sistema de amenazas incluye modelados de amenazas donde se identifican los recursos involucrados en el proceso y todas las posibles amenazas, vulnerabilidades y controles de seguridad que se relacionan con estos recursos, debe también contener una evaluación de posibilidad de éxito para cada uno de estos ataques y su posible impacto. Finalmente, debe incluir le recomendaciones y controles que pueden mejorar los resultados y mitigar estas amenazas. Este modelado de amenazas ayuda a las organizaciones a identificar los requerimientos de seguridad y las mayores preocupaciones de seguridad en el ambiente. Algunas de las mayores preocupaciones identificadas por la NIST son:

- **Falta de controles físicos de seguridad:** como se ha mencionado, los dispositivos de teletrabajo pueden estar virtualmente en cualquier lugar del planeta, un control de mitigación común es el encriptado del dispositivo y fuertes políticas de autenticación como MFA. Siempre habrá otros riesgos como el uso de dispositivos con datos sensibles en lugares públicos o dispositivos desatendidos, que solo la cultura organizacional puede corregir.
- **Redes no seguras:** al no tener control sobre las redes externas todas se pueden considerar como no seguras, muchos de los usuarios pueden utilizar conexión por cable o inalámbrica en diferentes ubicaciones, incluso utilizar teléfonos o tarjetas de datos. Estas redes pueden ser víctimas de ataques como hombre en el medio o similares donde se observa, captura o modifica el tráfico de red. Las

organizaciones deben pensar que estas redes están comprometidas y deberían utilizar comunicaciones encriptadas para minimizar los riesgos, además de mecanismos de autenticación mutua donde se puedan verificar ambos participantes en una comunicación.

- **Identificar dispositivos infectados en internas:** este punto habla específicamente de dispositivos a partir del modelo de BYOD y establece que los dispositivos ajenos a la organización deben tratarse como maliciosos o infectados y se deben planear todas las precauciones con esa premisa. Una de las maneras más sencillas para mitigar el impacto de estos dispositivos es con una red independiente para estos dispositivos, pero esto puede afectar algunos procesos de negocio.
- **Acceso externo a los recursos internos:** en este punto se debe comprender que el acceso a recursos internos representa un riesgo de seguridad y se debe asegurar que los recursos compartidos, de manera externa o en redes externas, son estrictamente necesarios para algunos procesos de negocio. Las organizaciones deben considerar el balance entre los beneficios y posible impacto al comprometer cada uno de estos recursos y si se desean compartir, de manera externa, deben tener políticas endurecidas que los protejan apropiadamente de las posibles amenazas externas, además de establecer otros controles de seguridad.

2.2.1.1.2. *Métodos de acceso remoto.* La NIST divide los métodos de acceso remoto en cuatro categorías que se basan en sus arquitecturas generales, *tunneling*, portales de acceso, acceso por escritorio remoto y acceso directo a aplicaciones. Todas tienen en común las siguientes características:

- Todas dependen de la seguridad física de los clientes.
- Todas pueden utilizar diferentes métodos de autenticación.
- Todas pueden encriptar el tráfico entre los dos nodos de comunicación.
- Todas permiten que los usuarios almacenen información en sus dispositivos.

2.2.1.1.2.1. *Tunneling.* El *tunneling* o también conocido como VPN (Virtual Private

Network o en español red virtual privada) permite establece una comunicación segura entre redes, lo que incluye Internet y otras redes públicas. Este permite que el usuario/dispositivo pueda acceder recursos de la organización por medio de un VPN *gateway* para llevar esto a cabo el cliente precisa de tener el *software* cliente de la VPN o está contado a una red con un VPN *gateway*. El VPN *gateway* se encarga de enviar la autenticación del usuario, administrar el control de accesos, entre otros. Esta arquitectura utiliza la criptografía para cifrar la conexión y asegurar la confidencialidad e integridad de la información transmitida entre ambos nodos, por otro lado, la comunicación entre el VPN *gateway* y el recurso interno no tienen ningún método de encriptación. Se debe considerar que, del lado del dispositivo, el agente de VPN necesitaría de los controles necesarios para no ser comprometido, al igual que la data que repose en este dispositivo, es decir, extraída de la VPN.

Por lo general las VPN utilizan Ipsec (Internet Protocol Security), SSL (Secure Sockets Layer) o SSH (Secure Shell). La NIST recomienda las publicaciones de la NIST 800-77 o 800-113 que dan una guía para la configuración de esta tecnología. Algo beneficioso de este modelo es que, aunque no protege los que hay después del VPN *gateway*, este puede dirigir a los usuarios a un segmento específico de la red donde solo hay acceso a ciertos recursos.

2.2.1.1.2.2. Portales de acceso. Los portales de acceso son servidores que ofrecen acceso a una o más aplicaciones por medio de una interfaz centralizada. El usuario utiliza un cliente para acceder al portal, la mayoría de las veces estos portales son *web* y pueden ser accedidos por medio de cualquier buscador. La aplicación debe instalarse en el servidor que tiene el portal instalado, debe tener comunicación con el servidor de la aplicación. La comunicación entre el servidor con el portal y el cliente del portal debe ser segura y esto depende de la configuración del servicio y de las capacidades de la solución.

Sus características de seguridad son similares a las del *tunneling*, esta solución también protege la información entre el cliente y el servidor, además de soportar la autenticación, el control de acceso y otras características. La diferencia más importante es la ubicación de la data, tanto de la aplicación como de la información, que se mantendrá en el servidor. La información se transmite al cliente en forma de imágenes renderizadas que se almacenan temporalmente en la máquina cliente (como imágenes). Esta solución le permite

a la organización tener control sobre cómo el *software* y los datos se aseguran. Uno de los problemas que tiene esta solución es la cantidad de instancias que pueda ejecutar el servidor de una aplicación y al exceder el límite puede afectar un proceso organizacional o afectar el rendimiento/experiencia de los usuarios.

Existen diferentes soluciones basadas en portales, los portales *web* proveen acceso a distintas aplicaciones *web* desde un solo portal, también existen portales que simulan una sesión o un escritorio remoto donde la experiencia es similar a la de un sistema operativo y le da acceso a un número de aplicaciones. Algo similar a la solución anterior es VDI (Virtual Desktop Infrastructure) que es similar al acceso remoto, donde un usuario se conecta a una máquina virtual que se reutiliza entre los usuarios, cualquier cambio se descarta, esto logra que la imagen siempre este en cumplimiento con la organización y evita cambio no autorizados durante la sesión. Algo que se puede considerar es una nueva tecnología emergente conocida como VMI (Virtual Mobile Infrastructure) que simula el mismo escenario de VDI para dispositivos móviles.

2.2.1.1.2.3. Acceso por escritorio remoto. Esta arquitectura le permite al usuario controlar una máquina en particular la organización, por lo general su propia máquina dentro de la organización, el usuario tendría control del teclado y el *mouse* sobre esta máquina, además de que puede ver la pantalla del dispositivo. Esta modalidad permite tener acceso a todos los recursos como si estuviera trabajando desde la red de la organización. Hay dos maneras de poner esta arquitectura en práctica, la primera es conectándose directamente al dispositivo interno y la segunda es por medio de un dispositivo intermedio confiable, ambas pueden tener limitaciones según la seguridad perimetral de la organización, ya que la conexión directa puede necesitar la aprobación de un *firewall*. Por eso, el uso de un dispositivo intermedio suele ser la solución más segura y sencilla, este dispositivo puede ser el mismo *firewall*.

Cuando se utiliza un cliente de *software* para conectarse directamente al dispositivo organizacional, el *software* se encarga de proteger la confidencialidad e integridad de las comunicaciones entre los sujetos, este método puede ocultar este tráfico a los controles de red como *firewall* y otros que no pueden analizar el tráfico. Esto puede generar más riesgos que beneficios por lo que muchas organizaciones no utilizan este medio.

Cuando se utiliza este dispositivo intermedio, es este componente el responsable de encriptar la comunicación entre los sujetos y asegurarse que haya una autenticación apropiada, algunas veces soporta métodos adicionales de autenticación como MFA. En esta modalidad este servidor intermedio es clave por lo que se deben tomar todas las precauciones necesarias para asegurarlo y debe tener los controles apropiados para mitigar las amenazas presentes.

Ambos métodos son descentralizados, lo cual creara una superficie de ataque más grande y la organización tendrá que asegurar cada estación de trabajo para que sean accedidas de manera segura. Se recomienda ver estas máquinas como máquinas que están expuestas al Internet en el perímetro de la organización. La NIST recomienda evitar soluciones como el Remote Desktop Protocol de Microsoft (RDP) o el Virtual Network Computing (VNC).

2.2.1.1.2.4. Acceso directo a aplicaciones. Muchas veces el acceso remoto se puede dar sin la necesidad de un *software* para eso, algunas aplicaciones tienen sus opciones de acceso remoto y por lo general proveen una serie de controles de seguridad. La aplicación tendría su propio cliente para uso interno y externo y este será la que inicia la comunicación con el servidor organizacional.

Un ejemplo común de este esquema es un servidor de correo, donde se puede tener un cliente de correo o incluso puede utilizar un acceso *web*, adicionalmente, todo el proceso de autenticación y comunicación lo lleva a cabo el cliente o el buscador. Este modelo es utilizado comúnmente con servicios o servidores que se ubican en el perímetro de la organización y por lo general aplicación de bajo impacto.

2.2.1.1.3. Recomendación claves. El documento de la NIST tiene la siguiente lista de recomendación generales para el acceso remoto:

- Para soportar la confidencialidad, integridad y disponibilidad, todos los componentes de teletrabajo y soluciones acceso remoto, así como los clientes y servidores deben asegurarse contra las posibles amenazas y se debe estudiar cada una.

- Antes de diseñar y desarrollar soluciones de teletrabajo o acceso remoto, la organización debe desarrollar un modelo de sistema de amenazas para todos los recursos que serán accedidos de manera remota.
- Cuando se planean las políticas y controles de seguridad, la organización debe asumir que los clientes están o estarán comprometidos.
- Las organizaciones deben planear la seguridad de su plan de acceso remoto, asumiendo que las redes intermediarias no son seguras.
- Las organizaciones deben asumir que las máquinas cliente serán infectadas de *malware* y deben establecer los controles de seguridad necesarios.
- Las organizaciones deben medir el impacto/riesgos y beneficios de los diferentes métodos de acceso remoto antes de implementar una solución. Las organizaciones deben asegurarse de la disponibilidad de los recursos compartidos por los distintos medios, además de los pasos necesarios para su endurecimiento contra ataques o amenazas.
- Cuando se planean las soluciones de acceso remoto, las organizaciones deben considerar las implicaciones en la seguridad del método de acceso remoto utilizado y cuán bien cubrirá los requerimientos organizacionales este método.
- Para BYOD las organizaciones deben considerar la implementación de redes independientes.

2.2.1.2. Seguridad para las soluciones de acceso remoto. El documento de la NIST trata de otros temas que se relacionan con el lado de servidor como proveedor de servicios, se hace hincapié en la parte de autenticación, ya que es el enfoque del trabajo.

2.2.1.2.1. Acceso remoto: autenticación, autorización y control de acceso. A continuación, define el acceso remoto, la autenticación, la autorización y el control de acceso.

2.2.1.2.1.1. Autenticación. Existen muchas maneras de autenticar a los usuarios remotos, así como contraseñas, certificados digitales, *tokens*, entre otros. Se recomienda usar diferentes contraseñas para distintos servicios o plataformas, ya que estos ayudan a proteger recursos de credenciales robadas y, al mismo tiempo, no se recomienda el uso de muchas

contraseñas distintas, ya que muchos usuarios pueden tener problemas al recordarlos y promover otros métodos que no siempre son seguros. La recomendación en organizaciones que precisan de un nivel más alto de seguridad es utilizar la combinación de diversos métodos de autenticación. Una de las limitaciones del MFA es que algunos de los dispositivos clientes que pueden no tener las capacidades para leer tarjetas inteligentes o características biométricas.

Para darle un grado mayor a la complejidad a la autenticación muchas organizaciones pueden solicitar una reautenticación después de largas sesiones de trabajo o un tiempo determinado sin interacciones. En algunos casos se puede incluso solicitar una autenticación mutua entre los dos sujetos involucrados y así verificar que ambas son los únicos que participan en la comunicación, usualmente se utilizan certificados para eso.

2.2.1.2.1.2. Autorización. Después de identificar al sujeto que solicita acceso remoto a la organización o uno de sus recursos se debe determinar a cuáles recursos puede acceder. Algunas veces la autorización puede estar determinada por el estado del cliente y para estos por lo general se necesita de un agente en la máquina cliente que indica el estado del cliente y no puede dar información del estado de políticas y nivel de parcheo. Algunas veces estas herramientas pueden dar contexto de la clase de dispositivo y, de esta manera, discernir qué tipo de recursos puede acceder. Estas verificaciones adicionales del dispositivo permiten limitar el acceso más o poner el dispositivo en un estado de cuarentena.

2.2.1.2.1.3. Control de acceso para redes de comunicaciones. Uno de los componentes principales para asegurar el acceso a las redes de comunicación y proteger el contenido en ella es el uso de la criptografía. La NIST recomienda los algoritmos aprobados, el uso FPIS 140 y ambos lados de la interacción deben aprobar la validación de FPIS 140. Ipsec y SSL por lo general incluyen mecanismos de encriptación aprobados y por lo general cuentan con pruebas para verificar la integridad. Se recomienda que cualquier método criptográfico no aprobado por la NIST se deshabilite como método de precaución.

Se puede considerar el uso de *split tunneling*, el cual permite seleccionar que tráfico viajará por medio de la VPN y cual no. Esto permite aumentar la eficiencia de las comunicaciones y reduce la carga sobre la VPN, también ayuda a liberar la carga sobre los controles establecidos para examinar el tráfico al enfocar estos controles solo en el que pasa

directamente a la organización, pero si parte del tráfico que no viaja por la VPN es sensible puede resultar en problemas de seguridad si esta máquina se encuentra en una red poco segura.

2.2.1.2.2. Recomendación claves. No todas las recomendaciones dadas en esta sección del documento de la NIST aplican para esta investigación, se destacarán solo las que apliquen a este trabajo.

- Las organizaciones deben considerar cuidadosamente la seguridad de cualquier solución de acceso remoto que se ejecute en un servidor donde se ejecuten otros servicios o aplicaciones.
- Las organizaciones deben considerar todos los factores de seguridad cuando se está pensando en la ubicación en la red del servidor soportando el acceso remoto, estos factores deben incluir el rendimiento, tráfico y otros. Lo usual es ver estos servidores en el perímetro de la red.
- Para asegurar que el acceso es restringido apropiadamente, el servidor de acceso remoto debe autenticar cada usuario (que se encuentre teletrabajando) antes de darle acceso a los recursos de la organización y debe utilizar la autorización para asegurarse de que el usuario solo tenga acceso a los recursos necesarios. Es importante considerar la autenticación mutua para comprobar que ambos actores son legítimos.
- Toda información sensible que es accedida por medio de acceso remoto de preservar su confidencialidad e integridad por medio del uso de criptografía. Se recomiendan algoritmos aprobados por las NIST y basados en FIPS.
- Las organizaciones deben planear como se administrarán los clientes remotos y su *software* de seguridad, esta administración de dispositivos debe funcionar remotamente y de manera segura.

2.2.1.3. Seguridad del dispositivo cliente de teletrabajo. Existen dos tipos de dispositivos clientes, computadoras personales, las cuales son computadores portátiles o de escritorio que ejecutan sistemas operativos como Windows, OS X y Linux y dispositivos

móviles como pequeñas computadoras móviles, teléfonos inteligentes y tabletas, las cuales pueden correr una gran variedad de sistemas operativos, pero por lo general iOS y Android. Cabe destacar que las diferencias entre los dispositivos son cada vez menores y muchos dispositivos móviles ofrecen capacidades similares a computadoras personales, aunque en el ámbito de la seguridad todavía existen grandes diferencias.

Adicionalmente, estos dos tipos se pueden dividir en cuatro categorías, organizacionales máquinas adquiridas, configuradas y administradas por la organización; controladas por terceros son máquinas administradas o brindadas por compañías ajenas a la organización. BYOD son dispositivos completamente administrados por el usuario y este es el único responsable de mantenerla y asegurarla y desconocidas son dispositivos en las redes externas de la organización donde no existe ningún control.

Algunas de las amenazas principales de los usuarios o dispositivos con modalidad de teletrabajo son *worm*, código malicioso en móviles, caballos de Troya, *rootkits*, *spyware* y *bots*; estas infecciones pueden suceder por medio de correos, sitios *web*, descargas de archivos, archivos compartidos, *software* de punto-a-punto, mensajería instantánea y redes sociales. Otro riesgo mencionado es el posible robo o pérdida de estos dispositivos, además de cualquier acceso físico a los dispositivos por terceros o dispositivos infectados.

Recordemos que el teletrabajo incrementa la superficie de ataque, ya que expande la red organizacional a estas redes públicas o privadas fuera de la organización y como se ha destacado los clientes deben asegurarse apropiadamente y su seguridad debe ser mantenida regularmente.

2.2.1.3.1. Asegurando computadores personales para el teletrabajo. La NIST afirma que una de las medidas más importantes es el uso de un *firewall* personal, correctamente instalado, configurado y actualizado, esto lo aseguran porque los *firewalls* personales pueden ayudar a terminar amenazas de red en muchos escenarios. Un *firewall* personal debe tener diferentes perfiles o configuración para evitar ser muy restrictivo en redes conocidas (según cero confianza se deben tratar todos los ambientes por igual), un posible problema con el uso de perfiles es que el sistema falle y utilice uno menos restrictivo en ambientes riesgosos.

La segunda consideración según la NIST es tener la habilidad de aplicar actualización de sistema operativo y aplicaciones, el uso de políticas para obtener esas actualizaciones desde los proveedores es a veces complicado y no da visibilidad del estado actual de la máquina. Muchas organizaciones hacen un sistema de administración de actualizaciones centralizado, lo cual permite actualizar de acuerdo con los planes organización, así como definir cuándo y cómo se instalan y dar, finalmente, visibilidad del cumplimiento.

Otras consideraciones destacadas por la NIST son:

- Para usuarios administrativos se recomienda tener dos cuentas, una con acceso limitado que debe ser la cuenta que utilicen para su trabajo diario y para inicio de sesión y para algunas tareas administrativas o que requieran más privilegio una cuenta de administrador que debe utilizarla solo cuando es necesario. Esto puede evitar que un atacante obtenga control de la cuenta administrativa.
- Utilizar el bloqueo de sesión, esto es importante para evitar que otros usuarios o personas ajenas a compañía puedan acceder a datos por una máquina desatendida y que sea desbloqueado solo por otro proceso de autenticación. Esto no evitaría el robo de la máquina el uso de otras técnicas, pero puede evitar un acceso rápido de algún sujeto en la proximidad.
- Asegurar físicamente los activos en ambientes no seguros (para cero confianza todos los son), el activo puede quedar desatendido y ser robado.

2.2.1.3.2. Asegurando dispositivos móviles para el teletrabajo. No es muy común, pero muchas organizaciones también utilizan dispositivos móviles para visitantes o consultores, por lo que este punto puede aplicar en áreas más allá de teletrabajo. Algunas maquinas recurrían a *Software* de administración de dispositivos móviles (MDM, Mobile Device Management), esto usualmente permite controlar las aplicaciones que se instalan en el dispositivo y muchas de las configuraciones. La NIST SP 800-124 es una guía para asegurar los dispositivos móviles, el documento estudiado para la investigación destaca los siguientes puntos del 800-124:

- Limitar las capacidades de red de los dispositivos, por estos hablamos de restringir la conexión a redes no seguras o sin seguridad básica, compartir Internet y bluetooth.
- Los dispositivos deben tener un agente *antimalware* y *firewall*, deben estar habilitados y correctamente y configurados. En redes externas serán los únicos controles conocidos.
- Asegurar la actualización del dispositivo, *firmware* o actualizaciones de *drivers*, sistema operativo y aplicaciones.
- Utilizar la criptografía de la data en reposo, en el almacenamiento interno o los medios removibles de almacenamiento.
- Requerir métodos fuertes de autenticación.
- Restringir aplicaciones, utilizar *whitelisting* y *blacklisting*.

Como se mencionó la organización puede utilizar MDM, otra opción es una solución de MAM (Mobile Application Management). MDM tiene la capacidad de aplicar una serie de políticas de seguridad en nombre de la organización, incluso hacerlo en algunos dispositivos que no son de la organización, MDM también permite borrar datos de forma remota y en caso de robo o extravío aplicar políticas de encriptación. MAM, por otro lado, solo se aplica a las aplicaciones empresariales por lo general crea un ambiente aislado para las aplicaciones y su data, puede ofrecer encriptación o solicitar que el dispositivo sea encriptado por el usuario antes de instalar las aplicaciones, adicionalmente permite el borrado de este ambiente protegido, de manera remota, en caso de extravío o robo.

El foco de la investigación no son los dispositivos móviles (teléfonos inteligentes, tabletas o similares), pero se agrega como referencia para toma de decisiones. Adicionalmente, las empresas interesadas pueden también revisar la publicación NIST SP 1800-21 (NIST, 2020) que también extiende el uso, implementación y buenas prácticas para un sistema que soporte dispositivos móviles.

2.2.1.3.3. Protegiendo información en dispositivos cliente en teletrabajo. El teletrabajo por lo general involucra la creación y edición de información relacionada con el

trabajo, como correo, documentos de texto, hojas de Microsoft Excel, entre otros. Los datos son siempre importantes sin importar su naturaleza, por eso, todos los datos que se relacionan con trabajo deben tratarse como activos organizacionales. Las primeras dos sugerencias de la NIST son proteger el dispositivo como ya se ha expuesto en este documento y respaldar esta información en una ubicación controlada por la organización. Algunas organizaciones pueden optar por no almacenar información en los dispositivos y utilizar soluciones de almacenamiento externo.

Información sensible como PII (Personal Identifiable Information o en español Información de Identificación Personal) debe ser protegida, aunque no sea información organizacional, muchos usuarios tienden a guardar información personal en sus dispositivos. Estos dos tipos de información pueden dañar la reputación de la compañía o el empleado, incluso puede utilizarla para atacar al empleado o usar para romper contraseñas (un gran porcentaje de contraseñas utilizan datos personales).

2.2.1.3.3.1. Encriptado de datos en reposo. Todos los dispositivos que se utilizan para teletrabajo (incluso los que no lo son si seguimos los principios de cero confianza), sin importar su tamaño, pueden ser robados y los sujetos mal intencionados pueden intentar obtener información de estos dispositivos. Las políticas de las llaves criptográficas deberían seguir una misma política empresarial para proteger la información de manos ajenas. La NIST advierte que la eficacia de las llaves de encriptación para un disco completo depende de que los dispositivos en reposo sean apagados para evitar exponer la llave de encriptación o dejar los dispositivos descriptados, ya que al iniciar el dispositivo y desbloquearlo, la información queda abierta.

2.2.1.3.3.2. Respaldo información de los dispositivos en teletrabajo. Todas las organizaciones deberían poseer políticas de respaldo periódicas, estas políticas deben cubrir los dispositivos en teletrabajo y móviles, es posible que la organización dependa de diferentes métodos para aplicar estas políticas y asegurarse de que sus activos están configurados correctamente. Pueden existir consideraciones adicionales si la naturaleza de la información es diferente y si la organización desea llevar a cabo un respaldo de manera remota o en un ambiente externo. De cualquier manera, la información que se respalde debe viajar encriptada y debe hacerse una evaluación de su integridad.

2.2.1.4. Consideraciones de seguridad para un ciclo de vida de teletrabajo y acceso remoto. La NIST construye esta guía sobre cómo se deben incorporar todos los detalles de seguridad cubiertos en el documento, los describe en cinco fases, además, se basa en la publicación NIST SP 800-64. Algunas organizaciones pueden utilizar un esquema enfocado en la metodología de administración de proyectos para la implementación y puede tropicalizar la solución sugerida más adelante.

1. **Iniciación:** en esta fase antes del diseño de teletrabajo o acceso remoto, la organización debe identificar las necesidades que la empresa tiene en el teletrabajo, debe tener una idea general sobre cómo el teletrabajo se alineará con la misión de la organización. Una vez identificadas las necesidades se debe crear una estrategia general de la implementación, se debe desarrollar la política de seguridad soportando las tareas que se pueden llevar a cabo y como se alinea a la misión de la organización para este último punto la organización requerirá especificar los requerimientos de negocio y funcionales de la solución. Algunas consideraciones adicionales para los requerimientos y diseño son:
 - a. **Sensibilidad del teletrabajo:** se debe considerar la sensibilidad de la información que está involucrada en las tareas identificadas.
 - b. **El nivel de confianza en el cumplimiento de la política de seguridad:** este nivel de confianza solo puede asegurarse por la capacidad de la organización en aplicar las políticas y controles necesarios en los dispositivos remotos.
 - c. **Costo:** el costo puede variar ampliamente según los controles y las decisiones tomadas para aplicar o desarrollar las políticas como es deseado. Este rubro puede incluir los mismos dispositivos que se utilizan por los empleados.
 - d. **Ubicaciones de teletrabajo:** el riesgo puede ser menor si estos dispositivos se utilizan únicamente desde las casas de los empleados o ubicaciones designadas, muchas veces ese no es el caso, lo cual incrementa el riesgo.
 - e. **Limitaciones técnicas:** puede que sea necesario tener o adquirir ciertos dispositivos para necesidades específicas en ambientes de teletrabajo, la

adquisición o las capacidades técnicas para configurar estas soluciones deben considerarse.

- f. Cumplimiento con políticas: muchas organizaciones estarán regidas por estándares internacionales y tienen que cumplir con los requerimientos establecidos.
2. Desarrollo: en esta fase el personal debe especificar las características técnicas del teletrabajo y el acceso remoto y debe incluir los componentes que se relacionan. Esto puede incluir los métodos de autenticación, criptografía, *firewalls* y otros componentes que establezcan los controles de seguridad necesarios. Se deben considerar todos los escenarios posibles para definir las políticas acordadas (a partir del modelo de cero confianza esto no debe cambiar nada). Finalmente, se debe evaluar y entender si las políticas pueden desplegarse y aplicarse correctamente a todos los clientes. Esta fase debe definir qué componentes se requieren para la implementación. Consideraciones adicionales para la fase de diseño:
 - a. Arquitectura: se debe considerar la arquitectura organizacional y los cambios requeridos para la implementación, así como cada componente encajará en la arquitectura actual.
 - b. Autenticación: se deben pensar en los métodos disponibles de autenticación para el modelo seleccionado y los dispositivos por implementar, así como cualquier limitación establecida en los estándares que rijan la organización.
 - c. Criptografía: se debe seleccionar el algoritmo de encriptación y protección de comunicaciones, la selección del algoritmo puede estar limitada a los equipos y estándares que rijan la organización.
 - d. Control de acceso: se deben seleccionar los tipos de acceso y el nivel permitido para cada uno, así como cuando el acceso deba denegarse.
 - e. Seguridad del dispositivo: estas son la consideración de políticas de seguridad y aplicaciones de seguridad como *antimalware* y *firewall*.

3. Implementación: en esta etapa el equipo se configura para cumplir con los requerimientos de seguridad y operacionales. Por mejores prácticas la NIST recomienda documentar toda la configuración e implementarla en un ambiente de prueba antes de su implementación en producción. La implementación incluye alterar la configuración de otros equipos o controles de seguridad, lo cual puede impactar la organización si no se prueba adecuadamente. Aspectos que deben evaluarse durante las pruebas e implementaciones:
 - a. Conectividad: se debe probar que los usuarios pueden establecer la conexión con los recursos como se espera. Eso incluye probar que no tengan acceso a los recursos no permitidos por la solución.
 - b. Protección: debe evaluar que todo tráfico o flujo de información está protegido como se estableció en los requerimientos.
 - c. Autenticación: se debe confirmar que la autenticación siempre se solicita y es necesaria para cada solicitud de acceso, todas las políticas de autenticación deben estar aplicadas y en cumplimiento. Es primordial revisar que la autenticación está configurada y funciona como se desea.
 - d. Aplicaciones: se debe probar que las aplicaciones involucradas funcionan adecuadamente por acceso remoto y local.
 - e. Administración: se debe confirmar que la gestión se puede llevar a cabo exitosamente para cada componente involucrado en el proceso.
 - f. Registros: se debe comprobar que los registros se llevan a cabo y que la integración con otros componentes funciona según lo indicado.
 - g. Rendimiento: parte de las pruebas es comprobar que las diferentes horas de operación organizacional no afectan el rendimiento o la experiencia de los empleados en teletrabajo. Algo importante es considerar días de actualización, lo cual suele cargar la red organizacional junto con el tráfico usual.
 - h. Implementación de la seguridad: la implementación de teletrabajo puede generar más vulnerabilidades y debilidades en la seguridad organizacional y

algunas organizaciones pueden optar por llevar a cabo una prueba extensiva de vulnerabilidades en los nuevos dispositivos o escenarios introducidos a la organización.

- i. Configuración por defecto: se debe revisar y confirmar que ninguna de las configuraciones por defecto de los componentes implementados sigue en funcionamiento y han sido reemplazadas por las nuevas definidas por la organización. Esto puede incluir puertos que se utilizan por servicios, ya que usarlos en su puerto natural puede facilitarle el trabajo a un sujeto mal intencionado.
4. Operaciones y mantenimiento: esta fase debe incluir las tareas relacionadas con seguridad que la organización debe llevar a cabo periódicamente una vez que la solución está en producción, como revisión de registros, detección de ataques, respuesta a incidentes y recuperación. Todas estas tareas deben estar documentadas en una Política de Gestión de la Configuración. Algunas de las actividades que se deben llevar a cabo en esta etapa son:
 - a. Confirmar que las actualizaciones se aplican correctamente y que siguen el diseño de la propuesta.
 - b. Confirmar que el reloj de todos los componentes involucrados está sincronizado. Esto es importante para relacionar los registros adecuadamente.
 - c. Reconfigurar cualquier control como sea necesario, como lo determinen los controles o pruebas conducidas por la organización.
 - d. Detectar y documentar las anomalías detectadas en la infraestructura de teletrabajo.
 5. Eliminación o remoción: esta etapa entra en vigor una vez que la solución ha sido implementada y sucede cuando alguno de los componentes de la solución se retira, necesita actualizarse, limpiarse o desecharse. Deberá documentar como la organización realiza lo cambios en su solución.

2.2.1.5. Recomendación de la NIST para los empleados realizando teletrabajo. La

NIST tiene una publicación la Seguridad Básica para Teletrabajo (Greene, 2020) que está enfocada en los empleados y no necesariamente en las organizaciones, pero puede utilizarla como una guía para la construcción de una cultura organizacional en el teletrabajo. Estas recomendaciones aplicarían para cualquier dispositivo.

1. Conocer las políticas de ciberseguridad organizacional, entenderlas y corroborarlas, de manera que se pueda saber si el dispositivo cumple estas políticas.
2. Proteger la red de casa, los empleados deberían utilizar seguridad WPA2 o WPA3, tener una contraseña segura (ojalá utilizando las mismas reglas que la organización utiliza para la contraseña de inicio de sesión). La organización puede ayudar a sus empleados para asegurarse de que cumplen con la configuración de la red. la publicación de la NIST no lo establece, pero debe ayudarles a configurar el punto de acceso correctamente y revisar que este no esté configurado por defecto y que una persona pueda acceder a su configuración.
3. Asegurarse de utilizar la VPN organizacional. La publicación de la NIST indica que el usuario puede configurar una, pero esto no se alinea con el modelo de cero confianza.
4. Cuando se utilizan dispositivos ajenos a la organización, el usuario debe asegurarse de que cumple con la configuración de seguridad base. La organización puede dar guías y asistencia si se permitiera el uso de estos dispositivos.
5. Mantener todos los dispositivos que se utilizan para trabajar actualizados. La compañía debe soportar estas acciones en los dispositivos empresariales. Para dispositivos externos la organización puede dar guías para soportar a los sujetos con dispositivos externos.
6. Reportar cualquier actividad inusual en los dispositivos que se utilizan para teletrabajo, la organización debe comunicar las fuentes de comunicación en caso de dudas o problemas de seguridad.

2.2.1.6. Consideraciones de seguridad para el intercambio de archivos en Internet.

Otra publicación que se puede destacar es el boletín informativo de la NIST, IITL: Security Considerations for Exchanging Files Over the Internet (Scarfone, Schol y Souppaya, 2020) que expone los escenarios que se pueden dar en una organización al compartir información, sea de manera remota o interna y trata de discutir como los usuarios pueden compartir archivos importantes por correo o medios gratuitos de transferencia de archivos. El teletrabajo incrementa esta transferencia de archivos, por las razones obvias al no estar todos los empleados en un mismo lugar y no mostrar nuestra pantalla o imprimir un informe para compartirlo personalmente, todas estas acciones en el ambiente de teletrabajo se hacen por medios digitales.

2.2.1.6.1. Consideraciones de seguridad para mejorar el intercambio de archivos.

Muchos métodos de intercambio actuales tienen opciones de seguridad deficientes, algunos no tienen o poseen métodos de encriptación débiles y algunos no validados por FIPS (la NIST establece que se deben asegurar los datos utilizando métodos validados por FIPS, Federal Information Processing Standards o en español el estándar federal de procesamiento de información). Utilizar estos métodos no seguros puede exponer la información y ser víctimas de algún método de escaneo, lectura o captura de los datos en las redes que estos atraviesan. En algunos casos las organizaciones almacenan estos datos en servidores seguros o proveedores que no brindan la seguridad de los datos almacenados y pueden guardar copias de estos. Lo que propone la NIST para mejorar la seguridad en el intercambio de archivos es lo siguiente:

- Las organizaciones deben identificar todos los usuarios que necesitan compartir datos, los que envían y los que reciben, tanto si es dentro o fuera de la organización y es importante saber la naturaleza de la información.
- Las organizaciones deben solucionar las necesidades del intercambio de archivos, considerando la seguridad y la usabilidad, también es importante educar a los usuarios para que puedan utilizar adecuadamente la solución.
- Cuando se utilizan métodos criptográficos para proteger la confidencialidad e integridad de los archivos y su intercambio, las organizaciones deben implementar los algoritmos aprobados por la NIST y validados por FIPS.

- Las organizaciones deben monitorear que los controles y las soluciones aprobadas que se utilizan. La organización debe detectar el uso de otros métodos y solucionar esto antes de que se vea comprometida la organización.
- Las organizaciones deben responder efectivamente si se ve comprometida la información.

2.2.1.6.2. *Posibles soluciones para asegurar el intercambio de archivos.* La NIST lista una serie de soluciones agrupadas por método de transmisión, puede que algunas organizaciones utilicen otros métodos o soluciones híbridas. La organización debe evaluar cuidadosamente la seguridad y usabilidad de la solución, el objetivo principal debe ser salvaguardar la confidencialidad e integridad de los archivos en tránsito y en algunos casos estas soluciones pueden ayudar a asegurar los datos en reposo.

- Correos electrónicos: es uno de los métodos de transmisión más popular porque es conveniente, rápido y universal; solo se necesita un correo electrónico, casi todas las organizaciones cuentan con este o los usuarios tienen una cuenta personal, usualmente estos métodos no tienen ninguna seguridad para la transmisión de esta información. Algunas de las opciones para proteger la información en correos electrónicos son:
 - Comprimir y encriptar los archivos adjuntos: se puede utilizar una herramienta para encriptar y comprimir el archivo, el receptor requeriría conocer la contraseña, la cual no debe ser una contraseña fácil y debe transmitirse seguramente al receptor (lo cual incrementar la superficie de ataque).
 - Utilizar la característica de encriptación de la solución de correo: en algunas soluciones de correo electrónico los clientes y el servidor pueden encriptar los correos electrónicos organizacionales, sean de la organización o no, si el receptor del correo es externo, tendría que utilizar un portal para acceder su contenido.
 - Utilizar el estándar de llave de encriptación para correos electrónicos: como S/MIME (Secure/Multipurpose Internet Mail Extensions o en español

extensiones seguras/multipropósito de correo electrónico). Esto requiere clientes de correo y no utilizar portales *web*. Esto puede presentar limitaciones, como cuando se envían correos fuera de la organización.

- Uso de servicios o productos de encriptación de terceros: las funcionalidades de estos proveedores varían mucho, algunas pueden encriptar los correos, los archivos o solo archivos sensibles según las características.
- Servicios de archivos compartidos: esto puede incluir un ambiente de archivos compartidos con varios servidores que soportan la transmisión de archivos. Muchos de estos servicios son en la nube, lo cual puede indicar que el proveedor puede tener acceso a estos, por lo que se recomienda verificar las políticas y obligaciones contractuales con el proveedor.
- Soluciones de gestión de transferencia de archivos: estas soluciones son específicas para la transferencia segura de archivos. Por lo general permiten la administración, automatización, monitoreo y registro de las actividades de transferencia de archivos en la organización. Muchas incluyen encriptación, revisión de integridad, autenticación y auditoría y ofrecen características de cumplimiento con estándares internacionales.
- Aplicaciones móviles o aplicaciones *web* personalizadas: muchas organizaciones desarrollan su propia solución particular para asegurar el intercambio de archivos o usan clientes para dispositivos móviles, todas estas utilizan HTTPS para encriptar la transferencia.

2.2.1.6.3. Soluciones posibles para detectar el intercambio inadecuado de archivos protegidos. Como se mencionó, es importante detectar las fallas al proteger apropiadamente los archivos.

- Soluciones de DLP (Data Loss Prevention o en español prevención de pérdida de datos), estas soluciones pueden monitorear redes, dispositivos clientes y algunas aplicaciones cuando se transfieren archivos sensibles.

- Sistemas de detección y prevención de intrusiones a la red, así como un *firewall* y otros controles de red que pueden monitorear el tráfico de red o identificar el uso inadecuado de las aplicaciones de transmisión de archivos.
- Registros de los servidores de correo electrónico y otros servidores de transferencia de archivos, de los archivos transferidos y cuales estaban protegidos y cuáles no.
- Soluciones de CASB (Cloud Access Security Broker o en español agente de seguridad para el acceso a la nube) es una solución que monitorea el intercambio de archivos con otros componentes en la nube y puede dar visibilidad a las aplicaciones en la nube y los riesgos asociados.

2.3. PCI

La PCI (Payment Card Industry) Security Standards Council o español el Consejo de Estándares de Seguridad para la Industria de Tarjeta de Pago, establece una serie de reglas que deben cumplir las organizaciones que utilizan tarjetas de crédito como método de pago, con el fin de proteger la información de los dueños de las tarjetas procesadas por la organización. De las vulnerabilidades detectadas por PCI algunas aplican en ambientes de teletrabajo, esta es la lista de las posibles vulnerabilidades:

- Dispositivos de punto de ventas.
- Dispositivos móviles, computadoras personales y servidores.
- Puntos de conexión *wireless*.
- Aplicaciones *web* de compra.
- Sistemas de almacenamiento físico.
- Transmisión de los datos de tarjetas a los proveedores.
- Conexiones remotas.

Para cumplir con el cumplimiento de PCI se debe:

- Evaluar: identificar todas las ubicaciones donde está la información del dueño de la tarjeta, llevar a cabo un inventario de los activos de TI y negocio involucrados en el proceso de pago. Parte de la evaluación es analizar las vulnerabilidades de estos dispositivos que pueden exponer información de los clientes.
- Reparar: reparar las vulnerabilidades identificadas, remover de manera segura la información del cliente e implementar procesos de negocio seguros.
- Reportes: se deben documentar los detalles de las evaluaciones y remediaciones para reportar posteriormente el cumplimiento a la organización dueñas de las tarjetas de crédito.

Adicionalmente, los Estándares de Seguridad de la PCI incluyen diferentes estándares:

- PCI Estándar de Seguridad de Datos: aplica para todas las entidades que almacenan, procesan y transmiten información de tarjetas de crédito.
- Requerimientos de Seguridad de Transacciones con PIN: son un grupo de requerimientos de características y administración de dispositivos que se utilizan para la protección del PIN de los clientes y otros procesos de pago.
- Estándar de Seguridad de Datos de la Aplicación de Pago: está enfocada en desarrolladores de *software* que almacenen, procesen, transmitan información de tarjetas o información sensible de autenticación.
- Estándar de Encriptación Punto a Punto de PCI: provee un *set* de requerimientos para conexión de punto a punto.
- Requisitos de seguridad lógica de producción de tarjetas PCI y requisitos de seguridad física: es un grupo de buenas prácticas para los fabricantes y productores de tarjetas.
- Requisitos de seguridad del proveedor de servicios de *token* de PCI: este se enfoca en los proveedores de servicios de pagos por *tokens*.

2.3.1. PCI Estándar de Seguridad de Datos. De estos estándares de la PCI solo el

PCI Estándar de Seguridad de Datos aplica abiertamente para muchas organizaciones, los demás estándares son organizaciones muy específicas, en este se incluye cualquier organización que almacene o transmita información sensible del dueño de una tarjeta, aunque muchas de las ventas se realicen desde plataformas *web* o locales, con el teletrabajo esto puede haber cambiado en algunas organizaciones. A continuación, se detallan las metas y los requerimientos establecidos por las PCI:

1. Construir y mantener una red y sistemas seguros.
 - a. Instalar y mantener un *firewall*.
 - b. No usar configuración por defecto.
2. Proteger la información personal de los dueños de tarjetas.
 - a. Proteger la información almacenada de tarjetas.
 - b. Encriptar la transmisión de información de tarjeta en todo tipo de redes.
3. Mantener un programa de gestión de vulnerabilidades.
 - a. Proteger todos los sistemas contra *malware* y actualizar regularmente el *software* antivirus y los programas.
 - b. Desarrollar y mantener sistemas y aplicaciones seguras.
4. Implementar medidas de control de acceso fuertes.
 - a. Restringir el acceso a la información de tarjetas solo para necesidades de negocio.
 - b. Identificar y autenticar el acceso a los componentes.
 - c. Restringir físicamente los accesos donde se almacene información de tarjetas.
5. Monitorear y probar las redes regularmente.
 - a. Rastrear y monitorear el acceso a los recursos de red y la información de tarjetas de crédito.
 - b. Regularmente, probar los sistemas de seguridad y los procesos.

6. Mantener una política de seguridad de información.
 - a. Mantener una política que gestione la seguridad de información de todo el personal y la organización.

2.3.1.1. Implementar y mantener sistemas y redes seguras bajo el cumplimiento de la PCI DSS. PCI establece una serie de requerimientos que deben existir para cumplir con el estándar:

1. Instalar, configurar y mantener un *firewall* para proteger la información de tarjetas, el *firewall* debe controlar el tráfico que entra y sale de la organización, incluso entre áreas más sensibles dentro de la organización.
 - a. Establecer e implementar estándares de configuración de *firewalls* y enrutadores e identificar todas las conexiones entre ambientes y redes donde se comparta información de tarjetas, documentar y crear diagramas de estas interacciones, debe también contener la justificación de negocio y las configuraciones técnicas para cada implementación. La revisión de la configuración y la documentación debe suceder cada 6 meses.
 - b. Desarrollar configuraciones de *firewall* y enrutadores que restrinjan toda entrada y salida de tráfico no confiable de las redes y de los clientes y solo permitir los protocolos necesarios para las operaciones de negocio en el ambiente (en cero confianza todas las redes serías considerable no confiables por lo que se aplicaría este punto en todas las redes).
 - c. Prohibir el acceso directo desde Internet a cualquier componente del sistema con información de cliente de tarjetas.
 - d. Instalar un *firewall* personal o equivalente en cualquier dispositivo que se conecte con Internet o fuera de la red organizacional y tenga acceso a información de clientes.
 - e. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.

2. No utilizar la configuración por defecto de los componentes de seguridad, como contraseñas y parámetros de seguridad.
 - a. Siempre se deben cambiar todas las configuraciones por defecto y desactivar todas las características o cuentas que no estén en uso.
 - b. Configurar todos los componentes y corregir todas las vulnerabilidades conocidas y en consistencia con las definiciones de la industria. Definir un plan para actualizar y corregir cualquier nueva vulnerabilidad.
 - c. Usar una fuerte criptografía y aprobada por las NIST.
 - d. Mantener un inventario de todos los componentes involucrados en el proceso de tarjetas.
 - e. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
 - f. Los proveedores deben proteger la información de los clientes de tarjetas.
3. Proteger los datos de los dueños de tarjetas, esto puede incluir cualquier medio donde se almacene la información y debe prevenir el uso sin autorización de estos. Esta información no debe almacenarse al menos que sea necesario y una vez no se utilice deben removerse y no usarse.
 - a. Limitar el almacenamiento y tiempo de retención de información de tarjetas al tiempo que sea solamente el requerido para el negocio o por razones legales o regulatorias y que conste en la documentación de la política de retención de datos. Se debe purgar toda la información no necesaria al menos cada cuarto de año.
 - b. No se debe almacenar información sensible después de la autorización. Toda información sensible de autenticación debe limpiarse y ser irrecuperable.
 - c. Se debe enmascarar el número de tarjeta si por alguna manera se muestra, solo personas con alguna justificación de negocio deben ver el número completo.

- d. Cuando se almacene el número de tarjeta debe guardarse, de manera que no sea leíble en cualquier medio donde se almacene. Para esto, se pueden usar muchos métodos como *tokens* o criptografía.
 - e. Documentar e implementar los procedimientos necesarios para proteger las llaves de encriptación.
 - f. Documentar e implementar los procesos y procedimientos necesarios para la administración de llaves de encriptación.
 - g. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
4. Encriptar la transmisión de datos de tarjeta en redes públicas o no seguras, esto puede asegurar que el tráfico interceptado no sea leíble.
- a. Usar una criptografía fuerte y protocolos de seguridad para proteger la información de tarjeta durante su transmisión en medios abiertos o redes públicas.
 - b. Nunca enviar información de tarjetas por medio de tecnologías como correo electrónico, mensajes instantáneos, SMS, *chats*, entre otros.
 - c. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
5. Proteger todos los sistemas contra vulnerabilidades y actualización regularmente el *antimalware* y programas.
- a. Desplegar *software antimalwe/antivirus* en todos los sistemas que puedan ser afectados por estos. (Bajo cero confianza serían todos).
 - b. Asegurarse que todos los mecanismos de *antimalware/antivirus* están actualizados, realizan escaneos periódicos y generan registros de auditoría.
 - c. Asegurarse que los mecanismos de *antimalware/antivirus* se encuentran activamente en ejecución y que no pueden ser deshabilitados o modificados por usuarios.

- d. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
6. Desarrollar y mantener sistemas y aplicaciones de manera segura, se deben mitigar las vulnerabilidades en estos sistemas, muchos proveedores liberan actualizaciones de seguridad periódicas que ayudan a minimizar muchas de estas vulnerabilidades y se debe documentar el proceso de actualización sin impactar servicios críticos, además de utilizar procedimientos de control de cambios (como ITIL).
- a. Establecer un procedimiento para la identificación de vulnerabilidades de seguridad y evaluar los riesgos de estas.
 - b. Proteger todos los sistemas y *software* de las vulnerabilidades conocidas por medio de la configuración o actualización necesaria. Instalar actualizaciones no más tarde de 1 mes.
 - c. Desarrollar aplicaciones internas y externas siguiendo las prácticas de PCI DSS y de la industria.
 - d. Seguir los procesos y procedimientos de control de cambios con todos los componentes y asegurarse de que estos cambios cumplan los requerimientos establecidos por la PCI DSS.
 - e. Prevenir vulnerabilidades comunes en el código durante el proceso de desarrollo y entrenar a los desarrolladores en buenas prácticas en el desarrollo seguro.
 - f. Asegurar las aplicaciones externas de la organización de ataques conocidos, por medio de evaluaciones de vulnerabilidades al menos una vez al año y después de cada cambio. Se pueden utilizar controles automatizados.
 - g. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
7. Restringir el acceso a la información de los usuarios de tarjetas a solo en caso de que sea necesario por el negocio. Debe existir una limitación de las

responsabilidades de cada sujeto en la organización y se debe conocer el mínimo de información que este sujeto necesita consultar.

- a. Limitar el acceso a los sistemas y datos personales de tarjetas a solo aquellos que lo requieren para su trabajo.
 - b. Establecer un sistema de control de acceso para los sistemas que restringen el acceso.
 - c. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
8. Identificar y autenticar el acceso a los sistemas.
- a. Definir e implementar políticas y procedimientos para asegurar la gestión apropiadas de la identificación de usuarios y administradores en todos los sistemas. Cada usuario debe ser identificable y cada sujeto debe tener su propia cuenta.
 - b. Desplegar al menos uno de estos controles para autenticar todos los usuarios, todas las contraseñas o datos de autenticación deben almacenarse con un algoritmo de encriptación fuerte:
 - i. Algo que ellos sepan: contraseña, frase, etc.
 - ii. Algo que ellos tengan: *token*, tarjeta inteligente, etc.
 - iii. Algo que ellos sean: como biométricos.
 - c. Asegurar todos los accesos administrativos individuales y todos los accesos remotos al ambiente o los sistemas involucrados en el almacenamiento/procesamiento de datos de tarjetas con MFA. MFA se considera el uso de alguno de los métodos descritos en el punto anterior, pero no se pueden requerir dos veces, solicitar dos contraseñas no cuenta como MFA.
 - d. Desarrollar, implementar y comunicar las políticas y procedimientos de autenticación a todos los usuarios.

- e. No se deben usar ID genéricos, compartidos, agrupados u otros métodos de autenticación. Todos los usuarios, sean internos o no, deben tener sus propias credenciales de autenticación.
 - f. Se deben usar otros mecanismos de autenticación como *tokens* físicos, tarjetas inteligentes y certificados asignados a usuarios individualmente.
 - g. Todo acceso a cualquier base de datos con información de tarjetas debe ser restringido. Solo administradores de bases de datos deberían ejecutar consultas en la misma y los ID/cuentas de aplicaciones solo deben utilizarse por las aplicaciones y no por usuarios.
 - h. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
9. Restringir acceso físico a la información de tarjetas.
- a. Usar la infraestructura apropiada para establecer los controles necesarios que limiten y monitoreen el acceso físico a los sistemas que almacenas la información de tarjetas.
 - b. Desarrollar los procedimientos necesarios para diferenciar entre personal interno y externo, como identificaciones.
 - c. Controlar el acceso físico para el personal interno en áreas sensibles y el acceso se aprueba cada vez que el individuo ocupe acceso y cualquier mecanismo para autenticar debe retornarse o debe marcar como inválidas una vez que la tarea haya terminado.
 - d. Asegurar que todos los visitantes que se les haya autorizado el acceso donde la información de tarjetas se procesa o almacena, tengan una identificación física u otra identificación que expire cuando el personal ya no se encuentre en las instalaciones. Se debe tener un registro físico de acceso y actividad, lo que incluye nombre del visitante, compañía y el acompañante interno. Estos registros deben guardarse por al menos 3 meses, a menos que haya otras restricciones legales.

- e. Físicamente, asegurar toda fuente de datos, como las ubicaciones y componentes donde se almacenen los respaldos. Preferiblemente, los respaldos deben almacenarse en otra ubicación.
 - f. Mantener control estricto sobre cualquier distribución interna o externa de fuentes de almacenamiento, como almacenamiento USB o discos.
 - g. Mantener control estricto sobre el almacenamiento y la disponibilidad de fuentes de información.
 - h. Destruir cualquier fuente de información que ya no se necesite por razones de negocio o legales.
 - i. Proteger los dispositivos que capturan información de tarjetas, de manera directa o física. Estos deberían incluir revisiones periódicas.
 - j. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
10. Monitorear y rastrear todos los accesos a la red o a los datos de tarjetas, los mecanismos de registro y la habilidad de registrar la actividad de usuarios es crítica para la eficacia de tareas forenses y gestión de amenazas. Cuantos más registros, más fácil será determinar la causa de algún problema o alguna amenaza en la red.
- a. Implementar registros de auditoría para relacionar todos los sistemas con los usuarios ejecutando tareas en ellos.
 - b. Implementar registros de auditoría automáticos para todos los sistemas y reconstruir eventos como:
 - i. Accesos individuales a datos de tarjetas.
 - ii. Todas las acciones hechas por un administrador o por un usuario con derechos raíz (*root*).
 - iii. Acceso a los registros.
 - iv. Intentos fallidos de acceso.

- v. Intentos y cambios de autenticación e identificación.
 - vi. Cambios, creaciones y borrado de cuentas con algún privilegio superior.
 - vii. Detención o pausa del registro automático de auditoría.
 - viii. Creación y borrado de objetos de sistema.
- c. Grabar registros de auditoría de todos los sistemas y de cada evento, lo que incluye como mínimo identificación de usuarios, tipo de eventos, fecha y tiempo, indicación de éxito o fallo, origen del evento, identidad del sistema o recurso afectado, componentes o recurso que creó el evento.
 - d. Usar tecnología de sincronización de tiempo, todas las horas de los sistemas críticos y de los controles implementados deben ser iguales para relacionar efectivamente los registros.
 - e. Asegurarse que los registros de auditoría no pueden alterarse.
 - f. Revisar los registros y eventos de seguridad para todos los sistemas que detecten anomalías o actividades sospechosas. Se deben revisar los registros críticos al menos una vez al día.
 - g. Retener el historial de los registros de auditoría por al menos un año y al menos 3 meses debe estar disponible (inmediatamente) para análisis.
 - h. Los proveedores de servicio deben implementar un proceso de detección y reporte de las fallas de los controles de seguridad críticos.
 - i. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.
11. Llevar a cabo pruebas de seguridad en los procesos y sistemas de seguridad, las pruebas de seguridad son necesarias, ya que todos los días se detectan nuevos ataques y vulnerabilidades, estas pruebas deben probar todas las nuevas tendencias en cuanto a ataques y vulnerabilidades descubiertas por el fabricante.
- a. Implementar un proceso de revisión de puntos de acceso Inalámbrico, detectar e identificar todos los puntos de acceso autorizados y no autorizados. Tener

un inventario de puntos de acceso e implementar procedimientos de respuesta a incidentes en caso de puntos de acceso no autorizados.

- b. Ejecutar escaneos de vulnerabilidades de red internas y externas al menos una vez por cuarto y después de cualquier cambio significativo. Corregir cualquier vulnerabilidad y re escanear siempre que sea necesario hasta que no haya vulnerabilidades conocidas. Estos escaneos realizados por cuartos deben ser realizados por una persona aprobada (ASV, Approved Scanning Vendor).
- c. Desarrollar e implementar una metodología de pruebas de penetración, debe suceder al menos una vez al año y deben hacerse pruebas internas y externas, también se deben llevar a cabo después de cambios significativos. Cuando se utiliza segmentación de red, se deben hacer estas pruebas al menos una vez cada 6 meses.
- d. Se deben utilizar técnicas de prevención de detección/prevenición de intrusiones en la red interna. Se debe monitorear todo el tráfico en el perímetro del ambiente de datos de tarjetas.
- e. Desplegar un mecanismo de detección de cambios que alerte el personal de cualquier acceso no autorizado a los archivos de sistemas, archivos de configuración, archivos de contenido. Se pueden utilizar controles de comparación de archivos que pueden revisar semanalmente su integridad y levantar alertas.
- f. Documentar todas las políticas de seguridad y procedimientos operativos que se relacionan.

12. Mantener una política de seguridad de la información para todo el personal.

- a. Establecer, publicar, mantener y diseminar la política de seguridad, adicionalmente, se debe llevar a cabo la política de seguridad al menos una vez al año y se debe actualizar cuando el ambiente tenga algún cambio.
- b. Implementar un proceso de gestión de riesgos que debe ejecutarse al menos una vez al año y después de cada cambio significativo en el ambiente donde

se identifiquen activos críticos, amenazas, vulnerabilidades y debe entregar resultados de una prueba formal.

- c. Desarrollar políticas de uso para tecnologías críticas, que debe especificar el uso apropiado por todo el personal. Debe incluir acceso remoto, inalámbrico, dispositivos removibles, computadoras móviles, tabletas, dispositivos de mano, correo e Internet.
- d. Asegurarse de que las políticas y procedimientos de seguridad definan claramente las responsabilidades de seguridad de todo el personal. Los proveedores de servicio deben establecer sus responsabilidades de acuerdo con lo documentando.
- e. Asignar a los individuos o a los equipos sus responsabilidades de seguridad.
- f. Implementar un programa formal de concientización de las políticas y procedimientos de seguridad en todo el personal.
- g. Examinar todo individuo potencial antes de ser contratado para minimizar el riesgo de ataques desde fuentes internas.
- h. Mantener e implementar políticas y procedimientos para administrar a los proveedores de servicio con los cuales se comparte información de los dueños de tarjetas o que puedan influir/afectar la seguridad de esta información.
- i. Los proveedores de servicio deben aceptar la responsabilidad por escrito de la información de los dueños de tarjetas que posean, procesen y transmitan.
- j. Implementar un plan de respuesta a incidentes, que permita la rápida respuesta en caso de una brecha en el sistema.
- k. Los proveedores de servicio deben llevar a cabo y documentar todas las revisiones que se hacen cada cuarto para confirmar que el personal sigue las políticas de seguridad y los procedimientos operacionales.

2.3.1.2. Como cumplir con la PCI DSS. Cada organización y entidad que almacene, procese y transmita información de tarjetas debe cumplir con el estándar de PCI DSS, así

como toda compañía que expenda tarjetas de crédito debe seguir estos controles mínimos definidos. Las recomendaciones generales de la PCI para cumplir con los requerimientos definidos son:

- Alcance: determinar los sistemas y redes que están en el alcance de PCI DSS.
- Evaluar: Se debe examinar el cumplimiento de los sistemas y redes involucrados, sigue los requerimientos y procedimiento definidos por la PCI DSS.
- Reportar: el evaluador debe completar la documentación requerida como el SAQ (Self-Assessment Questionnaire o en español cuestionario de autoevaluación) y ROC (Reporto on Compliance o en español reporte de cumplimiento), lo que incluye toda la documentación de los controles de compensación.
- Certificar: completar apropiadamente el AOC (Attestation of Compliance o en español la certificación de cumplimiento).
- Enviar: Enviar el SAQ, ROC, AOC y cualquier otra documentación de soporte solicitada.
- Solucionar: Si se requiere, llevar a cabo la remediación necesaria sobre los requerimientos que no están implementados y se debe entregar un reporte de actualización de estos.

2.4. OECD

La OECD es la Organización para la Cooperación Económica y Desarrollo (Economic Co-operation and Development) según su sitio *web* (OECD) es un organismo internacional que trabaja en función de construir mejores políticas para mejores vidas. Su objetivo es diseñar las políticas que fomente la prosperidad, la igualdad, las oportunidades y el bienestar de todos. Tiene cerca de 60 años de experiencia. Esta organización junto con gobiernos, creadores de políticas y ciudadanos busca establecer estándares internacionales basados en evidencia y buscar soluciones a un gran rango social, económico y ambiental. La OECD no establece ninguna norma de cumplimiento, pero ha publicado diversos trabajos y publicaciones de mejores prácticas y recomendación relacionadas con tecnologías, las publicaciones en su mayoría están enfocadas en los productores de tecnología. Se realiza una

búsqueda sistemática de las mejores prácticas recomendadas por este ente que sean referentes para esta investigación.

2.4.1. Entendimiento de la seguridad digital de los productos: un análisis profundo. Del documento mencionado de la OECD (OECD, 2021) se pueden destacar unas claves para la definición de políticas de seguridad y las definiciones del riesgo digital.

2.4.1.1. Información clave para los creadores de políticas de seguridad. Algunos de los principales hallazgos de los casos de estudios durante el último año 2021/2020 son:

- Los dispositivos IoT (Internet of Things, en español Internet de las cosas) para consumidor tienen huecos de seguridad significativos, en todas sus etapas de ciclo de vida.
- En todos los casos de estudio de productos para consumidores los huecos de seguridad por mala configuración o por no instalación de actualizaciones de seguridad.
- Cuando los productos alcanzan el final de su vida útil dada por el fabricante o soporte son mayores en producto IoT y teléfonos inteligentes y es menor para servicios en la nube, también porque muchos de estos mantienen mayor soporte u opciones de migración cuando llegan a su fin de soporte.
- Huecos de seguridad durante el diseño y despliegue son significativos en nuevos productos, como IoT donde muchos tienen limitaciones de seguridad por diseño o por defecto y muchas de las opciones de seguridad no son las que se utilizan. Estos huecos de seguridad son menos comunes en mercados/productos más maduros como computadoras y teléfonos inteligentes.

2.4.1.2. Recomendaciones de la OECD en relación con la criptografía. Estas recomendaciones están en otra publicación localizar en el *blog* legal llamado Recommendation of the Council concerning Guidelines for Cryptography Policy (OECD Legal, 1997) (recomendación del consejo sobre las directrices para las políticas de criptografía) que están enfocadas en las recomendaciones para los países miembros en cuanto a la criptografía, la lista a continuación:

1. Establecer nuevas, adicionales, políticas, métodos, medidas, prácticas y procedimientos que reflejen y tomen en cuenta los principios que se relacionan con las pautas para políticas de criptografía.
2. Consultar, coordinar y cooperar en las pautas en el ámbito internacional y nacional.
3. Actuar en la necesidad de soluciones prácticas y operacionales en el área de las políticas internacionales de criptografía.
4. Diseminar las pautas en los sectores públicos y privados para promover el conocimiento de los problemas y políticas relacionadas con la criptografía.
5. Remover y evitar obstáculos a tratados internacionales en el proceso de creación de políticas de criptografía.
6. Declarar o publicar cualquier control establecido nacionalmente a la organización.
7. Revisar las pautas al menos una vez cada 5 años, con el objetivo de mejorar la cooperación en problemas que se relacionan con las políticas de criptografía.

2.4.1.2.1. Pautas para políticas de criptografía. Estas Pautas de OECD se crearon para promover el uso de la criptografía, crear conciencia en la necesidad de políticas de criptografía y leyes relacionadas con la criptografía, asistir a los responsables de tomar decisiones en el Sector Público y privado para implementar metodologías de criptografía que sean coherentes con las políticas nacionales e internacionales y promover la cooperación entre el Sector Público y privado.

Su alcance es primordialmente gubernamental, pero también contempla el Sector Público y privado, ya que el documento establece que el cambio debe iniciarse desde el gobierno primero.

El texto también destaca una serie de principios que deben considerarse:

- 1. Confiar en la criptografía:** los métodos deben ser confiables para generar el sentimiento de confianza en el uso de sistemas de comunicación e información.

2. **Seleccionar el método de criptografía:** los usuarios u organizaciones tienen el derecho de seleccionar cualquier método de criptografía que sea aplicable según las leyes y los estándares internacionales.
3. **Desarrollo de métodos criptográficos impulsados por el mercado:** los métodos criptográficos deben desarrollarse como respuesta a las necesidades, demandas y responsabilidades de los individuos, negocios y gobiernos.
4. **Estándares para métodos de criptografía:** se deben desarrollar y promulgar en el ámbito nacional e internacional estándares técnicos, criterios y protocolos para los métodos criptográficos.
5. **Protección de los datos privados y personales:** uno de los derechos fundamentales de cada individuo es la privacidad, incluido el secreto de sus comunicaciones y la protección de sus datos personales. Estos deben ser respetados por cualquier método de criptografía.
6. **Acceso legal:** las políticas nacionales de criptografía pueden permitir el acceso legal en texto plano o de llaves criptográficas de la información encriptada.
7. **Responsabilidad:** cuando sea establecido por un contrato o legislación, la responsabilidad de los individuos y entidades que ofrezcan algún servicio criptográfico debe ser clara.
8. **Cooperación internacional:** los gobiernos deben cooperar y coordinar las políticas de criptografía y evitar obstáculos comerciales sobre las organizaciones públicas y privadas.

2.4.1.3. Riesgo digital de seguridad. El riesgo digital de seguridad es resultado de la combinación de amenazas y vulnerabilidades, las cuales pueden resultar en incidentes que impacten la confidencialidad, integridad y disponibilidad de la información, productos y redes, los cuales pueden impactar económica y socialmente a la organización. Las vulnerabilidades son inherentes al código, diseño o implementación de un producto, las amenazas existen de forma independientemente y no están relacionadas directamente con un producto.

2.4.1.3.1. *Debilidades, vulnerabilidades y malas configuraciones.* El riesgo digital tiene dos tipos principales de vulnerabilidades que son vulnerabilidades de código y de configuración. Las vulnerabilidades de código son generalmente definidas por una debilidad dentro del código fuente del producto, el cual puede ser explotado por una amenaza y causar danos. Las vulnerabilidades de diseño como su arquitectura o limitaciones técnicas suelen ser difíciles de arreglar, ya que suelen ser limitadas por el *hardware* del producto, por lo general requiere un rediseño del producto. Las vulnerabilidades por configuración se pueden definir como una incorrecta o una configuración subóptima de un sistema o un componente dentro de un sistema que puede causar una vulnerabilidad, estas requieren un contexto específico, por el otro lado las de código siempre estarán ahí sin importar su configuración y, finalmente, las malas configuraciones no requieren una actualización, sino reconfigurarse correctamente.

La OECD también destaca que no todos los errores en el código son vulnerabilidades de las cuales un tercero se pueda aprovechar, pero puede afectar a la organización de otras maneras. Además, algunas vulnerabilidades son teóricas, se cree que puede existir o se puede llevar a cabo, pero no existe un código (en ese momento) para explotar esa vulnerabilidad o también puede que no sea tan fácil o necesite de otros factores.

2.4.1.3.2. *Amenazas, exploits y AIC (Availability, Integrity and Confidentiality).* Las amenazas pueden ser intencionales y no intencionadas (errores de usuarios, fallas en los servicios o desastres naturales) y los incidentes de seguridad digital pueden ser provocados por ambas, pero los ataques son solo ocasionados por las amenazas intencionales.

Cuando un sujeto se aprovecha de una vulnerabilidad usa un *exploit*, muchas veces un *exploit* es un código o un programa que está diseñado específicamente para usar una o varias vulnerabilidades. El impacto técnico de la seguridad digital usualmente se categoriza por como afecte la disponibilidad, integridad o confidencialidad de un producto, dato o red, a esto se le conoce como AIC (en español disponibilidad, integridad y confidencialidad).

2.4.2. Mejorando la seguridad digital en los productos: una discusión de políticas. Este texto (OECD, 2021) al igual que el texto anterior está se centra en el desarrollo de tecnologías y sus limitaciones o mejores prácticas y no en las organizaciones o al teletrabajo. De este documento se pueden destacar ocho puntos para el manejo del riesgo, el

cual puede implementarse en cualquier organización, ya que se alinea con muchos estándares de buenas prácticas.

2.4.2.1.1. Principios de las recomendaciones de la OECD en la gestión del riesgo de la seguridad digital. La OECD sugiere los siguientes ocho puntos para considerarse cuando se maneja el riesgo de la seguridad digital en una organización:

1. Conciencia, habilidades y empoderamiento: todas las partes interesadas deberían entender los riesgos de la seguridad digital y cómo manejarlo.
2. Responsabilidad: todas las partes interesadas deben tomar responsabilidad por la gestión del riesgo de la seguridad digital.
3. Derechos humanos y valores fundamentales: todas las partes interesadas deben manejar los riesgos de la seguridad digital, de una manera transparente y consistente con los derechos humanos y los valores fundamentales.
4. Cooperación: todas las partes interesadas deben cooperar, esto incluye equipos en otras ubicaciones geográficas.
5. Manejo de riesgos y ciclo de evaluación: los líderes y los que toman decisiones deben asegurarse de que el riesgo de la seguridad digital debe tratarse como parte de la evaluación continua de riesgos.
6. Medidas de seguridad: los líderes y los que toman decisiones deben asegurarse de que las medidas de seguridad son apropiadas, de acuerdo con los riesgos.
7. Innovación: los líderes y los que toman decisiones deben asegurarse de que la innovación se considera constantemente.
8. Preparación y continuidad: los líderes y los que toman decisiones deben asegurarse de que se ha adoptado un plan de preparación y continuidad.

2.5. ISO

2.5.1. ISO/IEC 27000:2018. A continuación, se define la norma ISO/IEC 27000:2018.

2.5.1.1. Generalidades. Esta normativa (ISO/IEC, 2018) aplica a organizaciones de todos los tipos y tamaños, que obtengan, procesen, almacenen y transmitan información, toda la información es importante y puede asociarse con procesos, sistemas, redes y personas que son activos importantes para lograr los objetivos de la empresa. Todos estos actores y activos corren el riesgo de ser afectados y se pueden implementar controles de seguridad de la información. Esta es la primera publicación de la familia 27000 y da base a los demás estándares de la familia.

2.5.1.2. Seguridad de la Información. Según la ISO la seguridad de la información se define como el asegurar la confidencialidad, disponibilidad e integridad (mencionada por la NIST y DoD, de manera similar) de la información. La seguridad de la información incluye las aplicaciones y la gestión apropiada de los controles que deben considerar una gran cantidad de amenazas y su objetivo es asegurar el éxito del negocio y su continuidad, además de minimizar las consecuencias de los incidentes que puedan suceder.

2.5.1.3. ISMS (*Information Security Management System*). En este estándar se habla del ISMS (sistema de gestión de la seguridad de la información), el ISMS consiste en políticas, procedimiento, pautas, recursos asociados y actividades que colectivamente administran la organización en función de la protección de los activos de información. El ISMS es una búsqueda sistemática para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de los activos de información de la organización, en función de cumplir los objetivos del negocio. Este se basa en la evaluación del riesgo y el riesgo aceptado por la organización. Sus principios son:

- Conciencia en la necesidad de la seguridad de la información.
- Asistir en las responsabilidades de la seguridad de la información.
- Incorporar el compromiso de la gestión y de los intereses de las partes involucradas.
- Mejorar los valores sociales.
- Ejecutar evaluaciones de riesgos que determinen los controles apropiados según los niveles aceptables de riesgo.

- Incorporar la seguridad como un elemento esencial en los sistemas y redes de información.
- Implementar una activa prevención y detección de incidentes de seguridad.
- Implementar un enfoque integral de la gestión de la seguridad de la información.
- Reevaluar, de manera continua, la seguridad de la información y llevar a cabo las modificaciones apropiadas.

2.5.1.3.1. Implementando un ISMS. Una organización que desee establecer un ISMS tiene que:

1. Identificar los activos de información y sus requerimientos de seguridad de la información asociados.
2. Evaluar los riesgos de seguridad de la información y los riesgos de las amenazas de seguridad de la información.
3. Seleccionar e implementar los controles relevantes para gestionar los riesgos no aceptables.
4. Monitorear, mantener y mejorar la eficacia de los controles asociados con los activos de la organización.

2.5.2. ISO/IEC 27001:2013. La 27001 (ISOTools) es una norma enfocada en la seguridad de la información y la mejora continua y habla de la definición e implementación de una SGSI (sistema de gestión de seguridad de la información) que buscara evaluar todo tipo de riesgos o amenazas que pueden poner en peligro la información de la organización. La implementación de una SGSI permite establecer los controles y estrategias más adecuada para eliminar y minimizar estos riesgos. Como casi todas las normas de la ISO se basa en un método de mejora continua.

2.5.2.1. Fases de un SGSI basado en ISO27001. Si una organización tiene un SGSI implementado en su organización debe pasar por las siguientes fases para implementarlo como la norma establece:

1. Análisis y evaluación de riesgos.

2. Implementación de controles.
3. Definición de un plan de tratamiento de los riesgos o esquema de mejora.
4. Alcance de la gestión.
5. Contexto de organización.
6. Partes interesadas.
7. Fijación y medición de objetivos.
8. Proceso documental.
9. Auditorías internas y externas.

Toda esta estructura es exitosa solamente si el SGSI puede garantizar que los riesgos de seguridad se identifican y han sido aceptados, gestionados o minimizados por la organización, de manera documentada y sistemática.

2.5.2.2. Controles de la ISO27001. No todos los controles aplican para la siguiente investigación, pero muchos pueden soportar la implementación correcta de cero confianza en una organización. A continuación, los controles que pueden apoyar y deben considerarse según la naturaleza del teletrabajo (Thycotic).

A.5 Políticas de Seguridad de la Información:

A.5.1 Gestión de la seguridad de la información: su objetivo es proveer la gestión de gerencia y soportar la seguridad de la información según los requerimientos del negocio y las leyes o acuerdos contractuales.

A.5.1.1 Políticas para la seguridad de la información: es un grupo de políticas para la seguridad de la información que deben ser definidas y aprobadas por la Gerencia, posteriormente se publican y comunican a todos los empleados y otros actores relevantes.

A.5.1.2 Revisión de las políticas de la seguridad de la información: Es importante que las políticas se revisen en los plazos definidos o cuando haya cambios significativos, de esta manera, asegurar que sea conveniente, adecuado y efectivas.

A.6 Organización de la Seguridad de la Información:

A.6.1 Organización interna: su objetivo es establecer la base para iniciar y controlar la implementación y operación de la seguridad de la información en la organización.

A.6.1.1 Seguridad de la información roles y responsabilidades: todas las responsabilidades deben ser definidas.

A.6.1.2 Segregar las tareas: (Esto apoya la política del mínimo acceso) busca segregar las tareas en conflicto y áreas de responsabilidad, así reducir las oportunidades de un acceso no autorizado o no intencionado, que pueden ocasionar una modificación o una acción no.

A.6.2 Dispositivos móviles y teletrabajo: su objetivo es asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.

A.6.2.1 Política de dispositivos móviles: consiste en políticas y medidas de seguridad necesarias para manejar el riesgo que representan los dispositivos móviles.

A.6.2.2 Teletrabajo: consiste en políticas y medidas de seguridad que deben implementarse para proteger la información que es accedida, procesada y almacenada por los dispositivos en modalidad de teletrabajo.

A.8 Gestión de Activos:

A.8.1 Responsabilidad por los activos: su objetivo es que la organización pueda identificar los activos y definir la protección apropiada.

A.8.1.1 Inventario de activos: los activos asociados con información y las instalaciones de procesamiento de la información deben identificarse y un inventario de estos activos debe generarse y mantenerse.

A.8.1.2 Propiedad de los activos: todos los activos en el inventario deben tener un responsable.

A.8.1.3 Uso aceptable de los activos: son un grupo de reglas para el uso aceptable de la información y los activos asociados con información o instalaciones de procesamiento de información deben identificarse, documentarse e implementarse.

A.8.2 Clasificación de la información: su objetivo es asegurar que la información recibe el nivel apropiado de protección según su importancia para la organización.

A.8.2.1 Clasificación de la información: la información debe clasificarse según los requerimientos legales, valor, criticidad y sensibilidad.

A.8.2.2 Etiquetado de la información: se debe desarrollar un grupo de procedimiento para el etiquetado de la información e implementarse de acuerdo con la clasificación adoptada por la organización.

A.8.2.3 Manejo de activos: es un grupo de procedimiento para el manejo de activo que debe ser desarrollado e implementado según el esquema adoptado por la organización.

A.9 Control de Acceso:

A.9.1 Requisitos de negocio de control de acceso: su objetivo es limitar el acceso a la información y a las instalaciones de procesamiento de información.

A.9.1.1 Política de control de acceso: unas políticas de control de accesos deben establecerse, documentarse y revisarse según los requerimientos del negocio y de la seguridad de la información.

A.9.1.2 Acceso a las redes y servicios de red los usuarios deben tener acceso a la red y a los servicios de red a los que se les ha autorizado el acceso.

A.9.2 Gestión de acceso de usuarios: su objetivo es asegurar que los usuarios autorizados puedan acceder a los sistemas y servicios especificados y prevenir los accesos no autorizados.

A.9.2.1 Registro y baja de usuarios: un proceso formal de registro y baja de usuarios debe implementarse para soportar la asignación de privilegios.

A.9.2.2 Aprovisionamiento de usuarios: un proceso formal de aprovisionamiento de usuarios debe implementarse para asignar o revocar los privilegios de todos los tipos de usuarios a todos los sistemas o servicios.

A.9.2.3 Gestión del acceso privilegiado: la asignación y uso de los accesos privilegiados debe ser restringido y controlado.

A.9.2.4 Gestión de la información secreta de autenticación de los usuarios: la asignación de la información secreta de autenticación debe controlarse por un proceso de administración formal.

A.9.2.5 Revisión de los privilegios de usuarios: se deben llevar a cabo revisiones de los privilegios de usuarios en intervalos regulares.

A.9.2.6 Eliminación y modificación de los privilegios de usuario los privilegios de los usuarios deben ser removidos o modificados cuando sus responsabilidades cambian o su contrato se termina.

A.9.3 Responsabilidades de usuarios: el objetivo es prevenir el acceso no autorizado a los sistemas y aplicaciones.

A.9.3.1 Responsabilidades de usuarios: los usuarios son responsables de salvaguardar su información de autenticación.

A.9.4 Control de acceso de sistemas y aplicaciones: su objetivo es prevenir el acceso no autorizado a sistemas y aplicaciones.

A.9.4.1 Restricción de acceso a la información: el acceso a la información y aplicaciones debe ser restringido según las políticas de control de acceso.

A.9.4.2 Procedimientos de inicio de sesión seguro: cuando sea necesario por la política de control de acceso, el acceso a los sistemas y aplicaciones deben controlarse con un procedimiento seguro de inicio de sesión.

A.9.4.3 Sistema de gestión de contraseñas: un sistema de gestión de contraseñas debe ser interactivo y debe asegurar la calidad de las contraseñas.

A.9.4.4 Uso de programas de gestión de privilegios: el uso de algunos programas o utilidades para la revisión de privilegios puede ayudar a revisar, restringir y ajustar los accesos.

A.10 Criptografía:

A.10.1 Controles criptográficos: su objetivo es asegurar el funcionamiento y eficacia del uso de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

A.10.1.1 Políticas en el uso de controles criptográficos: se debe desarrollar e implementar una política para el uso de controles criptográficos.

A.10.1.2 Gestión de llaves: la organización debe crear una política del uso, protección y de la vida útil de las llaves de criptografía.

A.12 Seguridad de operaciones:

A.12.2 Protección al *malware*: su objetivo es asegurar que la información y las instalaciones de procesamiento de la información están protegidas contra *malware*.

A.12.2.1 Controles contra el *malware*: se deben implementar controles de detección, prevención y recuperación que protejan a la organización de un ataque de *malware*.

A.12.4 Registros y monitoreo: su objetivo es guardar los eventos y generar evidencia.

A.12.4.1 Registro de eventos: los eventos deben guardar las actividades de los usuarios, excepciones, fallas e información de seguridad y deben ser producidos, guardados regularmente y revisados.

A.12.4.2 Protección de la información de los registros: las instalaciones y la información en los registros deben ser protegidas de modificaciones y acceso no autorizado.

A.12.4.3 Registros de los operadores y administradores: toda actividad, sea de un operador y administrador, debe que registrada y su entrada debe ser protegida y revisada.

A.12.4.4 Sincronización de relojes: todos los registros e información relevante basada en eventos debe estar sincronizada para ser relacionable.

A.12.5 Controles de sistemas operativos: su objetivo es la integridad de los sistemas operativos.

A.12.5.1 Instalación de aplicaciones en sistemas operativos: se debe implementar procedimiento que controles la instalación de aplicaciones en los sistemas operativos.

A.12.6 Gestión de las vulnerabilidades técnicas: su objetivo es prevenir la explotación de una vulnerabilidad técnica.

A.12.6.1 Gestión de controles de auditoría de sistemas: información acerca las vulnerabilidades técnicas de los sistemas de información debe estar disponible para su evaluación y medidas apropiadas para manejar el riesgo.

A.12.6.2 Restricciones en instalaciones de *software*: se deben establecer e implementar reglas acerca la instalación de *software*.

2.6. GDPR

El Reglamento General de Protección de Datos (UE, 2021) dicta los requisitos específicos para las empresas y organizaciones en lo referente a recolección, almacenamiento y gestión de los datos personales y aplica a todas las organizaciones cuya actividad se dirija a las personas que vivan en la Unión Europea.

El RGPD se aplica cuando:

La empresa trata datos personales y tiene su sede en la UE, independientemente de dónde se traten de hecho los datos.

La empresa tiene su sede fuera de la UE, pero trata datos personales relativos a ofertas de bienes o servicios a ciudadanos en la UE, o supervisa el comportamiento de ciudadanos en la UE.

Las empresas que no tienen sede dentro de la UE y que tratan datos de ciudadanos de la UE deben nombrar un representante en la UE (UE, 2021, s. p.).

GDPR no aplica en casos de fallecimiento, personas jurídicas o una persona que actúa con fines ajenos a sus actividades comerciales, empresariales o profesionales. El reglamento aplica a los datos personales como nombre, apellido, dirección, ID, ingresos, perfil cultural, IP y datos médicos. Además, GDPR establece que no se pueden tratar datos personales como raza, sexualidad, política, religión o filosofía, sindicalismo, datos genéticos, datos biométricos y datos penales; algunas de estas pueden tener excepciones. GDPR establece que debe existir un delegado de protección de datos personales, este lo nombra la empresa y debe supervisar el manejo de los datos, además de informar y aconsejar a los responsables de sus obligaciones.

2.6.1. Transferencia de datos fuera de la UE. GDPR acompaña a los datos que atraviesen la frontera de la UE y se debe garantizar la siguiente:

La protección de datos del país no miembro de la UE se considera adecuada.

La empresa toma las medidas necesarias para proporcionar las oportunas salvaguardias, como la inclusión de cláusulas específicas en el contrato celebrado con el importador no europeo de los datos personales.

La empresa se basa en motivos específicos para la transferencia (excepciones), como el consentimiento del interesado (UE, 2021, s. p.).

2.6.2. Tratamiento de datos. GDPR establece que los datos deben tratarse, de manera justa y lícita, con el fin necesario y con los datos necesarios para este fin y parte de las obligaciones de la empresa son:

El interesado ha dado su consentimiento.

Los datos personales son necesarios para respetar una obligación contractual con el interesado.

Los datos personales son necesarios para cumplir una obligación legal.

Los datos personales son necesarios para proteger los intereses vitales del interesado.

Los datos personales se tratan para una misión de interés público.

Se actúa en interés legítimo de la empresa, siempre que en el tratamiento de los datos del interesado no se vean gravemente afectados los derechos y libertades fundamentales de este; si los derechos de esa persona prevalecen sobre los intereses de la empresa, no se pueden tratar sus datos personales (UE, 2021, s. p.).

2.6.3. Violación de datos. La violación de cualquier tipo o envío de datos a terceros no autorizados representaría una violación de los derechos y libertades individuales y se debe notificar a la autoridad de protección de datos en un plazo de 72 h después de la alerta. La empresa puede verse obligada a informar a los afectados.

Capítulo III. Marco metodológico

3.1. Tipo de investigación

Esta investigación no produce nuevos conocimientos, el modelo de cero confianza es un modelo existente y ha sido aplicado por muchos años a diferentes escenarios de sistemas de información, se utilizan las bases del modelo de cero confianza y otros documentos y estándares para generar una propuesta de ciberseguridad para el teletrabajo, debido a la creciente necesidad de esta modalidad en tiempos de COVID-19.

Se investigan algunos de los problemas que muchas organizaciones pueden tener en la actualidad con el teletrabajo, en las áreas específicas de identidad, administración de dispositivos y data de usuarios. Posteriormente, se define una propuesta para estas tres áreas utilizando el modelo de teletrabajo y las mejores prácticas de los estándares internacionales.

3.2. Alcance investigativo

Según la finalidad de la investigación se considera que es una investigación exploratoria y proyectiva. Según Barrantes (2015) la investigación exploratoria se define como:

Es una investigación que se realiza para obtener un primer conocimiento de una situación para luego realizar una posterior más profunda, por eso se dice que tiene un carácter provisional. Por lo general, es descriptiva, pero puede llegar a ser explicativa (s. p.).

Según Bernal (2006) la investigación proyectiva se define como: “Busca establecer una solución para una situación en estudio. Se logra establecer una solución por medio de la exploración, descripción, explicaciones y proposición de alternativas de cambio, las cuales no necesariamente se deben ejecutar, sean factibles o no” (s. p.).

3.3. Enfoque de la investigación

El enfoque es mixto:

- El enfoque cuantitativo se utiliza para identificar los problemas, necesidades y retos de ciberseguridad que muchas organizaciones y sus colaboradores enfrentan en sus actividades diarias con una metodología de teletrabajo o trabajo remoto. Se puede hacer un censo de los problemas de los empleados y administradores con el modelo de teletrabajo y usando los conocimientos de cero confianza obtenidos durante la investigación como base.
- El enfoque cualitativo se utiliza para evaluar la información obtenida durante la investigación, seleccionar los controles necesarios según los estándares internacionales y proponer una propuesta con las necesidades identificadas.

3.4. Diseño de la investigación

- Se realiza una evaluación de las publicaciones de NIST en relación con el modelo de cero confianza y se seleccionan los puntos importantes para la investigación.
- Se revisan los estándares internacionales establecidos por la ISO y PCI para seleccionar los controles necesarios para generar una propuesta que cumpla con estos estándares.
- Se revisan las normativas de GDPR y OECD y se seleccionan los puntos importantes que deben considerarse como parte de la propuesta.
- Se realiza una encuesta en redes sociales para identificar problemas que se relacionan con la seguridad del teletrabajo y descubrir cuáles controles seleccionados durante los puntos anteriores existen en las organizaciones.
- Se seleccionan los controles según los problemas encontrada en la encuesta y con base en los estándares y normas revisadas anteriormente.
- Se explican los controles según el material revisado y así justificar la selección de cada uno.
- Se diseña la propuesta con todos los controles seleccionados.
- Se hace un análisis final y conclusiones de la investigación.

3.5. Población y muestreo

Es no probabilístico, ya que esta investigación no aplica a un grupo particular que pueda ser medible, ya que el grupo de estudio son aquellos que trabajen bajo la modalidad de teletrabajo.

3.6. Instrumentos de recolección

Según Bernal (2006) la investigación debe usar un instrumento de medición que se adecue mejor a su objetivo de estudio. Para la parte cuantitativa se utiliza la encuesta y para la investigación cualitativa se utiliza un análisis documental.

3.6.1. Encuesta. La encuesta (Bernal, 2006) es un documento formulado que establece preguntas concretas, ya sean abiertas o cerradas, que tratan de conocer la opinión del individuo acerca del tema de investigación. Se utiliza esta metodología para conocer los controles de ciberseguridad implementados por las organizaciones en teletrabajo.

3.6.2. Análisis documental. El análisis documental (Bernal, 2006) recolecta datos para soportar la investigación. Se utiliza este instrumento para estudiar el modelo de cero confianza y las recomendaciones de teletrabajo establecidas por el NIST y también relacionar estos modelos con los controles establecidos por las normativas y estándares internacionales.

3.7. Técnicas de análisis de información

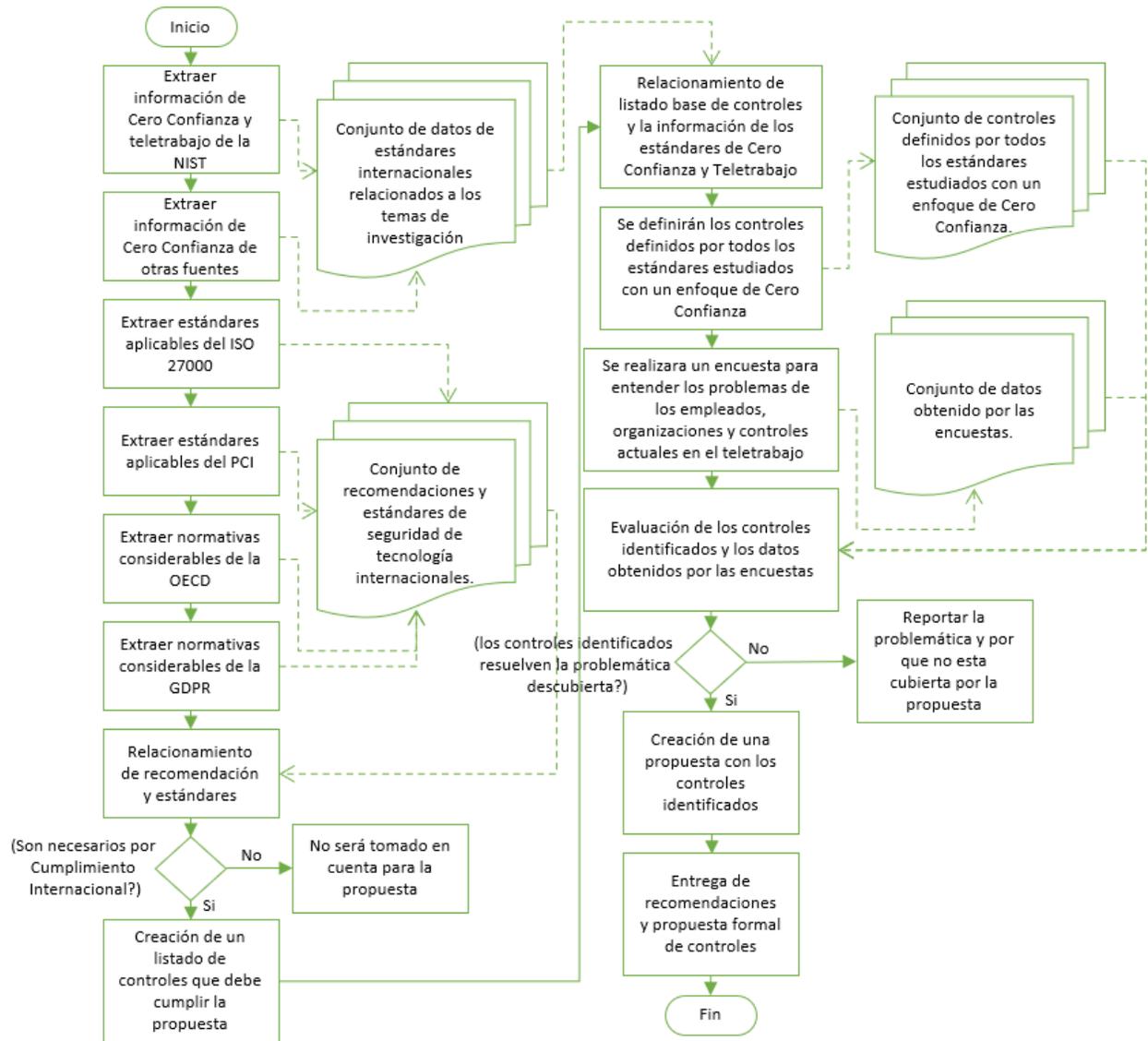


Ilustración 19

Mapa de Análisis de la información

Capítulo IV. Análisis de resultados

En este capítulo se muestran los resultados de los tres primeros objetivos de la investigación, en donde se han utilizado los instrumentos de encuesta y análisis documental.

4.1. Encuesta

La encuesta trata de responder el objetivo identificar los problemas, necesidades y retos de ciberseguridad que muchas organizaciones y sus colaboradores enfrentan en el día a día con una metodología de teletrabajo o trabajo remoto y trata de cubrir las áreas de autenticación, administración de dispositivos y almacenamiento de datos. La encuesta tiene un formato breve y sencillo, buscando así la participación de una audiencia amplia, por la misma razón se evitó el uso de lenguaje técnico en lo que se pudo.

4.1.1. Preguntas. La encuesta se ubica en un *link* donde ya no acepta respuestas, shorturl.at/IELY3. Consta de 5 preguntas y un encabezado.

1. Encabezado, se pretendía dar una pequeña introducción de la encuesta, además de aclarar que estaba relacionada con el teletrabajo y que era anónima.

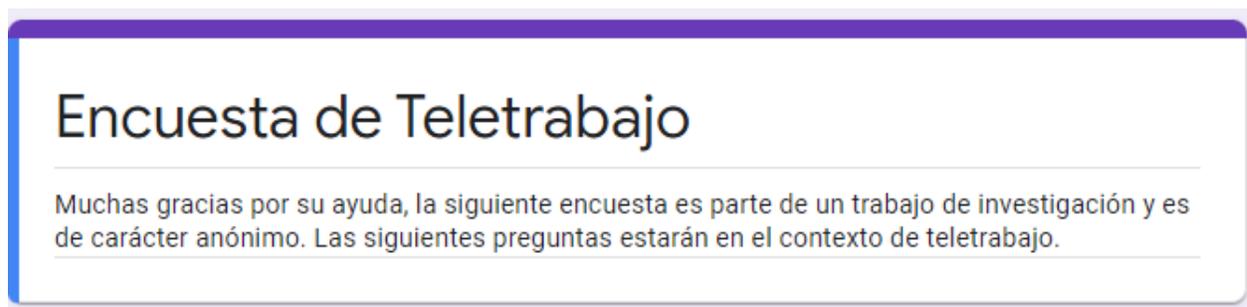
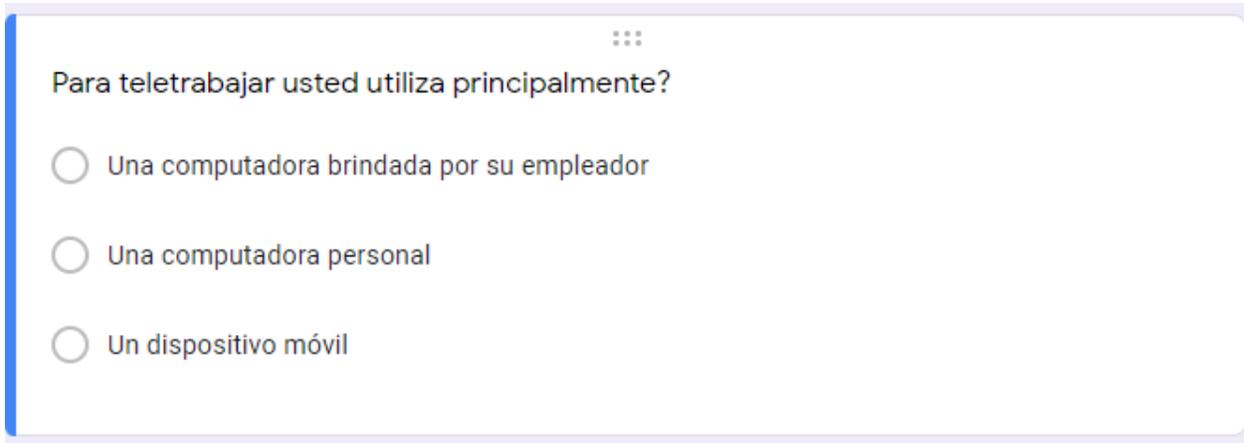


Ilustración 20

Encabezado de encuesta

2. La Primera pregunta fue, ¿Para teletrabajar usted utiliza principalmente? con tres opciones: A. Una computadora brindada por su empleador, B. Una computadora personal y C. Un dispositivo móvil. El objetivo de esta pregunta es entender la situación actual de las compañías nacionales que no tienen recursos para proveer a sus empleados de estaciones de trabajo o descubrir un escenario que es cada vez

más frecuente de teletrabajo que es con dispositivos móviles. Esto también puede dar una idea del control que tiene la empresa sobre el activo donde sus empleados realizan su trabajo.



Para teletrabajar usted utiliza principalmente?

- Una computadora brindada por su empleador
- Una computadora personal
- Un dispositivo móvil

Ilustración 21

Pregunta n.º 1

3. Segunda pregunta, ¿Cómo accede a su computadora de trabajo o aplicaciones de trabajo? esta pregunta tenía cuatro opciones disponibles: A. No utilizo ninguna contraseña, B. Utilizo una sola contraseña para todo, C. Utilizo diferentes contraseñas para mi equipo y aplicaciones y D. Utilizo una contraseña y otro método (*token*, PIN, tarjeta inteligente o biométricos). El objetivo es entender el proceso de autenticación definido por las organizaciones, según la investigación realizada durante el desarrollo del marco teórico la organización no debe dejar de solicitar autenticaciones y deben ser más seguras que una sola contraseña.

Como accede a su computadora de trabajo o aplicaciones de trabajo? *

- No utilizo ninguna contraseña
- Utilizo una sola contraseña para todo
- Utilizo diferentes contraseñas para mi equipo y aplicaciones
- Utilizo una contraseña y otro método (Token, PIN, Tarjeta inteligente o Biométricos (huella...

Ilustración 22

Pregunta n.º 2

4. Tercera pregunta, ¿Mantiene actualizado o sabe si el equipo se actualiza? (ej. actualizaciones de Windows), esta pregunta tenía tres opciones: A. Sí, B. No y C. No sé. El objetivo de esta pregunta es poner en evidencia el conocimiento de los usuarios acerca de las políticas de actualización y también conocer si las organizaciones realizan actualizaciones y sus empleados están conscientes de estas.

Mantiene actualizado o sabe si el equipo se actualiza? (Ej.: Actualizaciones de Windows)

- Si
- No
- No se

Ilustración 23

Pregunta n.º 3

5. Cuarta pregunta, ¿Cómo almacena sus archivos de trabajo?, esta pregunta contaba con 4 respuestas: A. Solo los guardo, B. Los guardo en una cuenta de OneDrive o Dropbox (o similares) personal, C. Los guardo en una cuenta de OneDrive o Dropbox (o similares) de la empresa y D. Los guardo en una ubicación remota. El objetivo de esta pregunta es conocer si las organizaciones tienen políticas o buenas prácticas o si sus empleados las conocen.

⋮

Como almacena sus archivos de trabajo?

- Solo los guardo
- Los guardo en una cuenta de OneDrive o Dropbox (o Similares) Personal
- Los guardo en una cuenta de OneDrive o Dropbox (o Similares) de la empresa
- Los guardo en una ubicación remota

Ilustración 24

Pregunta n.º 4

6. Quinta pregunta, ¿Para enviar correos electrónicos con archivos adjuntos utilizo?, esta pregunta tenía cuatro opciones: A. Mi correo personal, B. Utilizo un correo de empresa y solo adjunto el documento, C. Utilizo un correo de empresa, adjunto el documento y configuro la privacidad y D. Utilizo un correo de empresa y comparto un *link* con el archivo. El objetivo de esta pregunta es entender el riesgo que algunas empresas tienen al permitir o utilizar cuentas personales que no siguen ninguna política de seguridad organizacional, además de entender las prácticas o políticas implementadas por organizaciones al compartir archivos.

Para enviar correos electrónicos con archivos adjuntos utilizo?

- Mi correo Personal
- Utilizo un correo de empresa y solo adjunto el documento
- Utilizo un correo de empresa, adjunto el documento y configuro la privacidad
- Utilizo un correo de empresa y comparto un link con el archivo

Ilustración 25

Pregunta n.º 5

4.1.2. Publicaciones. La encuesta se llevó a cabo en redes sociales como se detalla a continuación:

- Facebook: se realizaron dos publicaciones.
 - o Publicación personal, la cual tuvo un alcance visible de 14 me gusta y 14 comentarios.
 - o Publicación en el grupo de Informáticos de Costa Rica, donde hubo un alcance de 79 me gusta y 41 comentarios. Se escogió este grupo por la facilidad, ya que su público puede entender la encuesta.
- Twitter: se llevó a cabo una publicación personal, la cual fue compartida 2 veces por contactos personales.
- LinkedIn: se llevó a cabo una publicación personal con 142 visualizaciones (de las cuales la plataforma detalla, IBM 10, Kyndryl 9 y Accenture 2), 4 reacciones y 2 comentarios.

4.1.3. Resultados. Durante un periodo de 2 semanas se recopilaron 476 respuestas por medio de las publicaciones mencionadas.

1. Resultados primera pregunta:

- a. No hubo resultados para dispositivos móviles como plataforma única de teletrabajo. La adopción de dispositivos móviles en el trabajo ha ido en aumento, pero los casos donde los empleados únicamente trabajen desde un dispositivo móvil son escasos. El escenario más común es tener ciertas aplicaciones en el dispositivo móvil personal o empresarial. Con el enfoque de cero confianza las organizaciones que permitan aplicaciones de trabajo (con acceso a recursos empresariales) en dispositivos móviles personales o empresariales (tabletas o teléfonos inteligentes) deben implementar una plataforma de administración similar a un MDM, esta plataforma debe permitir asegurar el dispositivo por medio de políticas de seguridad y debe ser capaz de implementar un perfil de trabajo que permita separar las aplicaciones, recursos y datos empresariales de los personales. El perfil de trabajo debe permitir la encriptación de la información empresarial, de esta manera, es posible evitar que la información almacenada en el dispositivo pueda ser accedida por el perfil personal. Siempre se debe asumir que el dispositivo ha sido vulnerado y que el perfil personal tiene aplicaciones maliciosas o el usuario puede intentar mover información fuera de las aplicaciones empresariales.
- b. Un 16.2 % (76 personas) de los entrevistados utilizan dispositivos personales para teletrabajar. Es un número elevado y puede que este número aumente o disminuya en los diferentes sectores empresariales. Muchas organizaciones corren el riesgo de permitir dispositivos personales sin las medidas adecuadas. En la actualidad, existen publicaciones y buenas prácticas para BYOD, las cuales pueden ayudar en la administración y en su aseguramiento. BYOD puede ser un escenario complicado, por ejemplo, la encuesta no revela si existe algún tipo de control sobre estos dispositivos o si estos dispositivos tienen algún tipo de restricción sobre el acceso a los recursos empresariales. Entre las mejores prácticas está el uso de un sistema de administración donde todas las máquinas personales deben enrollarse y el sistema de administración

debe aplicar políticas, por lo general las políticas de BYOD son menos restrictivas por la naturaleza del dispositivo. Tal vez el reto más grande en BYOD es que los dispositivos deben seguir siendo personales, lo cual limita la administración y el control que la organización puede tener sobre estos. En cero confianza los dispositivos BYOD pueden necesitar una red adicional donde el acceso a los recursos sea limitado y la organización debe generar reglas de acceso donde se limiten estos dispositivos.

Finalmente, un 83.8 % (399 personas) cuenta con una estación de trabajo brindada por su empleador. Por lo general estos dispositivos cuentan con algún cliente de administración o algún tipo de *hardening* (endurecimiento, se lleva a cabo aplicando configuraciones o cambios en el sistema operativo con la intención de mejorar su seguridad) que le permite a la organización asegurar, administrar, actualizar y escanear el dispositivo. Con el teletrabajo, muchos empleados utilizan sus estaciones de trabajo como computadoras personales, sin las políticas correctas el usuario puede vulnerar el dispositivo. En cero confianza el dispositivo empresarial debe tratarse como cualquier otro dispositivo, la única diferencia es que el PEP/PDP tendrá más información para confiar en el dispositivo, pero requerirá de una plataforma de administración.

Para teletrabajar usted utiliza principalmente?

476 respuestas

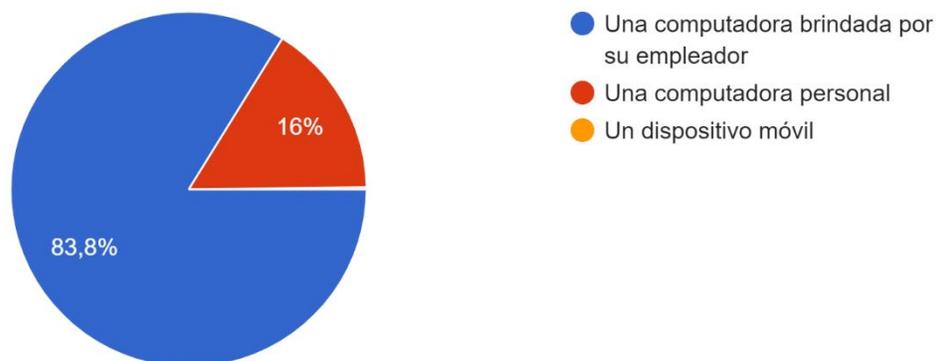


Ilustración 26

Resultados pregunta n.º 1

2. Resultados segunda pregunta:

- a. Un 2.3 % (11 personas) no utiliza contraseña para acceder a su computadora de teletrabajo o sus aplicaciones de trabajo. Se puede relacionar este grupo con las personas que trabajan desde un dispositivo personal, ya que en la actualidad es difícil encontrar computadores de trabajo sin contraseñas, también se pueden imaginar escenarios de emprendedores o pequeñas empresas que utilizan dispositivos personales o no tienen una infraestructura de identidad de usuarios. En cero confianza la autenticación es crítica y debe suceder cuantas veces sea necesaria, por lo que una plataforma de identidad es relevante.
- b. Un 10.5 % (50 personas) utiliza una sola contraseña para todo, quiere decir que utilizan la misma para iniciar sesión y para acceder a los recursos empresariales. Se puede asumir que una sola contraseña es un solo punto de fallo, pero a decir verdad el SSO (Single Sign-On) es cada vez más popular. SSO ayuda a los usuarios, elimina múltiples contraseñas y ayuda a las organizaciones para centralizar las políticas de contraseña, esto le permite a

la organización definir la complejidad y el tiempo de validez para cada contraseña de la organización. En cero confianza puede utilizar SSO y algunas de las buenas prácticas de mercado recomiendan su uso, incluso así, el MFA es necesario. La combinación de SSO y MFA permite centralizar sus políticas de contraseñas y pone a disposición los diferentes factores de autenticación. El SSO y MFA habilita el uso de los distintos factores de autenticación de forma independientemente, un usuario puede ingresar el PIN, *token* o algún biométrico cuando se le solicite autenticar y no debe ingresar su contraseña cada vez.

- c. Un 39.9 % (190 personas) utiliza diferentes contraseñas para iniciar sesión y para las aplicaciones empresariales. Se puede pensar que algunos de estos son los dispositivos personales donde tienen una contraseña personal o los dispositivos empresariales donde las aplicaciones utilizan una contraseña diferente. Otro escenario menos común es donde un empleado tiene diferentes usuarios para múltiples plataformas, roles o tareas dentro de la organización. El uso de diferentes contraseñas eliminaría un único punto de fallo y lo obligaría a enfocarse en un solo sistema o sistemas para obtener el acceso deseado. El uso de múltiples contraseñas también agrega un nivel adicional de complejidad para el usuario, lo cual puede resultar en contraseñas repetidas, similares, sencillas o que se anoten en un lugar no seguro. En cero confianza y en algunas de las mejores prácticas se recomienda el uso de cuentas adicionales para tareas de administración únicamente y así sea necesario, pero también buscan facilitarle el trabajo al usuario por lo que el uso de una sola contraseña con MFA es lo más recomendado.

Un 47.3 % (225 personas) utiliza otros métodos de autenticación, además de la contraseña. Cerca de la mitad utiliza MFA y es posible que también utilicen SSO. Esto da una idea de cuál es el estado actual de las organizaciones, ya que el uso de MFA y SSO pudo haber sido propuesto para cumplir con algún estándar internacional o simplemente para seguir buenas prácticas de seguridad. Este resultado implica el uso de un modelo de cero confianza, pero indica su nivel de madurez de seguridad.

Como accede a su computadora de trabajo o aplicaciones de trabajo?

476 respuestas

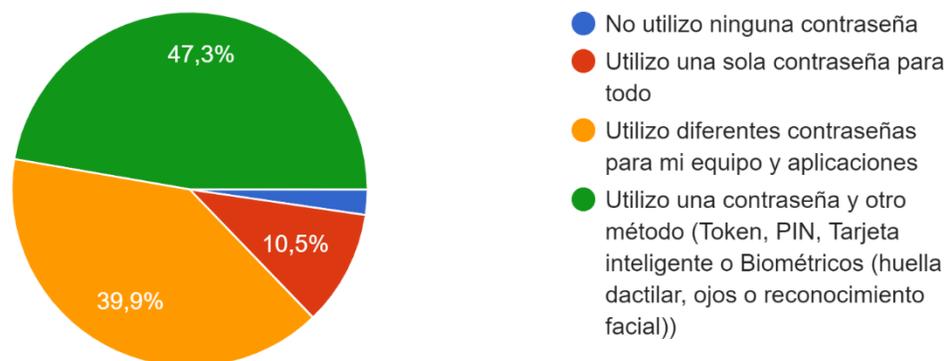


Ilustración 27

Resultados pregunta n.º 2

3. Resultados tercera pregunta:

- a. Un 2.5 % (12 personas) indica que sus dispositivos no se actualizan. Se puede pensar que son equipos viejos y, posiblemente, personales, ya que las máquinas posteriores a Windows 8 tienen las actualizaciones habilitadas de forma automática. En cero confianza es crítico que todos los dispositivos y aplicaciones estén actualizados a sus versiones más estables o probadas por la organización, ya que se debe asumir que los dispositivos ya pudieron ser o serán vulnerados.
- b. Un 2.7 % (13 personas) no tiene conocimiento de si su dispositivo se actualiza. Se puede pensar que este grupo es similar al primero, ya que Windows (sistema operativo más popular) notifica a sus usuarios cuando se llevan a cabo actualizaciones. Igual que en el punto anterior para cero confianza es crítico que los equipos se actualicen y que sus usuarios entiendan la importancia de eso.

El 94.7 % (451 personas) restante tiene conocimiento de que su dispositivo se actualiza, de manera periódica. Esto puede suceder de muchas maneras, sea por medio de un sistema de administración, un servidor WSUS local (puede utilizar VPN, esto genera mucho tráfico), políticas de actualización automática (directamente desde Windows) u otros medios. Esto no implica que la organización conozca el estado del dispositivo y las actualizaciones aplicadas, tampoco que tengan un modelo de cero confianza. En cero confianza la toma de decisión se apoya en el estado de seguridad del dispositivo y es crítico actualizar el dispositivo y saber el estado de cumplimiento respecto a los últimos parches.

Mantiene actualizado o sabe si el equipo se actualiza? (Ej.: Actualizaciones de Windows)

476 respuestas

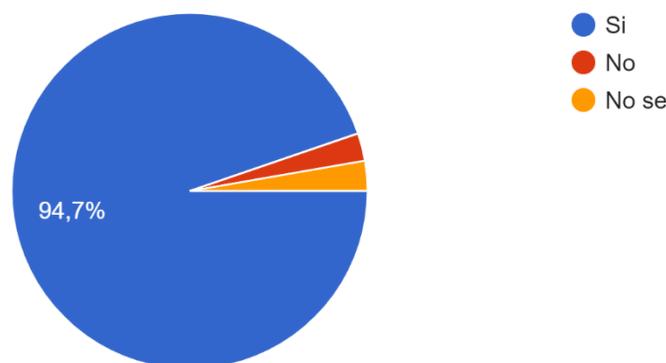


Ilustración 28

Resultados pregunta n.º 3

4. Resultados cuarta pregunta:

- a. Un 7.1 % (34 personas) utiliza almacenamiento en la nube personal. Se puede pensar que son usuarios con dispositivos personales o pequeñas empresas. El uso de almacenamiento personal de cualquier tipo representa un riesgo grande para la seguridad de una organización, se puede pensar en la falta de visibilidad al no saber dónde están almacenados, la falta de control y desconocimiento de la permanencia, lo cual puede ser un problema si se

termina una relación laboral. Adicionalmente, la cuenta personal puede tener problemas de seguridad como una contraseña débil, no tener MFA habilitado o carecer de seguridad adicional que algunos proveedores requieren (conocimiento de la ubicación de los archivos, ubicaciones específicas de almacenamiento y encriptado). En cero confianza y las buenas prácticas estudiadas en esta investigación se deben conocer dónde están almacenados o cómo se tratan los datos, además deben estar encriptados (para transmisión y reposo).

- b. Un 16.6 % (79 personas) guarda sus archivos en ubicaciones remotas. Muchas organizaciones cuentan con ubicaciones remotas (posiblemente SMB) para el almacenamiento de datos. Esta práctica le permite a la organización saber dónde se encuentran sus datos y tener más control sobre las políticas de seguridad. En cero confianza este es un escenario aceptado y toda la responsabilidad recae sobre la organización, por lo que esta debe definir políticas de seguridad, actualización, encriptación y transmisión para asegurar la seguridad de los datos.
- c. Un 17.6 % (84 personas) solo guardan los archivos. Es una práctica común entre los usuarios, consiste en guardar los archivos sin escoger una ubicación, por lo general se almacenarán en la carpeta Mis Documentos. Algunas organizaciones han migrado el perfil de usuario a ubicaciones remotas y así la información será almacenada fuera del equipo físico, incluso así, pueden quedar archivos localmente. En cero confianza la ubicación de los datos debe ser conocida y su almacenamiento debe ser encriptado, se puede pensar que la encriptación del disco duro resolvería este problema y, aunque cero confianza recomienda la encriptación de los discos duros no es para almacenar los datos localmente, agregar una ubicación remota de almacenamiento agrega una capa adicional de seguridad y en cero confianza es clave, ya que se presume que el equipo local ha sido vulnerado o robado y la información está segura en una ubicación remota conocida.

- d. El último 58.6 % (279 personas) utiliza servicios en la nube contratados por sus organizaciones. No todos estos servicios son seguros y, aunque algunos pueden establecer los controles necesarios por muchos de los estándares estudiados, pero pueden ser costosos, el uso de un servicio de almacenamiento en la nube no implica la adopción del modelo de cero confianza. En cero confianza y los estándares estudiados se recomienda el uso de plataformas donde se pueda encriptar la transmisión de los datos, también conocer la ubicación de los datos y que los datos en reposo estén encriptados. Se debe asumir que el dispositivo puede fallar, ser vulnerado o robado y los datos deben tener un respaldo o almacenarse en una ubicación remota segura, adicionalmente, el disco duro del dispositivo debe estar encriptado.

Como almacena sus archivos de trabajo?

476 respuestas

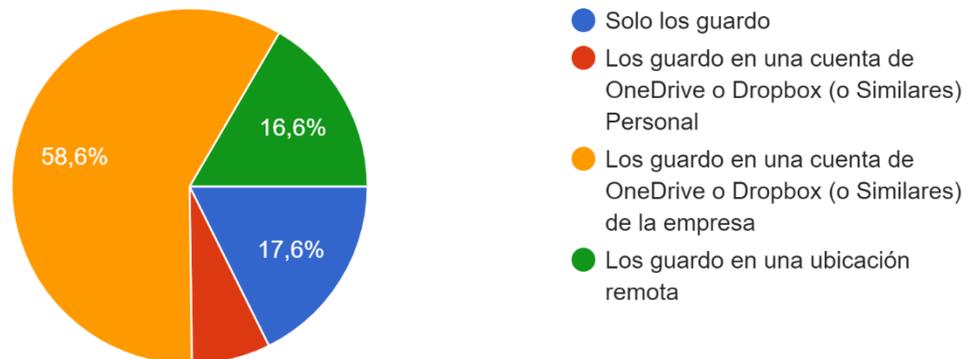


Ilustración 29

Resultados pregunta n.º 4

5. Resultados quinta pregunta:

- a. Un 0.6 % (3 personas) utiliza su correo electrónico personal para enviar documentos adjuntos. Entre los riesgos se puede destacar la falta de visibilidad sobre los correos enviados, falta de control sobre a quienes se les comparten datos de la organización, falta de control sobre la cuenta y,

finalmente, la organización desconocerá si documentos sensibles se encuentran almacenados en esta cuenta. En cero confianza se asume que el correo de la organización ha sido vulnerado y bajo esa premisa se establecen controles para minimizar el impacto, en una cuenta personal esto es imposible.

- b. Un 10.3 % (49 personas) envía *links* a los documentos por medio de un correo electrónico empresarial. Esta alternativa es cada vez más utilizada, al utilizar *links* se delegan los permisos de acceso a la plataforma donde se encuentren los archivos y al enviar el *link* por medio de un correo electrónico solo los que tienen permisos sobre los archivos podrán acceder a ellos. Por ejemplo, en SharePoint se pueden agregar usuarios, grupos o incluso crear un *link* con cierto nivel de acceso y en caso de ser necesario todos los accesos pueden revocarse. Otro ejemplo, son las carpetas compartidas u otras plataformas en la nube, donde se pueden definir los usuarios con los que deseamos compartir los archivos. El uso de *links* permite un control más granular sobre los archivos compartidos y evita que los documentos adjuntos sean enviados y accedidos por terceros o usuarios indeseados. El uso de *links* no implica el uso de un modelo de cero confianza. Cero confianza establece que los accesos deben ser granulares y revisados constantemente, adicionalmente no se debe confiar en los otros usuarios por lo que control sobre el acceso a los datos compartido es vital.
- c. Un 21.2 % (101 personas) utiliza su correo electrónico empresarial, adjunta el documento y configura la privacidad. La configuración de privacidad en Outlook (uno de los clientes de correo más populares) permite limitar la descarga, el reenvió, la copia y captura de pantalla sobre un correo electrónico o sus documentos adjuntos. Otros clientes de correo pueden ofrecer características similares, que permiten controlar quien tiene acceso a la información compartida por medios electrónicos. En cero confianza saber que la información que se comparte por correo la consultan solo por los usuarios que se desea es crítico y asegurar que no se reenvíe sin autorización es

importante. La configuración de privacidad de correo electrónico se alinea con cero confianza pero su uso no implica la adopción del modelo.

Finalmente, un 67.9 % (323 personas) solo adjunta el archivo utilizando su correo empresarial. Los usuarios solo adjuntan los documentos y se puede asumir que se reenvían o descargan. Una organización puede tener controles que le permitan saber cuándo se intenta enviar un documento sensible fuera de la organización. En el contexto de cero confianza no se puede saber quiénes acceden a un documento o quienes lo pueden abrir, ya que no se puede confiar en los usuarios que reciben el documento y cómo lo usen.

Para enviar correos electrónicos con archivos adjuntos utilizo?

476 respuestas

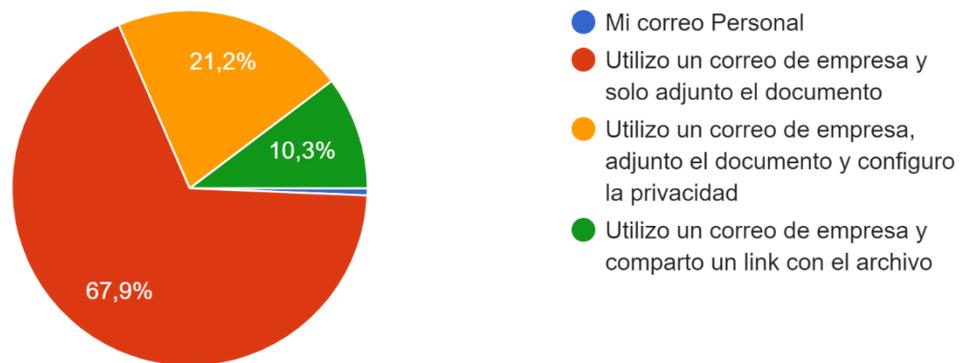


Ilustración 30

Resultados pregunta n.º 5

4.1.4. Conclusión de los resultados. Se puede concluir que muchas organizaciones han desplegado controles mínimos de seguridad que siguen las buenas prácticas del mercado. Por ejemplo:

- Una práctica mínima que la mayoría de las personas encuestadas reflejaron, es que las organizaciones han proveído a sus colaboradores con estaciones de trabajo y tienen los controles necesarios para mantener sus dispositivos actualizados.

- Se pudo observar que cerca de la mitad de las organizaciones han adoptado MFA, lo cual es una buena práctica de seguridad y ha sido ampliamente implementada por cumplimiento de normativas y estándares. Esta práctica puede prevenir ataques sobre una sola contraseña, utilizando algo que el usuario tiene, algo que el usuario es y algo que el usuario sabe.
- Menos de una cuarta parte de las personas encuestadas parece tener políticas de seguridad que permitan asegurar los documentos que se envían vía correo electrónico, lo que ayuda a limitar el acceso y asegurar que no se reenvíen, descarguen o copien sin autorización. Esta política de seguridad no es común en la actualidad y muchas organizaciones confían en sus colaboradores y no crean una cultura de seguridad.
- Una práctica común en la actualidad es el encriptado de disco duro, ya que sigue las buenas prácticas de seguridad y algunos de los estándares lo piden por cumplimiento. Aun así, el almacenamiento local no es seguro, ya que el activo puede ser perdido, robado, vulnerado o usado por un tercero. Estos riesgos siempre han existido, pero con el teletrabajo el riesgo aumenta, muchos usuarios trabajan fuera de casa en cafeterías, hoteles, restaurantes, otras casas o incluso en lugares más públicos. Dos terceras partes parecen almacenar sus archivos en la nube o una ubicación remota dedicada, lo cual asegura que la compañía o el usuario pueda recuperar su trabajo si algo le pasara a su dispositivo, además de que agrega otra capa de seguridad en caso de que la máquina no esté encriptada o el disco duro sea vulnerado.

Como se detalló, se encontraron cuatro puntos que siguen buenas prácticas de seguridad, pero esto no implica que las organizaciones hayan adoptado el modelo de cero confianza. Como se ha descrito, este modelo asume que todo puede o ha sido vulnerado por un tercero o un usuario interno y la organización debe asegurar que ningún tercero o usuario interno acceda a un recurso que no debe.

- La organización debe ser capaz de administrar los dispositivos que tienen acceso a los recursos de la organización, debe conocer el estado del dispositivo.

- Debe aplicar actualizaciones de sistema operativo y aplicaciones.
- Debe ejecutar escaneos de antivirus.
- Debe desplegar políticas de seguridad.
- Debe tener visibilidad del cumplimiento.
- La organización debe ser capaz de autenticar efectivamente a sus usuarios y conocer el comportamiento normal del usuario.
 - Debe establecer políticas de seguridad para la definición de contraseñas.
 - Debe autenticar algo que el usuario sabe, es y tiene.
 - Debe autenticar cuantas veces sea necesario.
 - Debe conocer el comportamiento normal de un usuario y evaluar las desviaciones.
- La organización debe ser capaz de dar control sobre el acceso a los archivos compartidos.
 - Debe ser capaz de reevaluar quien tiene acceso a los datos o recursos.
 - Debe ser capaz de retirar el acceso a usuarios que no necesitan acceso a un archivo para efectuar sus labores.
- La organización debe ser capaz de asegurar los datos de usuario.
 - Debe ser capaz de ejecutar respaldos.
 - Debe ser capaz de recuperar los datos de usuario.
 - Debe ser capaz de asegurar la ubicación y el almacenamiento de los datos.

4.2. Análisis documental

Se utiliza el análisis documental para responder a dos de los objetivos de la investigación, por lo que dividiré el análisis documental en dos secciones, uno de estándares internacionales y otro de normativas internacionales. Anteriormente, se llevó a cabo un

preanálisis en el marco teórico, con el fin de capturar la información más importante para el desarrollo de la investigación. Durante este preanálisis, se seleccionó lo relacionado con cero confianza teletrabajo y las áreas definidas en los alcances de la investigación, identidad, administración de dispositivos y almacenamiento de datos de usuario.

Las áreas seleccionadas vienen de los principios de la cero confianza definidos por la NIST, pero se utiliza información que Microsoft (s. f.) ha logrado resumir y estructurar en tres principios generales y seis pilares tecnológicos. La estructura creada por Microsoft es más fácil de entender cuando las organizaciones desean empezar la implementación del modelo de cero confianza, además, permite desarrollar o trabajar pequeñas áreas de la organización. El modelo de Microsoft se alinea con la investigación, ya que la propuesta es solo para teletrabajo y no para toda la organización ni todas sus áreas tecnológicas.

Microsoft en su Centro de Guía para cero confianza (Zero Trust Guidance Center) resume los principios generales en tres:

- a) Verificar explícitamente: autenticar y autorizar siempre en función de todos los puntos de datos disponibles.
- b) Utilizar la política de Menos Privilegios (Least Privileged): limitar el acceso de usuario con políticas de tiempo y acceso necesario para llevar a cabo sus tareas, utilizar políticas adaptables al riesgo y utilizar políticas de protección de datos.
- c) Asumir una ruptura de seguridad: siempre trata de minimizar el radio de daño y el acceso por medio de la segmentación. Verificar la encriptación de punto a punto, utilizar herramientas de análisis para tener visibilidades de las transacciones, impulsar la detección de amenazas y mejorar los controles de defensa.

Asimismo, define seis pilares tecnológicos, los cuales deben permitir visibilidad, automatización y orquestación.

- a) Identidad segura: este pilar contiene a los usuarios, servicios y dispositivos y como verificamos exitosamente su identidad, establece el uso de métodos fuertes

de autenticación y se asegura que la identidad sea segura o esté en cumplimiento. Sigue la política de Least Privilege.

- b) Estaciones de trabajo seguras: una vez que el acceso a un recurso es debido a un sujeto, los datos pueden fluir a muchos dispositivos diferentes, esta diversidad de dispositivos crea una gran área de ataque, por lo que es crítico tener control sobre los dispositivos, así como monitoreo y aplicación de políticas de cumplimiento para garantizar el acceso seguro.
- c) Aplicaciones seguras: las aplicaciones y API crean una interfaz de datos para los usuarios. Estas aplicaciones pueden ser de muchos tipos y pueden crear una gran área de ataque, la capacidad de la compañía de asegurar estas aplicaciones, monitorearlas o mejorar su seguridad puede ser limitada sin los controles adecuados.
- d) Datos seguros: Los datos deben permanecer seguros incluso si dejan los dispositivos, aplicaciones, infraestructura y las redes de la organización. La clasificación, etiquetado y encriptado de los datos es crítico para restringir el acceso con base en sus atributos.
- e) Infraestructura segura: sea en la nube o en premisas, la infraestructura es crítica para los procesos de la organización. La organización debe evaluar, configurar y actualizar su infraestructura para endurecer su seguridad. El uso de telemetría para analizar el comportamiento de sus activos es clave para reaccionar ante riesgos.
- f) Redes seguras: finalmente, la data es accedida por medio de la red. Los controles de seguridad en una red son críticos para tener visibilidad de ataques o comportamientos anómalos que sucedan dentro y fuera de la organización. La organización debe ser capaz de segmentar y configurar controles de protección en tiempo real, debe encriptar la comunicación, monitorear y analizar el tráfico.

De estos seis pilares es posible identificar muchos que soportarán el teletrabajo, pero no todos son críticos para cualquier organización. Por la naturaleza del teletrabajo solo se desarrollan identidad, administración de dispositivos y almacenamiento de datos.

4.2.1. Estándares internacionales. A continuación, se analizan y se relacionan los estándares estudiados para responder el objetivo específico 1: Reconocer los puntos importantes de ciberseguridad para esta propuesta a partir del modelo de cero confianza de los estándares internacionales de la NIST, ISO y PCI.

Entre los estándares revisados está el de la NIST (Rose, Borchert, Mitchell y Connelly, s. f.) que es uno de los pocos estándares basados en cero confianza con un enfoque general, se creó principalmente para organizaciones gubernamentales del gobierno de los Estados Unidos, pero el mismo documento afirma que puede reutilizarse en cualquier empresa. La NIST (Greene, 2020) también creó una publicación para la implementación del teletrabajo, la cual se toma en cuenta. Adicionalmente, el Departamento de Defensa de los Estados Unidos (Defense Information Systems Agency [DISA] and National Security Agency [NSA], 2021) creó una publicación basada en la publicación de cero confianza de la NIST y esta agrega controles y políticas que pueden tomarse en cuenta. Se utilizarán los tres documentos para definir los puntos importantes del teletrabajo con un modelo de cero confianza según la NIST y el DoD.

Los otros dos estándares tomados en cuenta en la investigación son el ISO 27001 y el PCI DSS. Ambos se incluyen por la necesidad de cumplimiento que existe por parte de muchas organizaciones nacionales y es necesario tomarlos en cuenta para que la propuesta sea aplicable en cualquier organización.

4.2.1.1. NIST. A continuación, se define la NIST.

4.2.1.1.1. Autenticación. Se define la autenticación.

Tabla 4

Controles NIST 1

Controles/Políticas	NIST: cero confianza	DoD: cero confianza	NIST: teletrabajo
Política del menor privilegio	X	X	

Políticas dinámicas de acceso	X		
RBAC	X	X	
ABAC	X	X	
Autorización individual	X		
Implementación de ICAM	X		
Uso de cuenta administrador			X
Autenticación constante	X		
MFA/CMFA	X	X	X
Minimizar zonas de confianza implícita	X		
Limitar la administración remota			X
Inventario de los sujetos físicos y virtuales	X		
Trazabilidad de usuarios	X		
Políticas de bloqueo de sesión			X

La NIST y el DoD utilizan la política del menor privilegio (Least Privilege) e indica la importancia de que los usuarios tengan el acceso necesario y por el tiempo necesario a los recursos que necesiten para desarrollar su trabajo. La NIST se apoya en reglas de acceso granular para lograr el menor privilegio y esto ocurre cuando el acceso a cada recurso individual debe evaluarse de manera individual. La NIST también destaca la importancia de las políticas dinámicas de acceso, es decir, políticas de acceso que puedan utilizar atributos

del sujeto, del ambiente y del dispositivo y con la capacidad de cambiar según las necesidades del negocio. El DoD apoya las políticas dinámicas con atributos con el uso de ABAC y con roles con RBAC. La NIST establece que el acceso a cada recurso debe darse por sesiones individuales y la autenticación individual es obligatoria antes de dar acceso a cualquier recurso. Todo esto se debe apoyar en un ICAM.

El estándar de teletrabajo de la NIST explica la importancia de las cuentas administrativas para tareas específicas, donde un usuario tiene una cuenta de acceso limitado y otra de acceso elevado (no usada para inicio de sesión). Esto puede agregar una capa adicional de complejidad.

Según la NIST cero confianza se apoya en la autenticación y autorización e implica que validar la identidad y su nivel de acceso es crítico, la organización debe ser capaz de llevar a cabo la autenticación cuantas veces sea necesario y de manera continua. Las políticas de acceso dinámicas deben trabajar con el proceso de autenticación y autorización y se deben usar los datos del dispositivo y del usuario para autorizar cuando sea necesario. Los estándares de la NIST y el DoD destacan la importancia del uso de MFA o CMFA y que su política de uso puede ser dinámica según el comportamiento del sujeto o su postura de seguridad.

La NIST establece que cero confianza reduce las zonas de confianza implícita, bajo la premisa de no confiar en ningún dispositivo o usuario, significa no confiar en zonas seguras de la intranet. El estándar de Teletrabajo destaca la importancia de la creación de políticas para la administración remota de servicios, servidores críticos o políticas de seguridad.

La NIST también destaca la importancia del inventario de actores en la organización, donde se deben conocer los sujetos físicos y virtuales de la organización, además detallar cuáles cuentas son especiales o privilegiadas, la organización debe ser capaz de establecer un ciclo de revisión y evaluación de cuentas. La NIST dicta que ninguna cuenta debe tener acceso a todos los recursos de la organización y todas deben cumplir los requerimientos mínimos de la naturaleza de su trabajo en el negocio. Por último, todas las cuentas deben tener trazabilidad sin importar su nivel de acceso.

El estándar de teletrabajo de la NIST destaca la importancia de las políticas de bloqueo de máquina o duración de sesión para el sistema operativo o aplicaciones. Esto se debe a que la organización debe obstaculizar el acceso de un tercero por medio de un sistema desatendido.

4.2.1.1.2. *Administración de dispositivos.* A continuación, se define la administración de dispositivos.

Tabla 5
Controles NIST 2

Controles/Políticas	NIST: cero confianza	DoD: cero confianza	NIST: Teletrabajo
Monitoreo de cumplimiento de dispositivos	X	X	X
Actualización de sistema operativo	X	X	
Actualización de aplicaciones	X	X	
Inventario de dispositivos	X		
Administración de dispositivos	X	X	X
Inventario de aplicaciones	X		
Antimalware	X	X	X
Actualización remota de antimalware			X
Firewall			X
Actualización remota de firewall			X

Escaneos periódicos

X

Los estándares de la NIST establecen que la organización debe ser capaz de monitorear el cumplimiento de los dispositivos, lo cual debe ser utilizado para evaluar la postura del dispositivo, ya que ninguno debe gozar de confianza heredada. La NIST destaca la importancia de actualizar y mantener actualizado el sistema operativo y las aplicaciones instaladas en los dispositivos y se debe conocer el cumplimiento de los dispositivos. El estándar de teletrabajo indica que la capacidad de administración de los dispositivos por la organización debe ser la misma para los dispositivos remotos y debe ser siempre capaz de monitorearlos y configurarlos cuando sea necesario.

La NIST indica que es fundamental un inventario de todos los dispositivos conectados en la red de la organización y se deben inventariar las aplicaciones instaladas en cada uno de los dispositivos. La implementación de un *antimalware* es apoyada por los tres estándares, pero la implementación de un agente de *firewall* solo se menciona en el estándar de teletrabajo. El estándar de teletrabajo especifica que se debe ser capaz de actualizar el *software* de *antimalware* y *firewall* cuando sea necesario y de manera periódica. La organización debe tener la capacidad de ejecutar escaneos periódicos y conocer los resultados. Finalmente, la organización debe conocer el estado de configuración, cumplimiento y estatus de cada dispositivo.

4.2.1.1.3. *Almacenamiento de datos*. Seguidamente, se define el almacenamiento de datos.

Tabla 6

Controles NIST 3

Controles/Políticas	NIST: cero confianza	DoD: cero confianza	NIST: teletrabajo
Toda comunicación debe ser segura	X		X
Implementación de un DLP		X	

Implementación de un DRM		X	
Implementación de CASB			X
Encriptación de datos en tránsito	X	X	X
Encriptación de datos en reposo	X	X	X
Encriptación basada en FIPS			X
Etiquetado de datos	X		X
Respaldo de datos			X
Correo electrónico encriptado			X

La NIST establece que todos los datos, información de usuarios o información de la organización son recursos y que todos los recursos y comunicaciones deben asegurarse sin importar su ubicación en la red. Ambos estándares de la NIST destacan la importancia del uso de un DLP y el estándar de teletrabajo agrega a la lista el uso de un DRM y de soluciones CASB; las herramientas mencionadas pueden ayudar a la organización con el aseguramiento de datos en reposo o en tránsito. Tanto la NIST como el DoD dictan que la información en tránsito o reposo debe estar encriptada y la NIST recomienda los métodos criptográficos avalados por FIPS. La encriptación incluye el disco duro de los activos de la organización.

La NIST establece que en cero confianza la organización debe conocer la naturaleza de cada uno de sus recursos (datos) y debe etiquetarlo según su naturaleza. El estándar de teletrabajo indica que la organización debe ser capaz de respaldar todos los datos en caso de un percance y los respaldos deben ser periódicos así dicten las necesidades del negocio.

Los correos electrónicos deben encriptarse o al menos su documento adjunto así lo indica el estándar de teletrabajo. Esto puede entrar en la categoría de datos en tránsito y se puede afirmar que tanto la NIST como el DoD avalan esta política. Otra solución sugerida

por la NIST en su estándar de teletrabajo es el uso de soluciones *cloud* para compartir archivos y manejar el acceso a estos, lo cual se alinea con otras políticas de cero confianza.

4.2.1.2. ISO. A continuación, se define la norma ISO.

4.2.1.2.1. Autenticación. Seguidamente, se define la autenticación.

Tabla 7
Controles ISO 1

Controles/Políticas	ISO
Política del menor privilegio	X
RBAC	X
Inventario de los sujetos físicos y virtuales	X
Inventarios de bajas de usuarios	X
Políticas de asignación, evaluación y revocación de privilegios	X
Políticas de restricción y control de cuentas privilegiadas	X
Políticas de aseguramiento de información de autenticación	X

La ISO también se alinea con la política del menor privilegio, esta establece la necesidad de segregar las tareas y áreas de responsabilidad. Además, indica que esto se puede llevar a cabo por el uso de roles, lo cual se alinea con el RBAC del estándar de teletrabajo de la NIST.

La ISO también indica que los usuarios autorizados deben acceder a los sistemas y recursos de manera segura y la organización debe implementar los controles necesarios para prevenir accesos no autorizados. La organización debe ser capaz de tener un inventario de usuarios activos y de las bajas. Además, debe ser capaz de definir una política o procedimiento para asignar y revisar los privilegios necesarios. La ISO establece que las

cuentas privilegiadas deben ser restringidas o controladas, lo cual debe estar definido en las políticas de seguridad. Finalmente, todas las cuentas deben revisarse y evaluarse periódicamente y se puede tomar en cuenta la implementación de un programa de gestión de privilegios.

La organización debe definir políticas de seguridad que aseguren la información de autenticación y debe ser segura y secreta. Se debe velar por que los empleados salvaguarden su información de autenticación. Los administradores deben definir políticas de contraseña para su complejidad o calidad y su validez.

4.2.1.2.2. Administración de dispositivos. Seguidamente, se define la administración de dispositivos.

Tabla 8
Controles ISO 2

Controles/Políticas	ISO
Inventario de dispositivos	X
Antimalware	X
Actualización remota de antimalware	X
Políticas de uso aceptable de activos	X
Registro de eventos	X
Políticas de instalación de aplicaciones	X

La ISO al igual que la NIST destaca la necesidad de tener un inventario de activos y establece la necesidad de conocer al responsable de cada uno. La ISO afirma que debe existir una política de uso aceptable de los activos de la organización, donde se establezca todo uso apropiado y aceptado por la organización. ISO dicta que debe existir un sistema de detección,

prevención y recuperación de *malware*, lo cual puede apoyarse con una política organizacional.

ISO destaca la importancia de los eventos generados por los usuarios y sus dispositivos, lo cual se alinea con la trazabilidad de usuario de la NIST, establece que toda actividad de usuarios debe guardarse, lo que incluye las excepciones, fallas e información de seguridad. Los registros estos deben generarse y guardarse regularmente, además de revisarlos periódicamente. La organización puede apoyarse en un sistema de relación de eventos.

Finalmente, la ISO destaca la importancia de una política de instalación de aplicaciones, la cual puede ser parte de la política de uso aceptable, donde establezca que aplicaciones se permiten o qué limitaciones tienen los usuarios con las aplicaciones aprobadas por la organización.

4.2.1.2.3. Almacenamiento de datos. A continuación, se define el almacenamiento de datos.

Tabla 9
Controles ISO 3

Controles/Políticas	ISO
Encriptación de datos en tránsito	X
Encriptación de datos en reposo	X
Etiquetado de datos	X
Política de controles criptográficos	X
Políticas de seguridad de la información	X

Según la ISO, toda la información debe clasificarse según su importancia, seguir sus requerimientos legales, valor organizacional, valor personal, criticidad y sensibilidad. La

organización debe definir un procedimiento de etiquetado de la información. Se debe implementar una política de controles criptográficos, que apoye a la gestión de las llaves privadas o públicas y el uso de la criptografía en sus dispositivos. La organización debe definir políticas para la seguridad de la información, la cual debe revisarse y actualizarse periódicamente.

4.2.1.3. PCI. A continuación, se define la PCI.

4.2.1.3.1. Autenticación. Seguidamente se define la autenticación.

Tabla 10

Controles PCI 1

Controles/Políticas	PCI
Política del menor privilegio	X
Autorización individual	X
Autenticación constante	X
MFA/CMFA	X
Políticas de aseguramiento de información de autenticación	X
Eliminación de cuentas compartidas	X
Documentación de todas las políticas y procedimientos	X

La PCI establece que la organización debe identificar y autenticar los accesos a todos los componentes que contengan información de tarjetas de crédito y debe seguir la política del menor privilegio. Esta política se alinea con la autorización individual y constante de la NIST, la única diferencia es que PCI solo lo establece para recursos o componentes con información de tarjetas de crédito.

La organización debe implementar métodos apropiados de identificación donde no existan cuentas compartidas y cada usuario use una cuenta individual. La información de autenticación debe almacenarse de manera segura, alineándose con la creación de una política de aseguramiento de información de autenticación como lo establece la ISO. PCI avala el uso de MFA, lo que asegura que el acceso sea individual e identificable y utiliza algo que el usuario conozca, tenga y sea. Finalmente, PCI pide documentar todas las políticas y procedimientos, esto se relaciona con lo que establece la ISO y la definición de políticas.

4.2.1.3.2. *Administración de dispositivos.* A continuación, se define la administración de dispositivos.

Tabla 11

Controles PCI 2

Controles/Políticas	PCI
Actualización de sistema operativo	X
Actualización de aplicaciones	X
Antimalware	X
Actualización remota de antimalware	X
Firewall	X
Actualización remota de firewall	X
Identificar activos que almacenan o procesen información de crédito	X
Evaluación y reparación de vulnerabilidades	X
Políticas de manejos de cambios	X

Documentación de todas las políticas y procedimientos	X
---	---

PCI define que la organización debe conocer que activos almacenan o procesan información de tarjetas de crédito durante el ciclo de vida de la información. Establece que en los dispositivos involucrados se deben detectar y reparar las vulnerabilidades y la organización debe reportar el estado y remediarlas cuando sea necesario. La PCI dicta que la organización debe instalar y mantener *software* de *antimalware* y agentes de *firewall*, además de conocer el estado del servicio y de su ejecución.

PCI afirma que se deben actualizar todas las aplicaciones y solucionar sus vulnerabilidades.

PCI establece que la organización debe ser utilizar las políticas de manejo de cambios, donde todos los cambios deben planificarse, probarse y desplegarse con el conocimiento y consentimiento de la organización y todos los responsables. Finalmente, PCI establece que la organización debe documentar las políticas y procedimientos que se relacionan. Otra vez se alinea con ISO y el desarrollo de políticas.

4.2.1.3.3. *Almacenamiento de datos*. Seguidamente, se define el almacenamiento de datos.

Tabla 12
Controles PCI 3

Controles/Políticas	PCI
Encriptación de datos en tránsito	X
Encriptación de datos en reposo	X
Políticas de seguridad de la información	X
Políticas de restricción de acceso a información de tarjetas de crédito	X

Documentación de todas las políticas y procedimientos

X

Según PCI toda la información de tarjetas de crédito debe protegerse por medio de métodos criptográficos, tanto en reposo o en transmisión. PCI se apoya en los estándares definidos por la NIST y los define como mejores prácticas para la selección de un algoritmo de criptografía. La información de crédito no debe enviarse por medios no oficiales o no encriptados.

PCI define que el acceso a la información de tarjetas de crédito debe ser restringido y que el acceso directo desde Internet a cualquiera de los componentes o activos que almacenen o procesen información de tarjeta de crédito debe ser prohibido. La información de tarjetas de crédito no debe almacenarse sin autorización del usuario y debe hacerse solo por el tiempo requerido.

Además, establece que debe existir una política de gestión de la seguridad de la información, la cual se alinea con lo que define la ISO. Asimismo, pide que todas las políticas y procedimiento se documenten de nuevo alineados con ISO.

4.2.1.4. Resultados. A continuación, se presenta la Tabla 13 con los 52 controles o políticas encontradas en el análisis documental de los estándares estudiados, así como su relación. Para facilitar el análisis se reunieron los dos estándares de las NIST y el estándar de la DoD (que se basó en el estándar de la NIST) en una sola columna llamada NIST.

Tabla 13

Resultados de los estándares internacionales estudiados

Controles/Políticas	NIST	ISO	PCI
Política del menor privilegio	X	X	X
Políticas dinámicas de acceso	X		
RBAC	X	X	

ABAC	X		
Autorización individual	X		X
Implementación de ICAM	X		
Uso de Cuenta administrador	X		
Autenticación constante	X		X
MFA/CMFA	X		X
Minimizar zonas de confianza implícita	X		
Limitar la administración remota	X		
Inventario de los sujetos físicos y virtuales	X	X	
Trazabilidad de usuarios	X		
Políticas de bloqueo de sesión	X		
Inventarios de bajas de usuarios		X	
Políticas de asignación, evaluación y revocación de privilegios		X	
Políticas de restricción y control de cuentas privilegiadas		X	
Políticas de aseguramiento de información de autenticación		X	X
Eliminación de cuentas compartidas			X
Documentación de todas las políticas y procedimientos			X

Monitoreo de cumplimiento de dispositivos	X		
Actualización de sistema operativo	X		X
Actualización de Aplicaciones	X		X
Inventario de dispositivos	X	X	
Administración de dispositivos	X		
Inventario de aplicaciones	X		
Antimalware	X	X	X
Actualización remota de antimalware	X	X	X
Firewall	X		X
Actualización remota de firewall	X		X
Escaneos periódicos	X		
Políticas de uso aceptable de activos		X	
Registro de eventos		X	
Políticas de instalación de aplicaciones		X	
Identificar activos almacenan o procesen información de crédito			X
Evaluación y reparación de vulnerabilidades			X
Políticas de manejos de cambios			X

Documentación de todas las políticas y procedimientos				X
Toda comunicación debe ser segura	X			
Implementación de un DLP	X			
Implementación de un DRM	X			
Implementación de CASB	X			
Encriptación de datos en tránsito	X	X		X
Encriptación de datos en reposo	X	X		X
Encriptación basada en FIPS	X			
Etiquetado de datos	X	X		
Respaldo de datos	X			
Correo electrónico encriptado	X			
Política de controles criptográficos		X		
Políticas de seguridad de la información		X		X
Políticas de restricción de acceso a información de tarjetas de crédito				X
Documentación de todas las políticas y procedimientos				X

4.2.2. Normativas internacionales. Se revisan las normativas y recomendaciones de la OECD y GDPR. Debido a que algunas organizaciones hacen negocios con la Unión Europea se debe considerar el GDPR, ya que su cumplimiento será obligatorio en caso de

manejar información de clientes ubicados dentro de la UE. Recientemente, Costa Rica pasó a ser parte de la OECD, la cual establece normativas que todavía no están sujetas a cumplimiento, pero es importante que las recomendaciones se consideren en caso de ser adoptadas por el gobierno. Con el siguiente análisis se responderá el objetivo específico 2: Revisar las normativas de GDPR y OECD en el contexto de ciberseguridad con el enfoque de cero confianza. Se utilizan las mismas áreas de análisis que en el punto anterior.

4.2.2.1. OECD. Las normativas de la OECD han sido definidas para organizaciones de manufactura tecnológica o de calidad de *software*, en ambos casos tienen un enfoque de seguridad, pero de manera lamentable no aplican para el caso de estudio en su totalidad.

De las normativas revisadas es posible destacar la importancia que la OECD le da a la criptografía y dicta que las organizaciones deben definir políticas, métodos, medidas, prácticas y procedimientos criptográficos. Además, destaca la importancia de alinearse con pautas internacionales y nacionales, en Costa Rica no hay ninguna pauta que supere a la ya estudiada y definida por la NIST. La OECD recomienda revisiones de la política, de manera cíclica, al menos cada 5 años.

Tabla 14
Controles OECD

Controles/Políticas	NIST	ISO	PCI	OEC D
Encriptación de datos en tránsito	X	X	X	X
Encriptación de datos en reposo	X	X	X	X
Política de controles criptográficos		X		X

4.2.2.2. GDPR. Al igual que la OECD, GDPR tiene un área específica de desarrollo, la cual es el tratamiento de los datos de habitantes de la UE. Lo único que se puede destacar de la normativa para el caso de estudio es que GDPR afirma que cuando exista un tratamiento de datos de habitantes de la UE debe existir un delegado de protección de datos personales y

que este y la organización deben asegurar que la transferencia de datos personales fuera de UE sea segura. Los controles de encriptación de datos en tránsito y reposo, junto con las políticas de seguridad de la información, pueden apoyar lo definido por GDPR.

Tabla 15
Controles GDPR

Controles/Políticas	GDPR
Encriptación de datos en tránsito	X
Encriptación de datos en reposo	X
Política de controles criptográficos	X
Políticas de seguridad de la información	X
Delegado de protección de datos personales **	X

4.2.2.3. Resultados. A continuación, la Tabla 16 presenta los cinco controles o políticas encontradas en el análisis documental de las normativas estudiadas y su relación. Solo se agregó una línea más a los ya que se encontraron en el punto 4.2.1, la cual ha sido marcada con asteriscos (**) porque solo aplica si se usan datos de habitantes de la UE.

Tabla 16
Resultados de las normativas internacionales estudiados

Controles/Políticas	OECD	GDPR
Encriptación de datos en tránsito	X	X
Encriptación de datos en reposo	X	X
Política de controles criptográficos	X	X

Políticas de seguridad de la información	X
Delegado de protección de datos personales **	X

4.2.3. Conclusión de los resultados. El análisis documental brindó una lista de 53 controles o políticas. Divididas de la siguiente manera, 20 para el área de identidad, 18 para el área de administración de dispositivos y 15 para el almacenamiento de datos.

Como se puede observar en la lista cero confianza se alinea con los estándares internacionales o normativas en el mercado y hay poco que puedan agregar que no contemple cero confianza. ISO agrega un poco más de controles y políticas. PCI agrega protección de la información de tarjetas de crédito.

El marco de referencia de cero confianza de la NIST va más allá de lo que establece la ISO y el PCI o cualquiera de las normativas, lo cual es un punto de mejora para cualquier organización actualmente este teletrabajando y tengo ISO o PCI implementadas.

Tabla 17

Resultados finales

Controles/Políticas	NIST	ISO	PCI	OEC D	GDP R
Política del menor privilegio	X	X	X		
Políticas dinámicas de acceso	X				
RBAC	X	X			
ABAC	X				
Autorización individual	X		X		
Implementación de ICAM	X				

Uso de cuenta administrador	X		
Autenticación constante	X		X
MFA/CMFA	X		X
Minimizar zonas de confianza implícita	X		
Limitar la administración remota	X		
Inventario de los sujetos físicos y virtuales	X	X	
Trazabilidad de usuarios	X		
Políticas de bloqueo de sesión	X		
Inventarios de bajas de usuarios		X	
Políticas de asignación, evaluación y revocación de privilegios		X	
Políticas de restricción y control de cuentas privilegiadas		X	
Políticas de aseguramiento de información de autenticación		X	X
Eliminación de cuentas compartidas			X
Documentación de todas las políticas y procedimientos			X
Monitoreo de cumplimiento de dispositivos	X		

Actualización de sistema operativo	X		X
Actualización de aplicaciones	X		X
Inventario de dispositivos	X	X	
Administración de dispositivos	X		
Inventario de aplicaciones	X		
Antimalware	X	X	X
Actualización remota de antimalware	X	X	X
Firewall	X		X
Actualización remota de firewall	X		X
Escaneos periódicos	X		
Políticas de uso aceptable de activos		X	
Registro de eventos		X	
Políticas de instalación de Aplicaciones		X	
Identificar activos que almacenan o procesen información de crédito			X
Evaluación y reparación de vulnerabilidades			X
Políticas de manejos de cambios			X

Documentación de todas las políticas y procedimientos						X
Toda comunicación debe ser segura	X					
Implementación de un DLP	X					
Implementación de un DRM	X					
Implementación de CASB	X					
Encriptación de datos en tránsito	X	X	X	X	X	X
Encriptación de datos en reposo	X	X	X	X	X	X
Encriptación basada en FIPS	X					
Etiquetado de datos	X	X				
Respaldo de datos	X					
Correo electrónico encriptado	X					
Política de controles criptográficos		X		X	X	
Políticas de seguridad de la información		X	X			X
Políticas de restricción de acceso a información de tarjetas de crédito				X		
Documentación de todas las políticas y procedimientos						X
Delegado de protección de datos personales**						X

Capítulo V. Propuesta

Como se pudo observar durante el análisis de resultados, muchas de las organizaciones han implementado controles de seguridad mínimos o controles de seguridad alineados con las mejores prácticas en el mercado, esa afirmación no implica que las organizaciones tengan una estrategia basada en cero confianza. La confianza en sus empleados y los ambientes de casa ha sido uno de los principales problemas del teletrabajo y como se puede observar en el desarrollo del trabajo el modelo de cero confianza pone en duda todos esos ambientes posibles en la organización y fuera de ella y prepara para enfrentar lo peor y minimizar los riesgos.

A continuación, se desarrolla una propuesta de ciberseguridad para el teletrabajo a partir del modelo de cero confianza la cual pueda ser aplicable en cualquier organización. Para lograr lo cometido se tomaron en cuenta los estándares internacionales de la ISO y PCI, así como las normativas de la OECD y GDPR. La propuesta a continuación tomara en cuenta solo las partes que al investigador le parecieron pertinentes durante su análisis de estándares y normativas, por lo tanto, no debe utilizarla como marco de referencia para la implementación o para cumplir con este estándares y normativas. Cada organización debe cumplir cualquier obligación de cumplimiento legal que tenga su área de negocio o países de operación. Puede que la investigación no haya capturado todos los estándares o normativas pertinentes para algunos casos especiales, por lo que la organización tendrá que tomar en cuenta cualquier otro estándar o normativa no evaluado en esta investigación. Finalmente, la persona investigadora recomienda evaluar la propuesta y revisar los controles propuestos en fin de utilizar los más adecuados en el momento de la implementación.

Cabe destacar que esta propuesta no es una guía para una implementación completa de cero confianza para una organización, como se ha descrito solo contempla algunas partes de la organización y está enfocado en el teletrabajo.

Se usa de referencia el modelo dado por la NIST para la implementación de cero confianza estudiado y desarrollado en el marco conceptual o la propuesta de la NIST en Sp800-37 RFM (Risk Management Framework for Information Systems and Organizations y Rose, Borchert, Mitchell y Connelly (s. f.).



Ilustración 31

Basado en el documento de la NIST y sus pasos documentados en el RMF

En la imagen anterior se pueden ver los pasos principales de la RMF, son los propuestos por la NIST cuando la organización ya implementó cero confianza y busca expandir el modelo. Abajo es posible ver la explicación de cada paso según la NIST:

1. Evaluación.

- a. Inventario de sistemas: la organización debe identificar cualquier componente de *hardware* (portátiles, teléfonos, IoT, etc.) o artefacto digital (cuentas de usuario, aplicaciones, certificados digitales, etc.).
- b. Inventario de usuarios: la organización debe conocer los sujetos de la organización, estos pueden ser físicos o virtuales, así como cuales tienen permisos especiales o privilegiadas. Finalmente, estas cuentas deben revisarse y evaluarse, con fin de corregir atributos o roles incorrectos. Ninguna cuenta debe acceder a todos los recursos de la organización. Todas las cuentas deben tener la flexibilidad necesaria para cumplir los requerimientos del negocio. Todas las cuentas deben tener trazabilidad.

- c. Revisión de procesos de negocio: la organización debe ser capaz de identificar y categorizar en importancia los procesos de la empresa, los flujos de datos y su relación con la misión de la empresa. El inventario debe detallar los procesos de negocio y las circunstancias donde se debe permitir o denegar el acceso a un recurso o sistema.
2. Evaluación de riesgos y desarrollo de políticas: se debe considerar para la identificación de un proceso candidato su importancia en los procesos de negocio, grupo de sujetos afectados y el estado actual de los recursos usados por el flujo de trabajo. La evaluación de riesgos puede ser hecha sigue la publicación NIST SP800-37 (Risk Management Framework, cuadro de administración de riesgos). Durante este proceso se deben identificar los recursos arriba (sistema de administración de ID, Bases de datos, microservicios, etc.), abajo (registros o bitácoras, monitoreos, etc.) y todas las entidades (sujetos, cuentas de servicio, etc.) de cada proceso o flujo de trabajo. Una vez se ha realizado la evaluación del riesgo y se conocen todos los actores del flujo del proceso, el administrador debe definir los criterios y las fuentes de información que se utilizan para construir el nivel de confianza que requiera el proceso de negocio, este puede requerir mayor afinación.
3. Despliegue: el arquitecto de la organización debe crear una lista de posibles soluciones, según las necesidades de la organización. Entre las preguntas recomendadas están:
 - a. ¿La solución requiere que componentes se instalen en los activos empresariales?
 - b. ¿La solución funciona donde los procesos empresariales existen completamente en el centro de datos local?
 - c. ¿La solución provee de medios para analizar los registros?
 - d. ¿La solución provee soporte a diferentes aplicaciones, servicio y protocolos?
 - e. ¿La solución requiere cambios en el comportamiento del sujeto?

4. Operación y monitoreo: los administradores empresariales deben implementar las políticas desarrolladas en los componentes seleccionados, lo cual requerirá de observación y monitoreo, hasta asegurarse de que las políticas son efectivas y permiten que el proceso funcione como se espera. Estos monitoreos bases pueden ser que se utilizan para construir patrones de comportamiento y detectar comportamientos anómalos.

El siguiente gráfico a continuación representa el modelo propuesto por esta investigación, como se puede observar tiene pasos adicionales para ayudar la implementación de la propuesta y que sea ajustable a diferentes organizaciones con diferentes procesos internos:

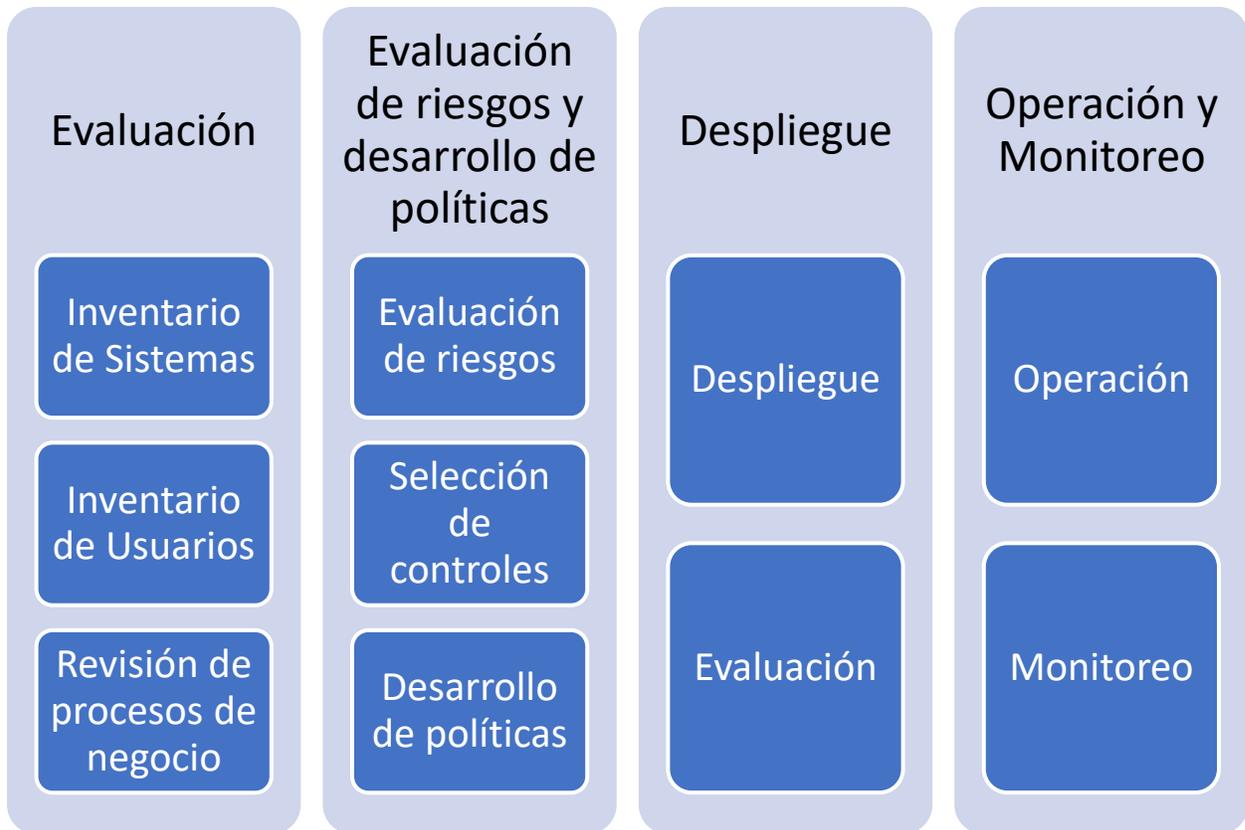


Ilustración 32

Ciclo de la mejora continua propuesta

5.1. Fase 1: Evaluación

5.1.1. Introducción. Como lo detalla la NIST y como se resume en el Marco conceptual, la implementación del modelo de cero confianza es un viaje, es decir, es un proceso continuo, la NIST afirma que las implementaciones de los modelos puros de cero confianza se hacen gradualmente, lo cual aplica a la propuesta, ya que esta empieza con tres áreas de la organización y con un enfoque de cero confianza. El proceso descrito por la NIST establece el siguiente orden de implementación y empezando por los activos o recursos más valiosos:

1. Implementación de principios.
2. Cambio de procesos.
3. Soluciones tecnológicas.

La propuesta no es una implementación pura de cero confianza pero es posible usar esos tres puntos de base durante el desarrollo de los pasos a continuación.

5.1.2. Propósito. La fase de evaluación se divide en tres secciones donde la organización tratará de descubrir todos los sujetos involucrados en los procesos de negocios, así como el flujo de tráfico en cada proceso de negocio, sus dependencias y sus posibles escenarios. Este proceso le permite a la organización enlistar los procesos candidatos en la migración al modelo de cero confianza.

5.1.3. Etapas. A continuación, se definen las etapas.

5.1.3.1. Inventario de sistemas. Seguidamente, se define el inventario de sistemas.

5.1.3.1.1. Introducción. Este es el primer paso para llevar a cabo la evaluación de los procesos de negocio y debe hacerse para toda la organización, independientemente de los sujetos involucrados en el teletrabajo, es una buena práctica tener un inventario de los sistemas organización y tener algún control sobre su estado. Se ha utilizado la documentación de la NIST como guía de desarrollo. Según la NIST esto incluye cuentas de usuario, pero estas se inventarían más adelante, por lo que no se contemplaran en el punto a continuación.

5.1.3.1.2. Propósito. El propósito de la primera etapa de la Fase I es conocer todos los dispositivos organizaciones que pueden interactuar con cualquiera de los procesos de negocio candidatos. Esto le permite a la organización conocer el estatus de los dispositivos, con el fin de conocer el cumplimiento de sus dispositivos o conocer la información disponible para crear las políticas o las reglas de acceso efectivas.

5.1.3.1.3. Procedimiento. Según la publicación de la NIST SP800-53 R4 (NIST, 2013) en el control CM-8: Inventario de componentes de Sistemas de Información el inventario de sistemas debe ser desarrollado por la organización y debe:

1. Debe reflejar la información actual de los sistemas de la organización.
2. Debe incluir todos los componentes entre los límites de la organización.
3. Debe tener la granularidad necesaria para su rastreo y reporte.
4. Debe incluir un responsable.

La organización debe revisar y actualizar el inventario, de manera periódica. El inventario puede contener un responsable asociado o usuario/dueño, especificaciones de *hardware*, información de licencias, *software* instalado, versiones de *software*, componentes de red, nombre de la máquina o nombres, direcciones de red, ubicación física y también puede contener información del *hardware* (fabricante, tipo de dispositivo, modelo y número de serie). El inventario puede utilizar códigos por objeto como se utiliza en muchos modelos de inventario y de evaluación de riesgo. Se pueden utilizar código como los ejemplificados a continuación:

Tabla 18

Códigos de inventario de Sistemas

Tipo	Código
Estación de trabajo	EDT
Portátiles	POR
Teléfonos	TEL
IoT	IoT
Aplicaciones	<i>APP</i>
Certificados	CER

Los dispositivos pueden inventariarse de la siguiente manera, en un *software* de inventario o plataforma:

Tabla 19

Ejemplo de inventario de activos

Tipo	ID	Nombre	Dueño	CPU	Memoria	Marc	Modelo	Número de serie	MAC	Dirección IP	Ubicación
EDT	WORKSTATION1000001		Mauro Domínguez	Intel® Core™ i5-11500HE Procesador (12M Cache, up to 4.50 GHz)	32 GB	Dell	OptiPlex 7090	VAVC-ADFS-432	30-65-EC	172.52.2.103	San José
POR	LAPTOP1000001		Laura Gala	Intel® Core™ i5-1155G7 Procesador (8M Cache, up to 4.50 GHz)	16 GB	Lenovo	ThinkBook 14 2. ^a Gen	3J45B-KJ34HB	00-44-EC	192.168.3.45	Heredia

				4.50 G Hz)							
TE L	TEL - 0000 001	CELLPHO NE1	Juan Ferná ndez	Snapd ragon 888 5G Mobil e Platfor m	8 GB	Sam sung	Samsu ng Galax y S21 Ultra 5G	SDA83 934	11- 48- EC - 6F - C4 -58	10.1.13	Alaju ela
Io T	IoT- 0000 001	CAMERA 1	Robert o Elizon do	-		Mi	Wirel ess Outdo or Securi ty Camer a	MI- 54564	52- 01- EC - 6F - C4 -58	171.25. 52.113	San José

Las aplicaciones deben inventariarse en otra tabla, ya que sus atributos y propiedades difieren y puede usarse un control similar al siguiente:

Tabla 20

Ejemplo de inventario de aplicaciones

Tipo	ID	Nombre	Dueño	Marca	Versión	Idioma
APP	APP- 0000001	Word	Marcos Brenes	Microsoft	2019	ESP

APP	APP- 0000002	Excel	Marcos Brenes	Microsoft	2019	ESP
-----	-----------------	-------	------------------	-----------	------	-----

Las aplicaciones deben ser relacionables con los activos en los que se encuentran instaladas, se pueden relacionar, de manera sencilla, con los ID de cada uno como llave primaria y se puede incluir información de la aplicación en el activo como su fecha de instalación:

Tabla 21

Relación de aplicaciones y activos

ID Activo	ID APP	Fecha de instalación
EDT-0000001	APP-0000001	10/15/2020
EDT-0000001	APP-0000002	10/15/2020

5.1.3.2. Inventario de usuarios. A continuación, se define el inventario de usuarios.

5.1.3.2.1. Introducción. El segundo paso de la Fase I complementa el primero, después de haber identificado los dispositivos lo siguiente es conocer los usuarios de la organización.

5.1.3.2.2. Propósito. En este paso no solo se busca inventariar de los usuarios regulares, se deben incluir las cuentas de administración o servicio, asimismo, sus grupos, roles y tipos. La organización debe ser capaz de obtener la información y verificar que los accesos que tiene cada cuenta son justo lo que requiere para llevar a cabo su trabajo y se debe comprobar que ninguna cuenta tiene acceso a todos los recursos de la organización. Este inventario, al igual que el primero, debe permitir conocer la información con la que cuenta para reconocer perfiles de usuario y patrones esperados de uso.

5.1.3.2.3. Procedimiento. El inventario de cuentas de usuario se describe de esta manera por la NIST, por lo que una solución similar puede utilizarla y se pueden agregar códigos similares para identificar las diferentes cuentas, en este caso se agregan cuentas de

usuarios y cuentas de servicio.

Tabla 22

Códigos de inventario de sistemas y usuarios

Tipo	Código
Estación de trabajo	EDT
Portátiles	POR
Teléfonos	TEL
IoT	IoT
Aplicaciones	APP
Certificados	CER
Cuenta de Usuario	CDU
Cuenta de Servicio	CDS

Nuevamente, los atributos de usuario son diferentes y precisa de otra tabla con la información de que la organización considere pertinente y que tenga disponible.

Tabla 23

Información de usuarios

Tipo	ID	Usuario	Nombre	Apellidos	Ubicación	Grupos de AD
CDU	CDU-0000001	ROLOAL	Rolando	Loal	San José	Windows_SYSADMINS, Remote_Users

CDU	CDU- 0000002	JEHERA	Jenny	Hernández	San José	Remote_Users, Contabilidad
CDS	CDS- 0000001	SQL_SVA CC	SQL_SVA CC	-	San José	SQL_DBA
CDU	CDU- 0000004	ANNARA	Ana	Naranjo	San José	Remote_Users, Tesoreria

En el ejemplo anterior se agregan los grupos de los que los usuarios tienen acceso como un ejemplo, puede existir una tabla de los grupos y otra de su relación. Los grupos pueden dar visibilidad de cuales cuentas son parte de grupo privilegiados o con permisos especiales, este inventario se puede apoyar con un sistema de manejo de privilegios que apoye la evaluación de los roles o permisos dados según los grupos a los que estas cuentas pertenecen.

5.1.3.3. Revisión de procesos de negocio. A continuación, se define la revisión de procesos de negocio.

5.1.3.3.1. Introducción. Este es el último paso de la Fase I y es donde el inventario de sistemas y de usuarios apoya la revisión de procesos de negocio. Todos los sujetos involucrados dan forma a los procesos o procedimientos que la organización considera migrar.

5.1.3.3.2. Propósito. En este paso se busca inventariar los procesos y sus procedimientos, además, debe enfocarse en los procesos involucrados con el teletrabajo, es decir, los usuarios o dispositivos que realicen procesos de negocio fuera de la organización. Una vez que se conocen los procesos y procedimientos involucrados es posible empezar a relacionar dispositivos, usuario o grupos con estos procesos y desarrollar diagramas de flujo que den visibilidad de lo que es aceptable o no, esto ayuda con el desarrollo de políticas de acceso y saber cuándo cero confianza debe confiar o no en un dispositivo o usuario para un proceso de negocio. La organización puede utilizar diferentes metodologías para desarrollar los diagramas de flujo, lo importante en este paso es relacionar los sistemas, los usuarios y

los procesos e identificar su relación y su comportamiento esperado o aceptado, así como el no esperado o no aceptado.

5.1.3.3.3. *Procedimiento.* Se puede empezar por departamento o unidad de negocio, sus procesos y procedimientos. Se necesita agregar un nuevo tipo al inventario:

Tabla 24

Códigos de inventario de sistemas, usuarios y procesos

Tipo	Código
Estación de trabajo	EDT
Portátiles	POR
Teléfonos	TEL
IoT	IOT
Aplicaciones	APP
Certificados	CER
Cuenta de Usuario	CDU
Cuenta de Servicio	CDS
Procesos	PRO
Diagramas	DÍA

Finalmente, se pueden usar ID relacionales para construir ID de proceso y procedimientos:

Tabla 25

Definición de código de departamento

Tipo	Departamento	ID
PRO	Tecnologías de información	PRO-TI

Tabla 26

Definición de código de proceso

Departamento ID	Proceso	ID
PRO-TI	Gestión de tecnología e infraestructura	PRO-TI-GDT

Tabla 27

Definición de código de procedimiento

Proceso ID	Procedimiento	ID	Criticidad	Diagrama de flujos
PRO-TI-GDT	Procedimiento de análisis de necesidades nuevas tecnologías en salud	PRO-TI-GDT-0001	Alto	DIA-000001
PRO-TI-GDT	Procedimiento de incorporación de tecnología	PRO-TI-GDT-0002	Medio	DIA-000002
PRO-TI-GDT	Procedimiento de gestión de tecnología	PRO-TI-GDT-0003	Bajo	DIA-000003

La organización puede utilizar alguna metodología del mercado para definir la criticidad, en el ejemplo anterior solo se utilizaron tres niveles. La organización puede definir

el método de medición que se adapte a los estándares que se adoptaron o a las necesidades del negocio.

La última columna de la última tabla es el ID del diagrama, cada proceso debe tener un diagrama de flujo de datos donde se detalle el flujo de los datos, la interacción con los sujetos, cuentas, sistemas u otros procedimientos, así como los diferentes casos de uso o eventos donde el acceso debe ser permitido o denegado. Se pueden utilizar los diagramas o flujos de datos agregados en la sección diagramas o flujos de datos, los cuales ilustran escenarios cubiertos por esta investigación.

5.2. Fase 2: Evaluación de riesgos y desarrollo de políticas

5.2.1. Introducción. En la Fase 2 la organización debe ser capaz de usar los datos de la Fase 1 y desarrollar una evaluación de riesgos y definir las políticas de seguridad y privacidad. Para ser exitosos en esta fase es fundamental haber descubierto todos los sistemas y los procesos de negocio involucrados en el teletrabajo.

5.2.2. Propósito. El propósito de la Fase 2 es evaluar los riesgos en los procesos que se identifican y los sujetos involucrados y utilizar los reportes de la evaluación de riesgos como evidencia para seleccionar los controles necesarios. Asimismo, desarrollar las políticas de seguridad y privacidad que posteriormente apoyarían la implementación y dan una base para las pruebas o actualización de políticas o configuración de los controles seleccionados.

5.2.3. Etapas. A continuación, se definen las etapas.

5.2.3.1. Evaluación de riesgos. Seguidamente, se define la evaluación de los riesgos.

5.2.3.1.1. Introducción. La evaluación de riesgos debe identificar las amenazas de los procesos seleccionados y los sujetos involucrados. Para este primer paso la organización puede utilizar cualquiera de la metodología en el mercado, se recomienda la que mejor se acople con el negocio.

En esta investigación se explican las publicaciones de la NIST que pueden usarse como referencia, pero también se puede recurrir a otras metodologías como la Magerit. Posteriormente, en este paso se exponen los puntos principales de las publicaciones SP800-37: Risk Management Framework (NIST, 2021), SP800-30: Guide for conducting Risk

Assessment (NIST, 2012) y SP800-53: Security and Privacy Controls for Federal Information Systems and Organizations (NIST).

5.2.3.1.2. *Propósito.* Según lo define la NIST, es determinar y relacionar los riesgos y amenazas de los procesos de negocio con los activos y usuarios que se identifican en la Fase 1. Se exponen otros propósitos que describen el objetivo de cada publicación en específico.

5.2.3.1.3. *Procedimiento.* Como se expuso en la introducción se habla de las tres publicaciones de la NIST:

1. Risk Management Framework, las fases 1 y 2 del RMF contienen un marco de evaluación de riesgos y selección de controles comunes.

1.1. Preparación.

1.1.1. Propósito: este primer paso preparar todos los niveles de la organización para manejar su seguridad y riesgos de privacidad.

1.1.2. Resultados:

1.1.2.1. Identificación de roles clave para el manejo de riesgos.

1.1.2.2. Establecer una estrategia para el manejo de riesgo organizacional y determinar el nivel de tolerancia de riesgo.

1.1.2.3. Evaluación del riesgo organizacional.

1.1.2.4. Estrategia de monitoreo.

1.1.2.5. Identificación de controles comunes.

1.2. Categorización.

1.2.1. Propósito: informar de los procesos y tareas del manejo de riesgo organizacional que determina el impacto adverso a la confidencialidad, integridad y disponibilidad de los sistemas de información que procesen, guarden y transmitan información.

1.2.2. Resultados:

- 1.2.2.1. Documentar las características de los sistemas.
 - 1.2.2.2. Completar la categorización de seguridad de los sistemas e información de la organización.
 - 1.2.2.3. Manual de categorización revisada y aprobada por el responsable.
2. Guide for Conducting Risk Assessments, esta publicación se basa en la SP800-39. Esta metodología define un proceso de manejo o evaluación de riesgos de cuatro etapas en donde cada etapa interactúa con la otra directamente. En esta publicación la NIST establece que el evaluador y la organización deben conocer el propósito, el alcance, los supuestos y limitaciones previstos, las fuentes de información y el modelo de riesgos utilizado.

2.1. Definición de riesgos:

- 2.1.1. Propósito: este paso busca definir los riesgos o darles contexto a los riesgos de la organización, describe y relaciona los riesgos con el ambiente para facilitar la toma de decisiones. Con esta información la organización puede producir una estrategia de manejo de riesgos, además de definir los límites de la organización o de los controles.

2.2. Evaluación de riesgos:

- 2.2.1. Propósito: identificar las amenazas a la organización, sistemas, activos o sujetos; identificar las vulnerabilidades internas y externas; identificar los posibles daños o escenarios en caso de materializarse una amenaza y la posibilidad de que sucedan.

2.3. Respuesta a riesgos:

- 2.3.1. Propósito: este paso se alimenta de la evaluación de riesgos realizada en el punto 2.2 y determina el tipo de respuesta que tendrá la organización a los riesgos que se identifican según el marco definido por la organización.

2.4. Monitoreo de riesgos:

- 2.4.1. Propósito: determinar la eficacia de la respuesta a riesgos, identificar el cambio en el impacto de los riesgos y verificar que los planes de respuesta se encuentran implementados y cumplen la misión de la organización, además de cumplir con cualquier marco legal relacionado.
3. Security and Privacy Controls for Federal Information Systems and Organizations, en el control RA-3 define 5 puntos:
 - 3.1. Evaluación de riesgos, la organización debe evaluar los riesgos con base en la posibilidad de ocurrencia y magnitud de daño para la organización en caso de un acceso no autorizado, usos no deseados, filtración de información, interrupción de servicios, modificación de servicios o datos o destrucción de activos o datos en sistemas de información y activos que procesen, almacenen y transmitan información.
 - 3.2. Documentación de los resultados de la evaluación de riesgos.
 - 3.3. Revisión de los resultados de la evaluación de riesgos.
 - 3.4. Diseminación de los resultados de la evaluación de riesgos.
 - 3.5. Actualización de la evaluación de riesgos en caso de cambios significativos u otros factores que puedan cambiar los resultados.

Una vez que se haya seleccionado la metodología de evaluación de riesgos, se debe documentar el proceso de evaluación, la definición de los riesgos y cada riesgo usando los procesos documentados. Posteriormente, se relacionan los riesgos con los activos que se identifican en los pasos anteriores y en los diagramas de flujo. Se propone construir una tabla de riesgos y tipos de riesgos con identificadores como se expuso en la Fase 1 con los activos o similar que le permita a la organización general un código por amenaza o riesgos identificado.

Durante la evaluación de riesgos se debe tener una mentalidad de cero confianza la cual se logra sigue los principios expuestos en la Fase 1, se debe recordar que ese es el primer para la adopción del modelo de cero confianza:

- Verificar explícitamente: autenticar y autorizar siempre en función de todos los puntos de datos disponibles.
- Utilizar la política de menos privilegios (Least Privileged): limitar el acceso de usuario con políticas de tiempo y acceso necesario para llevar a cabo sus tareas, utilizar políticas adaptables al riesgo y las políticas de protección de datos.
- Asumir una ruptura de seguridad: siempre trata de minimizar el radio de daño y el acceso por medio de la segmentación. Verificar la encriptación de punto a punto, utilizar herramientas de análisis para tener visibilidades de las transacciones, impulsar la detección de amenazas y mejorar los controles de defensa.

5.2.3.2. Selección de controles. A continuación, se define la selección de controles.

5.2.3.2.1. Introducción. La selección de los controles apropiados puede ser uno de los pasos más complicados para pequeñas y medianas empresas y es donde el costo y el personal técnico desempeñan un papel importante. En la actualidad, existen muchas organizaciones con controles alineados al modelo de cero confianza, mas no tienen la mentalidad del modelo y en otros casos algunas tienen controles que no ofrecen una solución alineada al modelo de cero confianza.

Muchas veces las organizaciones deben recurrir a múltiples proveedores para alinear los controles seleccionados con sus objetivos de negocio. Es importante que las organizaciones evalúen los controles actuales y su aplicabilidad con las políticas o controles definidos por la organización a partir del modelo de cero confianza.

5.2.3.2.2. Propósito. Según la NIST en su publicación de la RMF (NIST, 1) el propósito del paso de selección de controles es seleccionar, adaptar y documentar los controles necesarios para proteger el sistema y la organización de acuerdo con los riesgos que se identifican. Este paso debe generar:

1. Controles bases seleccionados y adaptados.
2. Controles designados a sistemas específicos, híbridos o comunes.
3. Controles asignados a componentes específicos de sistema.

4. Estrategia de monitoreo continuo en el sistema.
5. Planes de seguridad y privacidad que reflejen la selección de controles, así como su designación y asignación revisada y aprobada por los responsables.

5.2.3.2.3. *Procedimiento.* Es importante destacar que los controles son salvaguardas de los activos, empleados, clientes y recursos de las organizaciones, deben cumplir la función deseada por la empresa, ya sea protección parcial o total frente a las posibles amenazas que puedan materializarse. Con la evaluación de riesgos y frente a un riesgo una organización puede:

- Aceptar el riesgo: es cuando la organización decide no hacer nada. Una opción utilizada en amenazas poco importantes o con un impacto pequeño.
- Transferir el riesgo: es cuando el control implementado se maneja por un tercero que asumirá toda la responsabilidad.
- Mitigar el riesgo: es cuando la organización implementa y gestiona los controles seleccionados para reducir el impacto estudiado en la evaluación de riesgos.
- Evitar el riesgo: es cuando la organización intenta reducir o eliminar el riesgo con todos los controles considerados necesarios.

Todas estas acciones se respaldan con la documentación de la evaluación de riesgos y la documentación de las decisiones realizadas por el negocio. La organización debe continuar, de forma periódica, la evaluación de riesgos para tener visibilidad de estado real de cada uno de los riesgos de la organización.

Para las áreas seleccionadas ya hemos listado los controles alineados con el modelo de cero confianza en la sección 4.2.3, los cuales pueden adaptarse y seleccionarse por la organización según sus necesidades de negocio. Los diagramas de referencia bajo la sección 2.1.3.3 pueden utilizarse como ejemplos para la definición de controles y selección de soluciones y pueden apoyar la definición de políticas.

5.2.3.2.3.1. *Identidad.* Como guía de implementación es posible revisar la documentación de Microsoft (2021), en donde destaca que el riesgo con la identidad ha aumentado con la expansión del perímetro de las organizaciones, el cual ha crecido con el

uso de aplicaciones en la nube y por los trabajadores remotos. Asimismo, durante el desarrollo del trabajo se observó cómo el teletrabajo agrega complejidad a los sistemas de identidad de la organización y cómo los controles tradicionales de perímetro ya no se ajustan a las necesidades de la organización cuando sus empleados trabajan fuera de la red organizacional.

Microsoft (2021) asegura que los controles deben moverse donde la información y los usuarios están para ser efectivos, con el objetivo de asegurar que se verifica la identidad de los sujetos con un método de autenticación fuerte (como MFA y Acceso Condicional) antes de brindar acceso a los recursos empresariales. La organización debe confirmar que el acceso está autorizado y que es parte del comportamiento típico del sujeto. La autorización debe estar alineada con el principio del menor privilegio.

5.2.3.2.3.2. Administración de dispositivos. Es posible usar a Microsoft (s. f.) como guía y destacar la gran variedad de dispositivos que pueden acceder a una red organizacional y cómo los controles deben adaptarse a esto. En las organizaciones modernas no todos los dispositivos pueden administrarse o no todos son activos de la organización (BYOD o terceros), lo cual generará una variedad de configuraciones y diferentes niveles de actualización en la red de la organización.

La gran variedad de escenarios creada por la variedad de dispositivos aumenta la superficie de ataque y los controles de la organización deben evitar que los dispositivos no confiables tengan acceso a los recursos sensibles. Es posible destacar el principio de cero confianza, nunca confiar, siempre verificar, al seguir ese principio la organización debe verificar a todos los dispositivos que soliciten acceso a los recursos. Los principios de cero confianza deben aplicarse por medio de políticas y controles a los dispositivos de la organización y los dispositivos de terceros que precisen de acceso.

La organización debe ser capaz de aplicar las políticas sin importar su sistema operativo o naturaleza, si no pudiese aplicar las políticas definidas puede recurrir a otras opciones como la segmentación de red y dar acceso solo a los recursos públicos. También puede bloquear el acceso a todos los dispositivos que no cumplan con las políticas o controles definidos.

Es importante que las organizaciones puedan evaluar la confianza de las aplicaciones que corren en los dispositivos y evitar que información corporativa sea accedida por aplicaciones no confiables o desconocidas. Para los controles de dispositivos se deben considerar los siguientes puntos:

1. Las políticas de seguridad comprenden la seguridad de los dispositivos, la configuración de los dispositivos, la protección de aplicaciones (de ser posible por medio de MAM u otras soluciones), el cumplimiento del dispositivo y debe generar información de la postura de riesgo.
2. El despliegue de sistemas operativos y aplicaciones deben realizarse de manera segura y deben ser correctamente configuradas y actualizadas.
3. La organización debe velar por el acceso seguro de los datos de la organización.
4. Se debe verificar por medio de un control de acceso que las políticas de seguridad organizacionales han sido aplicadas antes de que los datos se accedan por un dispositivo.

5.2.3.2.3.3. *Almacenamiento de datos.* Nuevamente, como guía se consulta la guía de implementación del modelo de cero confianza para datos de Microsoft (2021), en esta área se habla de la importancia de proteger los datos organizacionales, es una de las mayores responsabilidades de los equipos de seguridad y cumplimiento. Explica que los controles de datos deben apoyarse con los controles implementados en los dispositivos, las aplicaciones, la infraestructura y las redes.

Por el alcance del trabajo de investigación solo se aborda identidad y la administración de dispositivos, pero las organizaciones pueden optar por expandir el alcance de la implementación si se alinea con sus necesidades de negocio. Para proteger los datos y asegurar que el acceso a los datos realice por los usuarios autorizados los datos deben ser inventariados, clasificados, etiquetados y cuando sea necesario encriptados.

Se pueden considerar los puntos a continuación para asegurar los datos, de manera eficiente:

1. Conocer los datos, la organización debe descubrir todos los datos en la organización y clasificarlos con etiquetas de sensibilidad.
2. Proteger los datos y prevenir la pérdida de datos. La información sensible debe protegerse con políticas de protección de datos y métodos de encriptación.
3. Monitorear y remediar, los datos sensibles deben monitorearse continuamente, con el fin de detectar violaciones en las políticas o comportamiento riesgoso de usuarios y modificar el acceso a los datos o las políticas de protección si fuese necesario.

Utilizando los puntos expuestos, la organización conoce sus datos, puede mejorar sus políticas, puede encriptar los datos sensibles, autoclasifica el contenido de los datos y monitorea el contenido sensible.

5.2.3.2.3.4. Otros recursos. A continuación, se mencionan otros recursos disponibles.

5.2.3.2.3.4.1. Microsoft. Ha facilitado un examen de madurez del modelo de cero confianza, el cual puede ayudar a la organización a entender el estado actual de la organización y conocer los controles ofrecidos por Microsoft, así como familiarizarse con las soluciones aptas para el modelo de cero confianza. Aún con este examen la organización se debe ejecutar la Fase 1 y la Fase 2, pero puede utilizarse como base. Los exámenes a continuación no se enfocan en el teletrabajo y pueden ser muy generales.

Los *links* de los exámenes de las áreas previstas en la investigación son:

- Identidad, <https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard:primaryr2>
- Administración de dispositivos, <https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard:primaryr3>
- Almacenamiento de datos, <https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard:primaryr6>

5.2.3.3. Desarrollo de políticas. A continuación, se define el desarrollo de políticas.

5.2.3.3.1. Introducción. En este paso la organización utiliza los resultados de los pasos anteriores para desarrollar las políticas de seguridad y privacidad organizacionales que se aplican a los controles seleccionados. Como lo define la NIST los resultados y los reportes generados por la evaluación de riesgos deben servir como evidencia para apoyar las políticas de la organización.

5.2.3.3.2. Propósito. El propósito de este paso es identificar las políticas que apoyan a los controles seleccionados, documentarlas, definir estrategias de comunicaciones, así como los responsables o involucrados.

5.2.3.3.3. Procedimiento. El control SA-1 de la publicación de la NIST SP800-53 explica el proceso según la NIST y puede usarse como la base para el desarrollo de políticas organizacionales. SA-1 busca desarrollar, documentar y diseminar el propósito, el alcance, los roles, las responsabilidades, el compromiso administrativo, la coordinación entre organizaciones internas y externas y el cumplimiento de los procedimientos que faciliten la implementación de políticas de los controles seleccionados en los sistemas y servicios. Además, este mismo control debe ayudar a la organización a definir la frecuencia de la revisión y la actualización de los procedimientos de definición de políticas. El control también aclara que los procedimientos y políticas deben reflejar cualquier ley, orden ejecutiva, directivas, regulación, políticas, estándares y guías internacionales y nacionales.

SA-1 debe ayudar a la organización a definir el procedimiento que seguirá la organización para la definición de políticas según los controles seleccionados en el punto de selección de controles. Las políticas deben definirse con base en los resultados de la evaluación de riesgos y los diagramas de flujos y toma en cuenta los controles seleccionados y las capacidades técnicas o tecnológicas de los controles y el personal.

Algunos de los controles que se identifican en la sección de conclusión de los resultados del Capítulo IV pueden apoyar en la definición de políticas, la documentación y su publicación. La organización debe seguir las políticas definidas por los estándares o regulaciones a las que se encuentre sujeta.

5.3. Fase 3: Despliegue

5.3.1. Introducción. En la Fase 3 o de despliegue también se utilizan recursos organizacionales especializados y, en algunas ocasiones, puede requerir de capacitaciones adicionales, porque en esta fase la organización pondrá en práctica los controles y las políticas seleccionadas de la Fase 2.

5.3.2. Propósito. El propósito de esta fase es definir la estrategia de implementación e identificar a los responsables de la configuración y de la implementación, de manera que trabajen con los procesos, activos y recursos que se identifican o que son afectados. Los responsables trabajan en conjunto para materializar los controles seleccionados e implementar las políticas definidas y así comprobar, finalmente, su funcionamiento y este no interrumpa los procesos de negocio.

5.3.3. Consideraciones. Se debe considerar uno de los controles destacados en el Capítulo IV, las políticas de control de cambios. Para control o gestión de cambios se puede mencionar a ITIL y sus mejores prácticas, que es tal vez uno de los estándares que más se utilizan en el ámbito mundial. Antes de comenzar la Fase 3, la organización puede considerar la implementación de una política de gestión de cambios o puede revisar/actualizar la que utilicen actualmente.

ITIL (Heflo, 2021) tiene de objetivo de utilizar los métodos y procedimiento más seguros y eficientes para las alteraciones tecnológicas en una organización, con el fin de minimizar el impacto y los accidentes. Es posible dividir el proceso de gestión de cambios en 6 componentes o actores:

1. El iniciador del cambio: cualquier persona puede iniciar un proceso de cambio, lo ideal es que sea una consciente de lo que se debe hacer, cómo y por qué.
2. Administrador de cambios: es el encargado de gestionar el ciclo de vida de todos los cambios que suceden en la organización. Debe asegurar que los cambios que suceden son positivos y con una interrupción mínima.

3. Junta Asesora de Cambios: es un grupo de empleados que apoya al administrador de cambios en el análisis y la toma de decisiones. Este grupo debe estar formado por miembros de las diversas áreas afectadas.
4. Junta Asesora de Cambios de Emergencia: esta junta decide sobre los cambios de emergencia que tengan un gran impacto a los servicios de TI.
5. Constructor del cambio: es la persona que documenta el cambio, lo planifica y, en muchas ocasiones, también lo ejecuta.
6. Implantador: es la persona que implementa el cambio, si no fuera el constructor puede ser un equipo de personas.

Para implementar la Gestión de Cambios de ITIL se puede revisar la documentación de este ente en profundidad y, con base en ITIL, la organización debe generar una estructura similar a la expuesta y así puede asegurar que los cambios se realizan de una manera en la que los riesgos o interrupciones sean mínimas y se documenten.

Como última consideración, la organización entre sus capacidades puede desarrollar un ambiente de pruebas. En el marco teórico se mencionó el uso de ambientes de pruebas o del ambiente de producción para estudiar el comportamiento antes de aplicar los controles y sus políticas y así conocer el estado actual de la organización. Se le recomienda al lector revisar los escenarios documentado en la sección del Marco teórico titulada Migración a un modelo de cero confianza.

Adicionalmente, las siguientes son solo guías y no cubren extensamente los pasos de despliegue y evaluación. Cada organización debe generar su plan con el arquitecto con base en las soluciones y controles seleccionados para cada proceso.

5.3.4. Etapas. A continuación, se definen las etapas.

5.3.4.1. Despliegue. Seguidamente, se define el despliegue.

5.3.4.1.1. Introducción. En el primer paso la organización empieza el despliegue de las soluciones seleccionadas y se aplican las políticas o configuración identificadas.

5.3.4.1.2. Propósito. Según RMF (NIST, 2021) el paso de despliegue debe

implementar los controles de los planes de seguridad y privacidad para los sistemas de la organización y tiene dos resultados:

- Controles especificados e implementados según los planes de seguridad y privacidad.
- Actualización de planes de seguridad y privacidad con los controles implementados.

5.3.4.1.3. Procedimiento. En la etapa de despliegue se pueden repasar los siguientes puntos:

1. Implementación de principios.
2. Cambio de procesos.
3. Soluciones tecnológicas.

Como se ha observado, durante las fases anteriores se implementaron los principios de cero confianza al hacerlos parte de la evaluación de riesgos, selección de controles y desarrollo de políticas. También se cambiaron los procesos como establece la Fase 2, cuando se seleccionan los controles y se desarrollan las políticas.

El siguiente paso es la implementación de soluciones tecnológicas y durante este proceso se debe pensar en el punto 1 y 2, los principios del modelo de cero confianza y el cambio de procesos que se basan en los principios es crítico para una implementación exitosa.

Repasando los principios:

- Verificar explícitamente: autenticar y autorizar siempre en función de todos los puntos de datos disponibles.
- Utilizar la política de menos privilegios (Least Privileged): limitar el acceso de usuario con políticas de tiempo y acceso necesario para llevar a cabo sus tareas, utilizar políticas adaptables al riesgo y políticas de protección de datos.
- Asumir una ruptura de seguridad: siempre trata de minimizar el radio de daño y el acceso por medio de la segmentación. Verificar la encriptación de punto a

punto, utilizar herramientas de análisis para ver las transacciones, impulsar la detección de amenazas y mejorar los controles de defensa.

5.3.4.1.3.1. Consideraciones. Como se documenta en el Marco teórico en la sección para introducir cero confianza a un modelo de red basado en perímetro, se deben seguir los puntos a continuación al seleccionar las soluciones e implementarlas:

1. Identificar soluciones candidatas.
 - a. El arquitecto de la organización o responsable debe desarrollar una lista de posibles soluciones según los procesos y controles seleccionados.
2. Selección de solución.
 - a. La selección de soluciones.
 - i. No será sencillo y la solución no siempre será la mejor del mercado o la que funcionó en otras organizaciones, cada empresa tiene sus procesos y objetivos de negocio y cada solución puede dar resultados diferentes a cada empresa.
 - b. Preguntas que debe hacer el equipo responsable de seleccionar las soluciones según lo documentado en la publicación de la NIST
 - i. ¿La solución requiere que componentes se instalen en los activos empresariales?
 1. Tenemos que ser conscientes de las implicaciones que tiene la instalación de algún cliente en máquinas que no se encuentren en la red de la organización y como la organización planea realizarlo.
 - ii. ¿La solución funciona donde los procesos empresariales existen completamente en el centro de datos local?
 1. Esta pregunta es muy importante porque la investigación actual se enfoca en el teletrabajo, por lo que es posible evaluar que funcione en ambos ambientes si la organización así lo desea.
 - iii. ¿La solución provee de medios para analizar los registros?

1. Como se ha observado durante toda la investigación, debe existir trazabilidad y la generación de registros y la compatibilidad con los sistemas de gestión de registros es crítico.
- iv. ¿La solución provee soporte a diferentes aplicaciones, servicios y protocolos?
 1. Es necesario ser conscientes de los problemas o facilidades de compatibilidad con el ambiente para no agregar complejidad a la implementación o al ambiente.
 - v. ¿La solución requiere cambios en el comportamiento del sujeto?
 1. Debemos entender como las nuevas soluciones cambian el flujo de datos o los procesos internos, capacitar a los empleados y evitar la resistencia al cambio por medio de la preparación correcta.
- c. Despliegue inicial.
 - i. Una vez que el flujo de trabajo candidato y la solución han sido elegidos empezará el despliegue inicial.
 - ii. Los administradores deben implementar las políticas desarrolladas en las soluciones seleccionadas.
 - iii. Así empezará el paso de evaluación.

5.3.4.1.3.2. *Identidad.* Según las guías de implementación de la NIST, cada organización debe definir qué recursos debe asegurar y el orden que se quiere y después de revisar la documentación de muchos otros fabricantes de soluciones no definen ningún orden de implementación específico y se enfoca en los procesos o las superficies que se desean proteger.

Es posible destacar dos de los principios de cero confianza que tienen una estrecha relación con la identidad, la autenticación y autorización. Además, se puede tomar en cuenta que durante el análisis documental se encontraron más controles para identidad que en

ninguna de las otras áreas estudiadas. Por esto, el investigador recomienda empezar la implementación de controles de identidad al abordar cada proceso.

En la investigación documental se encuentra la opinión de Jakkal (2020), vicepresidente corporativo de seguridad, cumplimiento e identidad de Microsoft, que comentó en una publicación de seguridad que la identidad debe ser el punto de inicio de cualquier implementación basada en un modelo de cero confianza. Él indica que sin importar la naturaleza de la organización y sus objetivos específicos, uno de sus pasos principales y tal vez su paso más fundamental en la implementación de cero confianza es una base sólida de identidad en la nube. La organización debe tener una autenticación fuerte, debe proteger las credenciales de los usuarios y debe proteger los dispositivos que se encuentran fuera de la organización.

Después de revisar la documentación de los distintos fabricantes de soluciones, el único que provee de una guía para la implementación es Microsoft (2021).

Plan base de implementación de soluciones de identidad:

- I. Etapa I:
 - a. Federación de sistemas de identidades en la nube y locales.
 - b. Configuración de políticas de acceso condicional.
 - c. El uso de las herramientas de análisis (disponibles en algunas de las soluciones de mercado).
- II. Etapa II:
 - a. Gestión de identidades y privilegios por medio de un gobierno de identidad.
 - b. Análisis en tiempo real de usuarios, dispositivos, ubicación y comportamientos para evaluar la postura de riesgo.
 - c. Integrar soluciones de seguridad para alertar de amenazas.

5.3.4.1.3.3. *Administración de dispositivos.* Según lo estudiado en la investigación el siguiente puede ser la administración de dispositivos, ya que esto puede facilitar la toma de decisiones y soportar muchos de los procesos de mantenimiento del modelo de cero

confianza. Además, soporta el aseguramiento de dispositivos mencionado en el punto anterior.

Ningún fabricante tiene una guía para la implementación de las soluciones ofrecidas por cada uno, pero se utiliza como base el dado por Microsoft (s. f.), ya que sus objetivos son aplicables a las distintas soluciones en el mercado.

Requerimientos obligatorios:

- Los dispositivos deben estar unidos a un dominio.
- Los dispositivos deben administrarse por medio de políticas de grupo o alguna solución de administración de dispositivos.
- Los dispositivos deben tener acceso a la red corporativa, ya sea físicamente o por medio de un VPN. Es de vital importancia desplegar políticas y administrar los dispositivos.

Plan base de implementación de soluciones de administración de dispositivos:

I. Etapa I:

1. Registrar los dispositivos con los proveedores de identidad de la nube, esto permite tener visibilidad de los usuarios accediendo a los dispositivos y de los dispositivos accediendo los recursos empresariales.
2. Proveer accesos solo a los dispositivos gestionados por proveedores de identidad de la nube y que cumplan con las políticas definidas por estos. La organización debe establecer las reglas de cumplimiento según las políticas y controles organizacionales y asegurarse de que los dispositivos cumplan un mínimo de seguridad antes de darles acceso. Es importante definir reglas de remediación para aquellos dispositivos que no cumplan con las reglas definidas.
3. Implementar una solución DLP o definición de políticas para los DLP en los dispositivos organizacionales o BYOD. La organización debe controlar lo que

el usuario puede hacer con los datos organización una vez que ha accedido a ellos.

II. Etapa II:

1. Implementar soluciones de agentes de antivirus y *firewall*, es importante que la organización pueda monitorear y gestionar la seguridad de los dispositivos. La solución seleccionada debe enviar los registros a una solución SIEM o similar que utilice la organización.
2. Control de acceso restringido a los dispositivos corporativos y BYOD, se pueden utilizar integraciones a soluciones de antivirus que generen información de los dispositivos y que permitan la implementación de políticas de cumplimiento y definir las reglas de acceso condicional con los atributos retornados por estas soluciones. La posición de riesgos del dispositivo influye en si el usuario o el dispositivo puede acceder a los recursos de la organización.

5.3.4.1.3.4. Almacenamiento de datos. Por último, se tiene el almacenamiento de datos, según lo investigado en una implementación pura de cero confianza todas las otras áreas deben soportar la seguridad de los datos. En esta investigación se ha limitado la seguridad de datos al almacenamiento de datos, ya que no se toma en cuenta la parte de redes de la organización, por lo que la parte cubierta de datos es menor a las otras áreas seleccionadas.

Se consultaron los fabricantes de soluciones y solo se encontró la guía de implementación de Microsoft (2021), la cual se usa como base para construir una guía. Normalmente, las organizaciones delimitan el control a sus datos por el acceso a su perímetro, muchas no conocen la sensibilidad de los datos. En algunos casos pueden utilizar etiquetas manuales para etiquetar documentos sensibles.

Requerimientos:

- Definir la taxonomía de las etiquetas de la organización.

- Definir las características de protección que están al alcance de su implementación.
- Mapear las características en el alcance de su proyecto y su línea de tiempo del proyecto de implementación.
- Revisar periódicamente las nuevas características y evaluar si se alinean con los requerimientos de su organización.

Para la implementación de soluciones de protección de datos almacenados es posible usar la siguiente guía:

I. Etapa I:

- a. Las decisiones de accesos son gobernadas por encriptación, este punto busca encriptar todo dato que sea sensible según las etiquetas lo definan. La organización debe configurar cuáles de las etiquetas definidas encriptaran los datos.
- b. Clasificación y etiquetado automático de datos.

II. Etapa II:

- a. Mejorar la clasificación de datos con modelos de ML.
- b. Utilizar una solución CASB para la toma de decisiones.
- c. Utilizar DLP para evitar filtración de información por medio de políticas basadas en la sensibilidad de las etiquetas.

Cabe mencionar que la encriptación de los dispositivos no se menciona en este apartado, solo la encriptación de los datos. Este control puede definirse con una solución de administración del dispositivo que despliegue políticas o instale clientes que realicen la encriptación del disco duro.

5.3.4.2. Evaluación. A continuación, se define la evaluación.

5.3.4.2.1. Introducción. En este último paso de la Fase 3 se revisa que las soluciones implementadas y las políticas de seguridad y privacidad definidas funcionan como se espera

y se ha documentado. La organización tiene la oportunidad de hacer cambios y mejorar el funcionamiento. Si se hace en un ambiente de pruebas se puede utilizar para refinar la configuración, pero esta etapa es igual de necesaria una vez que se mueva la solución a producción, ya que el comportamiento de los sujetos y las cargas pueden cambiar.

5.3.4.2.2. Propósito. Según RMF (NIST, 2021) el propósito del paso de evaluación es determinar que los controles se implementaron correctamente y operan como se deseaba. Se deben revisar resultados de los controles y verificar que son los esperados y que cumplen con el propósito y con los requerimientos de seguridad y privacidad de la organización. Entre sus resultados están:

- Selección de evaluador/equipo de evaluación.
- Desarrollo de los planes de evaluación de seguridad y privacidad.
- Aprobación y revisión de los planes.
- Evaluaciones controladas según los planes definidos.
- Desarrollo de reportes de evaluación.
- Remediación de controles deficientes.
- Actualización de planes de seguridad y privacidad con base en los cambios hechos en control implementados según los resultados o las remediaciones.
- Desarrollo de planes de acción y objetivos.

5.3.4.2.3. Procedimiento. Como se documenta en el marco teórico, en la sección para introducir cero confianza a un modelo de red basado en perímetro, la organización puede requerir de observación y monitoreo. En algunos casos puede necesitar de un alto monitoreo, la menos en las primeras semanas que son las más críticas y observar que los procesos de negocio no se vean entorpecidos por los controles o asegurar que estos funcionan como se esperaba y asegurar los recursos de la organización. Este paso debe durar lo suficiente para que la organización pueda asegurarse de que las políticas son efectivas y permiten que los procesos afectados funcionen como se espera. El proceso de monitoreo y observación de *log* y comportamiento de red debe darle a la organización las bases de los activos y recursos con

sus solicitudes, comportamientos y patrones de comunicación, con lo cual la organización puede generar perfiles de comportamiento.

Algunas estrategias de despliegue incluyen el monitoreo en el primer paso, como se había anotado, la organización puede desplegar algunos componentes sin configuraciones endurecidas, lo que posibilita la mayoría de las solicitudes y así observar y reportar el comportamiento antes de configurar las soluciones seleccionadas. Esto le da a organización el entendimiento de lo que sucede en la red diariamente y le permite registrar las conexiones y transacciones esperadas. Toda esa información puede utilizarla para la actualización de políticas y configuración de las soluciones seleccionadas. Hacer esto puede minimizar el tiempo de evaluación y monitoreo después de la implementación.

Para llevar a cabo la evaluación del despliegue la organización debe:

1. Selección de evaluador:
 - 1.1. La organización debe seleccionar a un equipo de evaluación, formado por miembros de los equipos afectados y el equipo de TI, que permita actualizar la configuración o tener la visibilidad necesaria.
2. Desarrollo de los planes de evaluación de seguridad y privacidad.
 - 2.1. La organización debe comunicar al equipo encargado de la evaluación la estrategia para seguir y la información que se espera obtener.
 - 2.1.1. Los integrantes del equipo que sean responsables de probar el proceso deben asegurarse de que funciona y cumple las necesidades del negocio.
 - 2.1.2. Los integrantes de TI o involucrados en la implementación, deben observar que la solución implementada se comporta como se espera.
 - 2.1.3. Los integrantes de TI deben asegurarse de que el tráfico de red y los registros se comportan como se espera.
3. Aprobación y revisión de los planes.
 - 3.1. Una vez los planes están definidos y las responsabilidades y actividades están fijadas, deben ser aprobados por los responsables.

4. Evaluaciones controladas según los planes definidos.
 - 4.1. Las evaluaciones deben ser controladas y el equipo debe trabajar en conjunto para asegurar que los resultados son los deseados. Esto puede ser más sencillo en un ambiente de prueba.
5. Desarrollo de reportes de evaluación.
 - 5.1. Una vez que la evaluación ha sido terminada se deben documentar los resultados y adjuntar cualquier anomalía o cualquier problema detectado durante la evaluación.
6. Remediación de controles deficientes.
 - 6.1. Si se han encontrado problemas de configuración o funcionamiento, la organización debe gestionar el cambio según los procesos de la organización.
7. Actualización de planes de seguridad y privacidad con base en los cambios hechos en control implementados según los resultados o las remediaciones.
 - 7.1. Si se han realizado cambios a la configuración de las soluciones implementadas y estos afectan los planes o políticas de seguridad y privacidad deben ser documentados.
8. Desarrollo de planes de acción y objetivos.
 - 8.1. Finalmente, se deben desarrollar planes de acción para la futura operación y monitoreo, que tengan definidos los objetivos de los equipos involucrados.

5.4. Fase 4: Operación y monitoreo

5.4.1. Introducción. Esta última fase es la que confirma que el análisis de riesgos, la selección de controles y soluciones implementadas funcionan como era esperado y que trabajan según las necesidades del negocio. Los empleados de TI ahora se enfocan en que funcionen según lo esperado y continuarán monitoreando las soluciones según se ha documentado en cada control durante las fases anteriores. La organización puede enfrentar cualquier cambio necesario por medio de la gestión de control de cambios y debe seguir los planes documentados para la reevaluación de cada control.

5.4.2. Propósitos. Según la NIST (2011) en su publicación SP800-128, enfocada en la configuración de sistemas de información administrados, el propósito de la etapa de operación y monitoreo (también referido como mantenimiento en algunas publicaciones de la NIST) es confirmar que la evaluación de riesgos estaba en lo correcto y debe confirmar que no hay vulnerabilidades o impactos adicionales en los controles de seguridad implementados, que no se identificaron durante las pruebas o en el ambiente de prueba.

5.4.3. Etapas. A continuación, se definen las etapas.

5.4.3.1. Operación. Seguidamente, se define la operación.

5.4.3.1.1. Introducción. Es cuando la organización aprueba que la implementación y la aplicación de los controles que se identifican durante la evaluación de riesgos es correcta y el sistema funciona como se esperaba.

5.4.3.1.2. Propósito. Según la NIST (2021) el paso de operación o de autorización consiste en dar el visto bueno por el responsable (puede ser una persona de la Junta Directiva) de determinar con los reportes y la documentación generada en los pasos anteriores que el control implementado permite una operación aceptable. Este paso debe generar:

- Paquete de autorización:
 - Resumen ejecutivo.
 - Planes de seguridad y privacidad.
 - Reportes de las evaluaciones.
 - Planes de acción.
 - Objetivos e hitos del proyecto.
- Estado de los riesgos.
- Respuestas a los riesgos que se identifican.
- Autorización de los controles que se implementan.

5.4.3.1.3. Procedimiento. El proceso de autorización o aprobación de la operación de las soluciones que se implementan lo cubre la NIST en la publicación 800-37 y puede usarse

como referencia. En este paso, como se detalló en el propósito, los ejecutivos y los responsables deben dar el visto bueno del proyecto y generar la documentación apropiada para apoyar la decisión, es fundamental que todas las correcciones mayores se realicen en la Fase 3.

Es importante que los resultados de las evaluaciones de riesgo apoyen la decisión de los responsables, en algunas organizaciones la evaluación de riesgos sucede después de cambios grandes en un proceso. Es importante que la organización haga una nueva evaluación de riesgos en la Fase 3 para que apoye la decisión de los ejecutivos, si los riesgos han incrementado o no están en el nivel deseado la organización puede no autorizar el despliegue y devolver el proyecto a la Fase 3 (NIST, 2012).

Algunas organizaciones crean una CCB (Configuration Control Board) que está conformado por personal calificado responsable de regular y aprobar cambios en los componentes de TI y su documentación durante su ciclo de vida en la organización (NIST, 2021). Esta puede usarse para aprobar el funcionamiento de la solución, en algunos casos la CCB puede involucrarse durante la aprobación de cambios (NIST, 2012).

5.4.3.2. Monitoreo. Introducción. Después de aprobar la implementación, la organización debe ser capaz de conocer la eficacia de los controles que se implementan y del cumplimiento con la legislación, directrices, políticas y estándares a los que la organización esté sujeta. Este paso debe dar visibilidad sobre los cambios que pueden afectar la evaluación de riesgos actual y soportar la ejecución de una nueva evaluación cuando sea necesario durante su ciclo de vida. Esta etapa debe ayudar a la organización a detectar fallas o áreas de mejora (NIST).

5.4.3.2.2. Propósito. Según NIST (2021), el propósito del paso de monitoreo es mantener la consciencia continua de la postura de seguridad y privacidad de los sistemas de la organización y soportar las decisiones de la gestión de riesgos. Entregables de este paso:

- Definición de la estrategia de monitoreo continuo.
- Monitores de sistemas y ambientes según lo definido en la estrategia de monitoreo continuo.

- Evaluaciones continuas de la eficacia de los controles aplicados según lo estipule la estrategia de monitoreo continuo.
- Generar resultados de las actividades de seguimiento.
- Definición del proceso de reporte a gerencia de la postura de seguridad y privacidad.
- Autorizaciones en curso realizadas con los resultados de las actividades de monitoreo.

5.4.3.2.3. Consideraciones. Algunas organizaciones pueden contar con un SIEM o SOC en donde los registros y las herramientas de monitoreo y relacionamiento se centralizan y todas las tareas y operaciones relacionadas con el monitoreo continuo se llevan a cabo. Es de vital importancia integrar las soluciones seleccionadas con las soluciones actuales de SIEM cuando sea posible. Si una organización no puede adquirir una solución SIEM o contratar un SOC de terceros, puede buscar soluciones alternativas.

5.4.3.2.4. Procedimiento. La NIST expande el monitoreo continuo en su publicación SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST, 2011) donde define las necesidades de las organizaciones en cuanto a monitoreo continuo se refiere:

- Mantener consciencia de la situacional de todos los sistemas de la organización.
- Mantener un entendimiento de las amenazas y las actividades de las amenazas.
- Evaluar todos los controles de seguridad.
- Recolectar, correlacionar y analizar la información relacionada con la seguridad.
- Proporcionar comunicación accionable del estatus de seguridad de todas las áreas de la organización.
- Gestión activa del riesgo por medio de los responsables.

La publicación SP800-137 puede servir de guía para una organización que necesita definir las estrategias necesarias para lograr todos los objetivos de este paso por medio de la

implementación de un ISCM. Para el monitoreo muchas organizaciones recurren a herramientas automáticas o de ML que les permitan evaluar todos los datos de los que dispone la organización, en algunos casos estas herramientas pueden solucionar problemas de seguridad o ejecutar una acción que detenga el daño inmediato. El uso de herramientas automáticas puede dar visibilidad sobre las desviaciones de los controles o del comportamiento de las soluciones (NIST, 2012).

En la publicación de la NIST SP800-53 R4 (NIST), hay cuatro controles por considerar en lo referente a monitoreo:

1. CA-7 Continuous Monitoring.
 - a. Propósito: Desarrollar una estrategia de monitoreo continuo en el sistema e implementar monitoreo de la organización según su estrategia de monitoreo.
 - b. Este control incluye:
 - i. Establecer métricas de sistema que se deban monitorear.
 - ii. Establecer monitoreo y evaluación de la eficacia de los controles.
 - iii. Evaluaciones de control continuo según la estrategia de monitoreo continuo.
 - iv. Monitoreo continuo de sistemas y de la organización según las métricas acordadas por la estrategia de monitoreo continuo.
 - v. Correlación y análisis de la información generada por la evaluación de controles y el monitoreo.
 - vi. Definir las acciones de respuesta de los resultados generados por el análisis de la información de monitoreo y la evaluación de controles.
 - vii. Reportar el estatus de seguridad y privacidad de los sistemas de la organización.
2. PE-20 Asset Monitoring and Tracking.

- a. Propósito: es utilizar tecnologías que permitan localizar y monitorear la ubicación y movimiento de los activos de la organización.
 - b. Esta información le permite saber dónde se ubican sus empleados y conocer si están en una ubicación segura o esperada, según su perfil de uso.
3. SI-4 Information System Monitoring.
- a. Propósito: definir que se desea monitorear en un sistema o una organización.
 - b. Este control habla de los siguientes puntos:
 - i. Monitorear los sistemas para detectar:
 - 1. Ataques o indicadores de ataques potenciales según los objetivos de monitoreo.
 - 2. Conexiones no autorizadas a la red local, a sistemas o por medio de conexiones remotas.
 - ii. Identificar uso no autorizado de los sistemas.
 - iii. Utilizar las capacidades internas de monitoreo y desplegar dispositivos de monitoreo.
 - 1. Desplegar estratégicamente dispositivos que recolecten información esencial de la organización.
 - 2. Desplegar controles en partes específicas de los sistemas o de la red recolectar o tener visibilidad sobre transacciones de interés para la organización.
 - iv. Analizar eventos y anomalías detectadas.
 - v. Ajustar los niveles de monitoreo cuando haya un cambio en el riesgo de la organización así sea necesario.
 - vi. Obtener la opinión legal de los equipos responsable sobre las actividades de monitoreo.

- vii. Proveer información de monitoreo al personal definido por la estrategia de monitoreo continuo cuando sea necesario o como sea definido.

Capítulo VI. Conclusiones y recomendaciones

6.1. Expansión del modelo de cero confianza

La propuesta actual cubre solo tres áreas de la empresa y se limita al teletrabajo, incluso así, provee a la organización de un punto inicial para expandir el modelo de cero confianza con la implementación de los tres principios en su cultura organizacional y con cambios en los procesos organizacionales, los cuales pueden suceder de forma gradual. El último punto, que son las implementaciones, puede llevarse a cabo utilizando las cuatro fases expuestas, ya que se basan en los puntos expuestos por la NIST cuando la empresa desea migrar secciones de esta a un modelo de cero confianza.

La expansión del modelo de cero confianza se relaciona con la confianza de los administradores y de la organización. La NIST recomienda empezar con los procesos no críticos como prueba y atravesar las cuatro fases para ganar confianza sobre las soluciones que se implementan y las estrategias de monitoreo. Este ciclo de implementación debe aplicarse sobre cualquier proceso candidato y cada vez que se desee hacer un cambio o revisión de las soluciones que se implementan.

6.2. Realidades del mercado

Las medianas o pequeñas organizaciones no suelen invertir en seguridad de la información y muchas no tienen consciencia de los riesgos o amenazas a las que se encuentran expuestas. Algunas organizaciones no tienen consciencia de si han sido vulneradas y no poseen los mecanismos o controles necesarios para evitar los ataques o para detectarlos. El factor humano desempeña un papel importante en la seguridad los empleados, deben tener una cultura organizacional en donde la seguridad cumpla un papel importante, he ahí la importancia de los principios de cero confianza los cuales pueden aplicarse diariamente. Una vez que la consciencia se crea en una organización obtener el apoyo de la alta gerencia es más sencillo, una vez que la Gerencia entiende los retos y los riesgos que pueden afectar a la organización y de la importancia de proteger los activos dentro de ella.

Las medianas y pequeñas empresas no suelen estar sujetas a estándares como ISO o ITIL, por lo que muchas no tienen procesos internos de evaluación de riesgos o de gestión de

control de cambios. Seguir la propuesta de implementar estas herramientas en la organización puede ayudar a tener un mejor conocimiento de los riesgos y de lo que sucede en la organización. Adoptar estas buenas prácticas aumenta la madurez de la organización, no solo de seguridad, sino su madurez en general y la prepara para la adopción de estándares internacionales.

Las capacidades técnicas en grandes, medianas y pequeñas empresas puede ser un gran reto y tener más capital puede facilitar la obtención de los recursos necesarios, de capacitaciones o la subcontratación. Muchas de las soluciones del mercado tienen diferentes planes con diferentes capacidades, los cuales pueden no ofrecer las mismas opciones o controles, pero claramente pueden dejar a la organización en mejor nivel. Muchas de las soluciones en la nube también resultan sencillas de configurar y muchos proveedores ofrecen documentación para que el personal pueda aprender o configurar sobre las tecnologías ofrecidas.

El desconocimiento del modelo de cero confianza puede ser un gran reto y es que no solo las pocas habilidades técnicas pueden afectar el cambio y los resultados. Los especialistas de seguridad y los ingenieros de tecnologías de información creen que los controles de perímetro son efectivos y les dan confianza a los dispositivos dentro de la organización. El nuevo modelo de trabajo, donde los dispositivos son diversos y los dispositivos salen y entran de la organización, los controles de perímetro y la confianza heredada del perímetro son obsoletos. No es solo definir controles con la mentalidad de cero confianza, también es planear y pensar con la mentalidad de cero confianza, es cambiar la cultura organizacional y educar a todos los empleados.

6.3. Soluciones

Como se ha observado, no existe una sola solución y la ideal para una empresa o la mejor calificada en el mercado no es siempre la mejor solución para todas las empresas. Cuando se consultó a Machado (comunicación personal, 2021), este hizo la observación de que muchas soluciones tienen sus beneficios y que algunas empresas deben optar por soluciones de diferentes proveedores para lograr sus objetivos. Cabe destacar que muchas de las soluciones de cero confianza están enfocadas en la red en su mayoría.

Para el Q3 del 2020 Forrester evaluó los proveedores de soluciones de cero confianza lo cual puede usarse como base para explorar cada solución. Como se mencionó anteriormente, este cuadrante no debe ser determinístico.



Ilustración 33

Cuadrante de cero confianza Q3 2020, Forrester (2020)

Se exploran algunas de las opciones según CDW (2021) y según eSecurity Planet (Shread, 2021).

6.3.1. Cisco y Duo. Ambas compañías han desarrollado un marco de seguridad de cero confianza que se enfoca en tres componentes claves de la organización:

- La fuerza laboral.
- Las cargas de trabajo.
- El lugar de trabajo.

Ambas empresas buscan con este marco prevenir el acceso no autorizado y contener las brechas, proteger las aplicaciones y datos en escala y con más visibilidad sobre los dispositivos que intentan acceder la red de la organización.

Referencias.

- https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/cisco/zero-trust-going-beyond-the-perimeter.pdf?cm_ven=acquirgy&cm_cat=bing&cm_pla=S3+Zero+Trust&cm_ite=Zero+Trust+General+B&s_kwcid=AL!4223!10!73461369100015!73461298719791&ef_id=9812241faf6f13f1022744d8252f54e7:G:s&mclid=9812241faf6f13f1022744d8252f54e7
- https://www.cisco.com/c/dam/global/en_ca/assets/pdfs/zero-trust-cisco-connect-vancouver-2020.pdf.
- <https://www.cisco.com/c/en/us/products/security/zero-trust.html>.

6.3.2. Palo Alto Networks. El enfoque de la arquitectura ofrecida por Palo Alto es una con un balance de la integridad y de los usuarios, dispositivos y servidores, junto con controles dinámicos para las aplicaciones locales o en la nube. Esta cuenta con una metodología de cinco pasos:

1. Definir la superficie de ataque.
2. Mapear los flujos de las transacciones.
3. Construir una arquitectura basada en cero confianza.
4. Crear una política de cero confianza.
5. Monitorear y mantener.

Referencias.

- https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/palo-alto-networks/zero-trust-deployment-at-palo-alto-networks.pdf?cm_ven=acquirgy&cm_cat=bing&cm_pla=S3+Zero+Trust&cm_i

te=Zero+Trust+General+B&s_kwcid=AL!4223!10!73461369100015!73461298719791&ef_id=9812241faf6f13f1022744d8252f54e7:G:s&msslkid=9812241faf6f13f1022744d8252f54e7

- https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/palo-alto-networks/zero-trust-dictionary.pdf?cm_ven=acquirgy&cm_cat=bing&cm_pla=S3+Zero+Trust&cm_ite=Zero+Trust+General+B&s_kwcid=AL!4223!10!73461369100015!73461298719791&ef_id=9812241faf6f13f1022744d8252f54e7:G:s&msslkid=9812241faf6f13f1022744d8252f54e7
- <https://www.paloaltonetworks.com/>

6.3.3. Okta. El modelo de Okta se enfoca en las tecnologías móviles, la nube y la seguridad basada en perímetro y las dificultades que enfrentan las organizaciones para proteger estos dos puntos. El modelo incluye características de cero confianza en identidad, mejores prácticas de seguridad, MFA y SSO.

Referencias.

- https://www.cdw.com/content/cdw/en/brand/okta.html?cm_ven=acquirgy&cm_cat=bing&cm_pla=S3+Zero+Trust&cm_ite=Zero+Trust+General+B&s_kwcid=AL!4223!10!73461369100015!73461298719791&ef_id=9812241faf6f13f1022744d8252f54e7:G:s&msslkid=9812241faf6f13f1022744d8252f54e7
- <https://www.okta.com/>

6.3.4. Microsoft. El modelo propuesto por Microsoft es uno donde no se asume que todo detrás del perímetro está seguro. Siempre asume que hay una brecha de seguridad y que se deben verificar todas las solicitudes, sin importar de donde vengan. En el Apéndice 1 se puede observar la arquitectura de Microsoft.

Referencias:

- https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/microsoft/microsoft-zero-trust-business-plan-ebook.pdf?cm_ven=acquirgy&cm_cat=bing&cm_pla=S3+Zero+Trust&cm_ite=

Zero+Trust+General+B&s_kwcid=AL!4223!10!73461369100015!7346129871
9791&ef_id=9812241faf6f13f1022744d8252f54e7:G:s&m sclkid=9812241faf6f
13f1022744d8252f54e7

- <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWlrfk>.
- <https://www.microsoft.com/security/blog/2020/09/29/microsoft-advanced-compliance-solutions-zero-trust-architecture/>
- <https://www.microsoft.com/security/blog/2021/03/02/4-ways-microsoft-is-delivering-security-for-all-in-a-zero-trust-world/>
- Material de referencia arquitectónica:
<https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fraw.githubusercontent.com%2FMicrosoftDocs%2Fsecurity%2Fmain%2FDownloads%2Fmicrosoft-cybersecurity-reference-architectures.pptx&wdOrigin=BROWSELINK>
- Diagrama de AAD de Microsoft en el Apéndice: “1. Azure Active Directory, Zero Trust Access Control”.
- Documentación de integraciones de identidad: <https://docs.microsoft.com/en-us/security/zero-trust/integrate/identity>.
- Documentación de integraciones de administración de dispositivos: <https://docs.microsoft.com/en-us/security/zero-trust/integrate/endpoints>.
- Etiquetas de sensibilidad: <https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide&preserve-view=true>.
- MIP y cumplimiento: <https://microsoft.github.io/ComplianceCxE/dag/>
- Microsoft Trust Center: clasificación de datos y taxonomía de etiquetas de sensibilidad: <https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-classification-and-labels>.

- Documentación de integración de datos: <https://docs.microsoft.com/en-us/security/zero-trust/integrate/data>.
- Documentación de integración y estrategias de cero confianza: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJD7>

6.3.5. Twingate. Ofrece una solución de VPN basada en cero confianza no se detallan más, ya que la solución es limitada y no aplica a las áreas que se seleccionaron.

Referencias:

- https://www.twingate.com/zero-trust/?utm_source=esecurityplanet&utm_medium=referral&utm_campaign=zt2&utm_content=top-cybersecurity.

6.3.6. Illumio. Es una plataforma de manejo de cargas de trabajo y seguridad de dispositivos que integra la microsegmentación y el *whitelisting*. Ofrece gestión de vulnerabilidades, microsegmentación, visibilidad de la red y encriptación. Es una solución que ofrece características de automatización y de gestión.

Referencias:

- <https://www.illumio.com/>

6.3.7. Akamai. Ha desarrollado una plataforma de seguridad basada en datos y entrega de contenido con un enfoque de cero confianza. Su plataforma incluye identidad, acceso de aplicaciones, SSO, MFA, protección contra amenazas y DDoS.

Referencias:

- <https://www.akamai.com/es>.

6.3.8. Unisys. Unisys Stealth es un modelo de seguridad que se basa en cero confianza que se basa en una metodología de cinco pasos, con una postura flexible en la que se pueden usar partes de esta solución.

Referencias:

- <https://www.unisys.com/glossary/zero-trust/>

6.3.9. Sysmantec. Ofrece su solución EndPoint Security como un agente de seguridad de múltiples plataformas y ubicaciones. Su solución utiliza inteligencia artificial y ML para relacionar y contextualizar amenazas a los datos. Además, ofrece gran variedad de integraciones con SIEM y SOC.

Referencias:

- <https://www.broadcom.com/products/cyber-security>.

6.3.10. AppGate. Ofrece una solución de controles de acceso y seguridad de red que se enfoca en cero confianza.

Referencias:

- <https://www.appgate.com/>

6.4. Madurez organizacional

Algunas organizaciones tienen una mayor curva de implementación y aprendizaje del modelo de cero confianza que otras, se puede afirmar que esto se debe a la madurez de cada una de las organizaciones. Es posible que las organizaciones costarricenses no hayan desplegado sus controles de seguridad actuales basadas en un modelo de cero confianza y cómo los haya implementado puede afectar la madurez de seguridad y del modelo de cero confianza. El nivel de madurez puede desempeñar un papel muy importante para la implementación y la adopción de un nuevo modelo de seguridad.

Anteriormente, estudiamos como el DoD establecía una tabla rápida para la evaluación de la madurez del modelo de cero confianza en base de los controles de seguridad que se implementan, es posible verlo en el Capítulo II, bajo el apartado Department of Defense (DoD) y el título Modelo de madurez. A continuación, una adaptación a las áreas que se seleccionaron:



Ilustración 34

Cuadro que se basa en el modelo de madurez del DoD

Según el DoD, la fase de preparación para el modelo de cero confianza se divide en las primeras 2 fases en el Cuadro 27, descubrir y evaluación. Ambas se cubren parcialmente en la Fase 1 de la propuesta. En la fase de descubrimiento no se menciona nada de registro de tráfico de red, porque el trabajo no cubrió nada de controles de red. En la fase de evaluación no se cubrió el descubrimiento del estado de cumplimiento, aunque se trata de inventariar los dispositivos, pero en la propuesta se debe suponer el peor de los casos donde no es posible saber el estado del cumplimiento de los dispositivos.

La propuesta debe ser capaz de ayudar a las organizaciones alcanzar la madurez inicial del modelo de madurez, segmentación de la red tiene un asterisco porque esto no se cubrió. La segmentación de la red es una práctica de seguridad común y puede llevarse a cabo, de ser necesario, para la implementación o las necesidades de la organización.

El nivel intermedio debe ser apoyado por la propuesta, muchos de los controles en la lista se mencionaron durante la investigación. Llegar este nivel de madurez puede requerir varias iteraciones de la propuesta con diferentes procesos candidatos. La microsegmentación puede evaluarse, pero no se cubrió en esta investigación. El uso de IA y ML es caro y

complejo, algunas soluciones ofrecen estos servicios y, aunque la NIST los recomienda para tener una respuesta más rápida, no se cubrieron extensamente por su complejidad y que puede no ser apto para cualquier organización. El último nivel es el nivel avanzado, este cubre puntos muy similares al intermedio y la propuesta y los temas investigados deben soportar este nivel de madurez.

6.5. Arquitecturas basada en el modelo de cero confianza



Ilustración 35

Arquitectura basada en el modelo de cero confianza

Según lo estudiado en la investigación, una arquitectura basada en cero confianza pura incluiría todas las áreas de información de las organizaciones. La propuesta actual solo cubre identidad, dispositivos y, parcialmente, datos. Para datos se establecen las bases para asegurar los datos de la organización. Fuera de esta propuesta se dejaron las aplicaciones como los API o aplicaciones de servicio y los otros recursos organizacionales como la infraestructura y las redes.

Como es posible observar en la Ilustración 35, todos los componentes de la organización están dirigidos por la política de seguridad, la cual se debe alinear con las políticas organizacionales, por eso, es óptimo definir y depurar estas políticas. Las áreas no cubiertas deben estar regidas por controles específicos que les den protección contra amenazas.

6.6. Factibilidad en Costa Rica

Como se ha detallado en la investigación, seguir el modelo de cero confianza puede ser un reto para el personal de la organización y puede requerir una inversión significativa, pero no es el caso de todas las soluciones. Cada organización debe definir los controles que seleccionarán para cada proceso organizacional, el modelo de cero confianza para esta propuesta tiene una visión más flexible, por lo que las organizaciones que deseen aplicarla pueden seleccionar los controles que consideren o pueda adquirir. Desde el punto de vista del investigador la importancia de un modelo de cero confianza son sus principios y el cambio de mentalidad que exige, es crear esa cultura sobre los principios y educar a la organización. El cambio de los procesos se dará poco a poco con el cambio de cultura y estos apoyarán la inversión en controles de seguridad.

La inversión es un gran reto no solo en Costa Rica, sino también en países de Latinoamérica y el primer mundo, pero el cambio de la cultura organizacional puede ayudar a las organizaciones a entender por qué una organización debe invertir en seguridad y cómo seleccionar controles de seguridad que le sirvan a la organización a la larga y para esta investigación con un énfasis en el modelo de cero confianza. Finalmente, se puede destacar que hay soluciones para pequeñas empresas que encapsulan varias características de cero confianza, por ejemplo, M365 de Microsoft cuenta con características de cero confianza y los planes básicos empiezan desde los \$5 USD por usuario al mes, muchos de sus planes ofrecen planes base de AAD, etiquetado de datos y políticas de acceso.

Por otro lado, la administración de dispositivos es un poco más cara y compleja. VMware tiene Workspace ONE que puede administrar dispositivos de todo tipo, como móviles por medio de MDM y MAM, su costo puede ser conocido por medio de sus canales oficiales y de la evaluación realizada por VMware. Microsoft tiene Microsoft Endpoint

Manager y System Center Configuration Manager, ambos tienen MDM y MEM tiene MAM. La licencia de MEM se incluye con M365 al adquirir una licencia E3 o superior con un valor de \$32 USD por usuario al mes. Existen otras opciones para la administración de dispositivo, pero la complejidad agregada puede ser la mayor de las tres áreas cubiertas, ya que requieren mucho tiempo y conocimiento en diversas áreas para sacar el máximo provecho. En Costa Rica muchas academias de tecnología ofrecen cursos de actualización profesional de estas plataformas.

Capítulo VII. Reflexiones finales

7.1. Modelo de cero confianza

La opinión del autor de este TFG, después de explorar el modelo de cero confianza, es que este modelo incorpora tres ideas que son fundamentales para los profesionales de seguridad y, aunque la NIST expone más principios, los más básicos son:

- a) Verificar explícitamente.
- b) Utilizar la política de menos privilegios (Least Privileged).
- c) Asumir una ruptura de seguridad.

Los controles tradicionales crean áreas de confianza, donde los dispositivos heredan la confianza de estas zonas y crean puntos débiles. Los usuarios tienen acceso a los recursos con métodos de autenticación básicos como contraseñas no seguras y no existe una verificación explícita del usuario, no se incluye algo que sea o tenga, creando un riesgo en caso de que la contraseña haya sido vulnerada. Finalmente, muchos profesionales de seguridad creen que los controles o los dispositivos son seguros por su ubicación o sus usuarios y no piensan en los riesgos de ser vulnerados. Estos tres puntos pueden cambiar cómo se ve o se planea la seguridad de la organización.

Cero confianza no debe ser el único modelo dentro de una organización. Esta debe estudiar los requerimientos de negocio y su arquitectura actual y entender los beneficios que puede traer cero confianza vs otros modelos. Cero confianza es aplicable a todos los ámbitos de la organización, pero cada organización es un mundo y por su nivel de madurez, naturaleza o presupuesto puede que otro modelo dé mejores resultados.

Una organización puede utilizar un modelo híbrido. En el Marco teórico es posible ver la publicación de la NIST donde se estudian los distintos despliegues del modelo de cero confianza, vale la pena destacar el título Modelo híbrido de cero confianza y basada en perímetro que es la combinación del modelo tradicional y cero confianza. Finalmente, se puede mencionar que toda organización debe estar consciente de las buenas prácticas del

mercado y siempre evaluar su aplicabilidad para fortalecer la postura de seguridad general de la organización.

7.2. Adopción de cero confianza en el mundo

Existen muchos reportes acerca de la adopción de cero confianza se empieza con un reporte de Microsoft junto con Hypothesis de la adopción de modelo en Estados Unidos de América (Hypothesis, 2021). Es posible destacar las cuatro razones en el ámbito mundial por las que las organizaciones se han migrado a un modelo que se basa en cero confianza.

1. Trabajo híbrido (teletrabajo y Oficinas) y COVID-19, el trabajo híbrido se ha visto acelerado con la pandemia de COVID-19 en todo el mundo. Cerca del 81 % de las organizaciones en el ámbito mundial han tenido que adoptar este modelo, de las cuales solo 31 % cuenta con la tecnología que soporte su trabajo híbrido. El 94 % de las organizaciones que trabajan híbridamente tiene serias preocupaciones de seguridad.
2. El modelo de cero confianza es flexible, no precisa cambiar toda la organización de la noche a la mañana y los controles pueden implementarse en procesos o áreas específicas.
3. Cero confianza mejora la habilidad de responder a las amenazas, el 76 % de las organizaciones entrevistadas han empezado por diseñar o implementar soluciones basadas en cero confianza y muchas reconocen que todavía falta terminar muchas áreas de implementación. Incluso así, todas aseguraron que el modelo ha incrementado la agilidad y velocidad en la detección de amenazas por medio de los nuevos controles o de servicios de análisis y mayor visibilidad.
4. Cero confianza es uno de los modelos principales de seguridad, según el reporte muchos de los especialistas y organizaciones en este todavía se hacen muchas mejoras, lo que le permite ser un modelo clave de seguridad por más años.

Como se mencionó en el Capítulo I, en el reporte de Thales (2021) es posible observar que muchas de las organizaciones en Latinoamérica se han visto afectadas por el trabajo híbrido y la pandemia de COVID-19, pero la adopción del modelo ha sido más lenta, esto se

debe a la capacidad técnica, la inversión y el desconocimiento, como se detalló en las conclusiones. En el mismo reporte se indica que solo 28 % tiene políticas basadas en cero confianza en contraste con el 76 % en Estados Unidos de América, adicionalmente, el 71 % cree que cero confianza puede ayudar a desarrollar una estrategia de seguridad para los recursos en la nube. Es claro que cero confianza puede ser puesto en práctica empezando con sus principios, es crítico educar a la organización y crear una cultura enfocada en la seguridad y tener más consciencia de que la confianza en los usuarios, dispositivos y redes solo crea más riesgos.

Referencias bibliográficas

- Abarca, A. A. (2013). *Técnicas Cualitativas de Investigación*.
- Barrantes, R. (2015). *Investigación: un Camino al Conocimiento*. UNED.
- Bernal, C. (2006). *Metodología de la Investigación: Para administración, economía, humanidades y Ciencias Sociales*. Pearson.
- CDC. (s. f.). *HIPAA Privacy Rule*. <https://www.cdc.gov/phlp/publications/topic/hipaa.html>
- CDW. (021). *A Zero Trust Model for Your Network*.
https://www.cdw.com/content/cdw/en/brand/zero-trust.html?cm_ven=acquirgy&cm_cat=bing&cm_pla=S3+Zero+Trust&cm_ite=Zero+Trust+General+B.&s_kwcid=AL!4223!10!73461369100015!73461298719791&ef_id=9812241faf6f13f1022744d8252f54e7:G:s&mclkid=9812241faf6f13f102274
- CISCO. (2020). *Cisco Connect Vancouver 2020*.
https://www.cisco.com/c/dam/global/en_ca/assets/pdfs/zero-trust-cisco-connect-vancouver-2020.pdf
- Cloudflare. (s. f.). *Cloudflare. Zero Trust Security | What a Zero Trust Network?*
<https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/>
- Cloudflare. (s. f.). *What is a bot?* <https://www.cloudflare.com/learning/bots/what-is-a-bot/>
- CrowdStrike. (2020). *What is DEVSECOPS?* <https://www.crowdstrike.com/cybersecurity-101/what-is-devsecops/>
- Dawson, C. W. (2016). *Projects in Computing and Information Systems-A Student Guide*. Addison-Wesley.
- Day, R. (2005). *Cómo escribir y publicar trabajos científicos*. Organización Panamericana de la Salud.
- Defense Information Systems Agency (DISA) and National Security Agency (NSA).

- (2021). *Zero Trust Reference Architecture*. Department of Defense (DOD).
[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v1.1\(U\)_Mar21.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf)
- Desarrollo, B. I.-A. (2020). *Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe*.
<https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>
- Echavarría, S. R. (2002). *Investigación: Un camino al conocimiento y enfoque cualitativo y cuantitativo*.
- Forrester. (2020). *Taking Security Beyond The Perimeter*. Illumio.
<https://reprints2.forrester.com/#/assets/2/1513/RES157494/report>
- Franklin, J. M.; Howell, G.; Sritapan, V.; Souppaya, M. y Scarfone, K. (2020). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2-draft.pdf>
- Gartner. (2021). *Zero Trust Architecture and Solutions*. Gartner.
<https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf>
- Gillis, A. S. (2020). *Searchsecurity*.
<https://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act>
- Gobierno de Canarias. (2015). *La taxonomía de Bloom, una herramienta imprescindible para enseñar y aprender*. Gobierno de Canarias.
<https://www3.gobiernodecanarias.org/medusa/edublog/cprofestenerifesur/2015/12/03/la-taxonomia-de-bloom-una-herramienta-imprescindible-para-ensenar-y-aprender/>
- Google. (s. f.a). *BeyondCorp*. <https://cloud.google.com/beyondcorp>

- Google. (s. f.b). *Google definitions*. <https://www.google.com>
- Greene, J. (2020). *Telework Security Basics*. *NIST Blog*.
<https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics>
- Heflo. (2021). *Gestión de cambios ITIL: utilice las mejores prácticas*. *Heflo*.
<https://www.heflo.com/es/blog/itil/gestion-cambios-itil/>
- Hengl, T. (2012). *The Unofficial Guide for Authors. From Research Design to Publication*.
Lulu.
- Hypothesis. (2021). *Zero Trust Adoption Report*.
<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha>
- ISO/IEC. (2018). *ISO/IEC 27000*.
https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf
- ISOTools. (s. f.). *La norma ISO 27001: Aspectos clave de su diseño e implantación*.
ISOTools. <https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf>
- Jakkal, V. (2021). *4 ways Microsoft is delivering security for all in a Zero Trust world*.
Microsoft Security Blogs. <https://www.microsoft.com/security/blog/2021/03/02/4-ways-microsoft-is-delivering-security-for-all-in-a-zero-trust-world/>
- Kaspersky Team. (2021). <https://www.kaspersky.com/blog/pandemic-year-in-infosec/39123/>
- Lockhart, E. (2015). *Virtual Mobile Infrastructure (VMI)*.
<https://searchmobilecomputing.techtarget.com/definition/virtual-mobile-infrastructure-VMI>
- Machado, S. (2021). *Sales Technical Specialist*. (R. Villalobos, Entrevistador)
- Meredith, D. (2020). *7 security threats introduced by COVID-19 and the WFH rush*.
<https://www.pluralsight.com/blog/security-professional/-7-security-threats->

introduced-by-covid-19-and-the-wfh-rush

Microsoft. (2020a). Securing identity with Zero Trust. *Microsoft*.

<https://docs.microsoft.com/en-us/security/zero-trust/deploy/identity>

Microsoft. (2020b). *Microsoft Intune is an MDM and MAM provider for your devices*.

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>

Microsoft. (2020c). *What is Azure Active Directory?* [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is)

[us/azure/active-directory/fundamentals/active-directory-what-is](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is)

Microsoft. (2020d). *What is Azure Information Protection?* [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection)

[us/azure/information-protection/what-is-information-protection](https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection)

Microsoft. (2021e). Secure endpoints with Zero Trust. *Microsoft*.

<https://docs.microsoft.com/en-us/security/zero-trust/deploy/endpoints>

Microsoft. (2021f). *Secure data with Zero Trust*. [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/security/zero-trust/deploy/data)

[us/security/zero-trust/deploy/data](https://docs.microsoft.com/en-us/security/zero-trust/deploy/data)

Microsoft. (2021g). *Securing identity with Zero Trust*. [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/security/zero-trust/deploy/identity)

[us/security/zero-trust/deploy/identity](https://docs.microsoft.com/en-us/security/zero-trust/deploy/identity)

Microsoft. (s. f.a). *Secure endpoints with Zero Trust*. [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/security/zero-trust/deploy/endpoints)

[us/security/zero-trust/deploy/endpoints](https://docs.microsoft.com/en-us/security/zero-trust/deploy/endpoints)

Microsoft. (s. f.b). *Zero Trust Guidance Center*. [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/security/zero-trust/)

[us/security/zero-trust/](https://docs.microsoft.com/en-us/security/zero-trust/)

MTSS. (2021). *Lista de salarios mínimos 2021*. MTSS.go.cr.

https://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salarios/lista_salarios_2021.pdf

Murray, N. (2008). *Writing up your University Assignments and Research Projects-A practical handbook*. Open University Press.

- Nabe, C. (2020). *Impact of COVID-19 on Cybersecurity*.
<https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html>
- NIST Risk Management Framework RMF. (2021). *Risk Management Framework (RMF)-Monitor Step*. <https://csrc.nist.gov/Projects/risk-management/about-rmf/monitor-step>
- NIST. (2011). *Guide for Security-Focused Configuration Management of Information Systems*. NIST Pubs.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf>
- NIST. (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST Pubs.
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf>
- NIST. (2012). *Guide for Conducting Risk Assessments*.
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- NIST. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*.
NIST.<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- NIST. (2020). *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*.
NIST. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf>
- NIST. (2021). *Computer Security Resource Center. Risk Management Framework (RMF)-Select Step*. <https://csrc.nist.gov/Projects/risk-management/about-rmf/select-step>
- NIST. (2021a). *Risk Management Framework (RMF)-Authorize Step*. NIST.
<https://csrc.nist.gov/Projects/risk-management/about-rmf/authorize-step>
- NIST. (2021b). *Configuration control board (CCB)*. NIST.
https://csrc.nist.gov/glossary/term/configuration_control_board

- NIST. (2021c). *Risk Management Framework (RMF)-Implement Step*.
<https://csrc.nist.gov/Projects/risk-management/about-rmf/implement-step>
- NIST. (2021d). *Risk Management Framework (RMF)-Assess Step*.
<https://csrc.nist.gov/Projects/risk-management/about-rmf/assess-step>
- NIST. (2021e). *Computer Security Resource Center*. <https://csrc.nist.gov/projects/risk-management/about-rmf>
- NIST. (s. f.a). *Computer Security Resource Center*.
https://csrc.nist.gov/glossary/term/Identity_Credential_and_Access_Management
- NIST. (s. f.b). *NIST Special Publication 800-53 R4*. Security and Privacy Controls for Federal Information Systems and Organizations.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- OECD Legal. (1997). *Recommendation of the Council concerning Guidelines for Cryptography Policy*. OECD Legal.
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289>
- OECD Publishing. (2021). *Encouraging Vulnerability Treatment*. OECD Publishing.
<https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1627941005&id=idyaccname=guestychecksum=8C219EC7B667A0AFBA400447E9CBF689>
- OECD Publishing. (2021). *Encouraging Vulnerability Treatment: Overview for Policy Makers*. OECD publishing. <https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1627952337&id=idyaccname=guestychecksum=0E22AD4ED153DC73167D8078C1AC8AEC>
- OECD. (2021). *Understanding the Digital Security of Products*. OECD.
<https://www.oecd-ilibrary.org/docserver/abea0b69-en.pdf?expires=1627856020&id=idyaccname=guestychecksum=AD93FAE7A45992584B81EDE02691DF79>

- OECD. (2015). *Digital Security Risk Management*. OECD.
<https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf>
- OECD. (2021). *Directorate for Science, Technology and Innovation Committee on Digital Economy Policy*. OECD.
[https://one.oecd.org/document/DSTI/CDEP/SDE\(2020\)3/FINAL/en/.pdf](https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/.pdf)
- OECD. (2021a). *Enhancing the Digital Security of Products*. OECD. <https://www.oecd-ilibrary.org/docserver/cd9f9ebc-en.pdf?expires=1627876973&id=idyaccname=guestychecksum=007432517C4E04FF611A1704B9B9BA3E>
- OECD. (2021b). *Smart policies for smart products*. OECD.
<https://www.oecd.org/digital/smart-policies-for-smart-products.pdf>
- OECD. (s. f.). *Together, we create*. OECD. <https://www.oecd.org/about/>
- PCI. (2018). *Requirements and Security Assessment Procedures*. pcisecuritystandards.
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1627673856136
- PCI. (2018). *PCI DSS Quick Reference Guide*. pcisecuritystandards.
https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1627673856190
- Pedreira, O.; Piattini, M.; Luaces, M. R. y Brisaboa, N. R. (2007). *Una revisión sistemática de la adaptación del proceso software*. Redalyc.
- Ramírez, J. (2014). *Como diseñar una investigación académica*.
- Rose, S.; Borchert, O.; Mitchell, S. y Connelly, S. (s. f.). *NIST Special Publication 800-207*. NIST.gov. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- Sampieri, D. R. (2014). *Metodología de la investigación*.

- Scarfone, K.; Schol, M. y Souppaya, M. (2020). *NIST. Security Considerations for Exchanging Files Over the Internet*.
<https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-08.pdf>
- Sharief, K. (2019). *What is a MAC Address? - Definition, Structure, Types and More*.
<https://www.computertechreviews.com/definition/mac-address/>
- Shread, P. (2021). *Best Zero Trust Security Solutions for 2021*. eSecurity Planet.
<https://www.esecurityplanet.com/products/zero-trust-security-solutions/>
- Souppaya, M. y Scarfone, K. (2016). *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. NIST.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>
- Tech Target. (2012). *Caballo de Troya*.
<https://searchdatacenter.techtarget.com/es/definicion/Caballo-de-Troya>
- Tech Target. (s. f.). *FIPS (Federal Information Processing Standards)*.
<https://whatis.techtarget.com/definition/FIPS-Federal-Information-Processing-Standards>
- Techopedia. (2017). *Man-in-the-Middle Attack (MITM)*.
<https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm>
- Techopedia. (2019). *Bring Your Own Device (BYOD)*.
<https://www.techopedia.com/definition/29070/bring-your-own-device-byod>
- Techopedia. (s. f.). *Defense Information Systems Agency (DISA)*.
<https://www.techopedia.com/definition/27901/defense-information-systems-agency-disa>
- TechTerms. (s. f.). *Whitelist*. <https://techterms.com/definition/whitelist>
- Thales. (2021). *2021 data Threat Report Latam Edition in ES*. ThalesGroup.

<https://cpl.thalesgroup.com/sites/default/files/2021-06/2021-data-threat-report-latam-edition-in-es.pdf>

Thales. (2021). *Informe de amenazas a datos de 2021*.

<https://cpl.thalesgroup.com/es/latam-data-threat-report#download-popup>

Thycotic. (s. f.). *Mapping to ISO 27001 Controls*. Esdebe.

<https://www.esdebe.com/perch/resources/iso-27001-annex-s-control-mapping.pdf>

UE. (2021). *Reglamento general de protección de datos*.

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Wigmore, I. (2019). *Intent-based Networking (IBN)*.

<https://whatis.techtarget.com/definition/intent-based-networking-IBN>

Wikipedia. (s. f.). *Digital rights management*.

https://en.wikipedia.org/wiki/Digital_rights_management

Wikipedia. (s. f.a). *IPsec*. <https://en.wikipedia.org/wiki/IPsec>

Wikipedia. (s. f.b). *OECD*. <https://en.wikipedia.org/wiki/OECD>

Wikipedia. (s. f.c). *Split tunneling*. https://en.wikipedia.org/wiki/Split_tunneling

Wikipedia. (s. f.d). *Blacklisting*. <https://en.wikipedia.org/wiki/Blacklisting>

Zhang, E. (s. f.). *What is Data Loss Prevention (DLP)? A Definition of Data Loss*

Prevention. <https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention>

Glosario

- AAD: Azure Active Directory es una solución en la nube de gestión identidad y acceso.
- ABAC: Attribute Based Access Control, en español control de acceso que se basa en atributos. Es un control de acceso lógico que incluye una lista de controles de acceso y accesos que se basan por roles, adicionalmente, realiza una evaluación de atributos y condiciones definidas.
- Activos: son los dispositivos que posee la organización, así como dispositivos físicos de control, puestos de ventas, terminales u otros dispositivos como IoT, entre otros.
- AIP: Azure Information Protection es una solución en la nube que permite descubrir, clasificar y proteger documentos o correos electrónicos por medio de etiquetas.
- Atributos: son características de un sujeto, objeto o condiciones de un ambiente.
- Autenticación: es la verificación de la identidad de un usuario, procesos o dispositivo.
- Autorización: es el proceso de dar acceso o denegar el acceso a los recursos en la red.
- Biométricos: son las características físicas únicas de un individuo que se utilizan para reconocimiento como control de seguridad.
- Blacklisting: es la acción de agrupar una lista de personas, páginas, locaciones, países u otras entidades que se evitan o no son confiables porque se marcaron como no aceptables.
- Bots: es un *software* que ha sido programado para hacer una tarea específica.
- BYOD: Bring Your Own Device es una política empresarial donde los empleados pueden usar sus propios dispositivos para trabajar.

- Caballos de Troya (troyanos): es un programa de código malicioso o dañino que ha sido ofuscado como un programa seguro, puede tomar el control del equipo o causar daños en este.
- CASB: Cloud Access Security Broker es un *software o hardware* en la nube o en premisas que actúa como intermediario de políticas de seguridad entre usuarios o proveedores de servicio.
- CDM: Continuous Diagnostics and Mitigation System, el sistema de diagnóstico y mitigación continuo es un programa que da un fortalecimiento dinámico de la ciberseguridad en las redes o los sistemas.
- Centros de datos: es una ubicación física donde se concentran los recursos computacionales necesarios para una organización.
- CMFA: Continuous Multi Factor Authentication ofrece una mejor alternativa para la monitorización de la actividad de usuarios y evaluación continua de biométricos en el caso de que el dispositivo haya sido accedido.
- Contenedores: es un ambiente virtual donde se agrupan aplicaciones y recursos.
- Criptografía: es el *arte* de codificar texto o datos donde, de manera segura, solo pueda decodificarse por el sujeto deseado.
- DEVSECOPS: Development Security Operations es una práctica que se utiliza para incorporar la seguridad, de manera continua, durante el desarrollo de aplicaciones, durante todo su ciclo de vida o desarrollo.
- Dirección MAC: MAC es Media Access Control, una dirección que identifica cada dispositivo en la red.
- DISA: Defense Information Systems Agency es la agencia estadounidense que soporta el combate con recursos de TI y comunicaciones.
- DLP: Data Loss Prevention es una serie de herramientas que se utiliza para asegurar la información sensible y evitar que se pierda o que se utilice inadecuadamente, es decir, que se acceda de manera no autorizada.

- DoS: Denial of Service es una interrupción ocasionada por un usuario no autorizado en una red de computadoras de manera maliciosa y, usualmente, es continua.
- DRM: Digital Rights Management es una tecnología o herramienta que se utiliza para establecer controles necesarios en la protección de la propiedad.
- En-premisas: On-prem es un término que se utiliza para referirse a los centros de datos físicos y privados de una organización.
- Enrutadores: los *switches* son dispositivos de red que operan en la segunda capa del modelo OSI, se utilizan para intercomunicar dispositivos.
- Federación: es un proceso que permite el transporte de la autenticación y los atributos por la red y que se envíe a otro sistema de gestión de identidad (Active Directory).
- Firewall: es un sistema de control para sistemas o redes diseñado para bloquear accesos no autorizados.
- FISMA: Federal Information Security Management Act es la legislación estadounidense que define las bases y estándares de seguridad para proteger la información y operaciones del gobierno.
- FPIS: Federal Information Processing Standards es una serie de estándares que documentan el proceso de los algoritmos de encriptación.
- Gateway: es un dispositivo de red que se utiliza para comunicar dos redes.
- GDPR: General Data Protection Regulation es la política definida por la Unión Europea para la protección de información y privacidad de los individuos que habitan dentro de la Unión Europea.
- Hacker: una persona que usa medios electrónicos para acceder manera no autorizada a información.

- Hacktivismo: es una actividad que obtiene acceso no autorizado a información o redes con un objetivo social o político.
- HIPAA: Health Insurance Portability and Accountability Act es una regulación estadounidense de los estándares que se utilizan para el uso y el revelado de la información de salud de los individuos.
- Hombre en el medio (MITM): Man-in-the-middle es una técnica de ataque donde un usuario no autorizado ve o lee información del tráfico en un punto medio.
- HTTPS: Hypertext Transport Protocol Secure es un protocolo de comunicación encriptado con TLS/SSL.
- IBN: Intent-based Networking es una forma de administración de redes que utiliza inteligencia artificial o Machine Learning.
- ICAM: Identity, Credential, and Access Management es en español identidad, credenciales y administración de accesos, es una serie de programas, procesos, tecnologías y empleados que se utilizan para crear una identidad digital segura.
- Identidad federada: en un ambiente federado, el sistema de gestión de identidad no autentica una identidad, el protocolo de federación es el que decide quién la valida y de dónde viene el usuario.
- Intune: es una solución en la nube de Microsoft que integra AAD, Azure Information Protection y Administración de dispositivos por MDM y MAM.
- IoT: Internet of Things es un concepto o definición que incluye dispositivos de cualquier naturaleza que estén conectados de manera constante a la red, controlados de manera remota y con una acción específica en el mundo físico.
- IPsec: es un protocolo de red que autentica y encripta los paquetes de información para dar una comunicación segura entre dos puntos sobre Internet.
- ISO: es una organización global que busca federar todos los estándares nacionales.

- Least Privilege (POLP): es una práctica de limitar el acceso de los usuarios al mínimo que estos necesiten.
- MAM: Mobile Application Management es un portal o una serie de políticas para la gestión de aplicaciones.
- MDM: Mobile Device Management es un sistema de gestión de dispositivos móviles.
- MFA: Multifactor Authentication es un método de autenticación que utiliza dos o más métodos para autenticar a un usuario.
- Microsegmentación: es la práctica de dividir la red en segmentos lógicos más pequeños, lo que posibilita el control granular de usuarios, aplicaciones, cargas de trabajo y dispositivos. Esto genera una superficie de ataque menor y facilita la seguridad de perímetro.
- NIST: National Institute of Standard and Technology es una agencia estadounidense que promueve la innovación y estándares nacionales de tecnología.
- Nivel de Confianza: es una fórmula que se utiliza para determinar el nivel de confianza que se tiene de un usuario o dispositivo de acuerdo con sus acciones en la red de la organización.
- NSA: National Security Agency es una agencia secreta creada después de la segunda guerra mundial, la cual busca asegurar las comunicaciones en el mundo y salvaguardar las transmisiones de Estados Unidos.
- Nube: los servicios en la nube se ubican en Internet, están asegurados por un administrador y los ofrecen proveedores.
- OECD: Organization for Economic Cooperation and Development es una organización de Naciones Unidas que busca la cooperación de sus miembros con el desarrollo económico y su desarrollo general.

- PCI: Payment Card Industry es ente que regula las empresas que maneja o procesa información relacionada con tarjetas de pago.
- PII: Personal Identifiable Information, en español información de identificación personal, es toda la información relacionada con un individuo, la cual puede utilizarse para identificarlo.
- Pishing: es una práctica fraudulenta en la que se envían correos con el propósito de suplantar correos oficiales de compañías para obtener información personal de un individuo, como contraseñas o información de tarjetas de pago.
- PKI: Enterprise Public Key Infrastructure es una serie de roles, políticas, *hardware*, *software* y procedimientos necesarios para crear, manejar, distribuir, usar, almacenar y revocar certificados digitales y administrar la encriptación de las llaves públicas. Este busca asegurar la transferencia de información en la red.
- Políticas: es una serie de reglas que definen lo que está permitido, usa atributos, condiciones e información disponible en una organización.
- Ransomware: es un *software* malicioso diseñado para bloquear el acceso a un sistema de computadoras, hasta que se pague por su acceso.
- RBAC: Role Based Access Control es una política de control de acceso que restringe el acceso a la información a sistemas por usuarios no autorizados. La organización puede crear roles para llevar a cabo tareas específicas y así heredar los privilegios asignados a estos roles.
- RDP: Remote Desktop Protocol es un protocolo que soporta servicios de terminal (por medio de una interfaz gráfica) en una red heterogénea.
- Rootkits: es una serie de herramientas que habilita el control de un usuario no autorizado a una computadora sin que se detecte.
- S/MIME: Secure Multipurpose Internet Mail Extensions, en español extensiones seguras multipropósito de correo electrónico, es un estándar que utiliza PKI para firmar información en correos electrónicos.

- Sandbox: es un ambiente de pruebas donde una aplicación o implementación puede probarse, de manera segura.
- SCCM: System Center Configuration Manager es una aplicación de Microsoft que puede administrar servidores y estaciones de trabajo, de manera segura.
- SDC: Software Defined Storage es un almacenamiento diseñado para separar el *software* del *hardware*.
- SDN: Software Defined Networks es una arquitectura dinámica, administrable, de costo efectiva y adaptable que permite controlar la red de manera programable.
- SIEM: Security Information and Event Management System es una aplicación que analiza en tiempo real las alertas de seguridad que genera el ambiente.
- Split Tunneling: es un concepto que permite a los usuarios el acceso medido a dominios seguros e Internet. Asimismo, permite controlar qué tráfico es dirigido por cada red.
- Spyware: es una aplicación que permite obtener información de la actividad conducida por una computadora.
- SSL: Secure Sockets Layer es un protocolo que asegura los datos enviados a Internet utilizando un método de encriptación.
- SSO: Single Sign-On es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación.
- Superficie de ataque: es la suma de todos los puntos diferentes donde un usuario no autorizado puede intentar leer o extraer información de un ambiente.
- Tarjetas inteligentes: son tarjetas con un *chip* o microprocesador con memoria propia en el que se puede encriptar o almacenar certificados.
- TLS: Transport Layer Security es un protocolo que provee autenticación, privacidad e información de integridad entre dos computadoras o aplicaciones.

- Tokens: puede ser *hardware* o un código con la información necesaria para dar acceso a una red, se utiliza para autenticar al usuario, de manera automática o manual.
- VDI: Virtual Desktop Infrastructure es una infraestructura que se utiliza para ejecutar instancias virtuales de computadoras o estaciones de trabajos.
- VMI: Virtual Mobile Infrastructure, es un modelo que permite acceder sistemas operativos desde dispositivos móviles.
- VNC: Virtual Network Computing es una plataforma en la nube que permite compartir aplicaciones de manera remota.
- Whitelisting: es una lista de ítems que tienen el acceso permitido de manera segura, según su postura en la red.
- Worm: es una aplicación que se autorreplica en la red y afecta el rendimiento de los dispositivos o de la red.

Apéndices

Azure Active Directory, Zero Trust Access Control

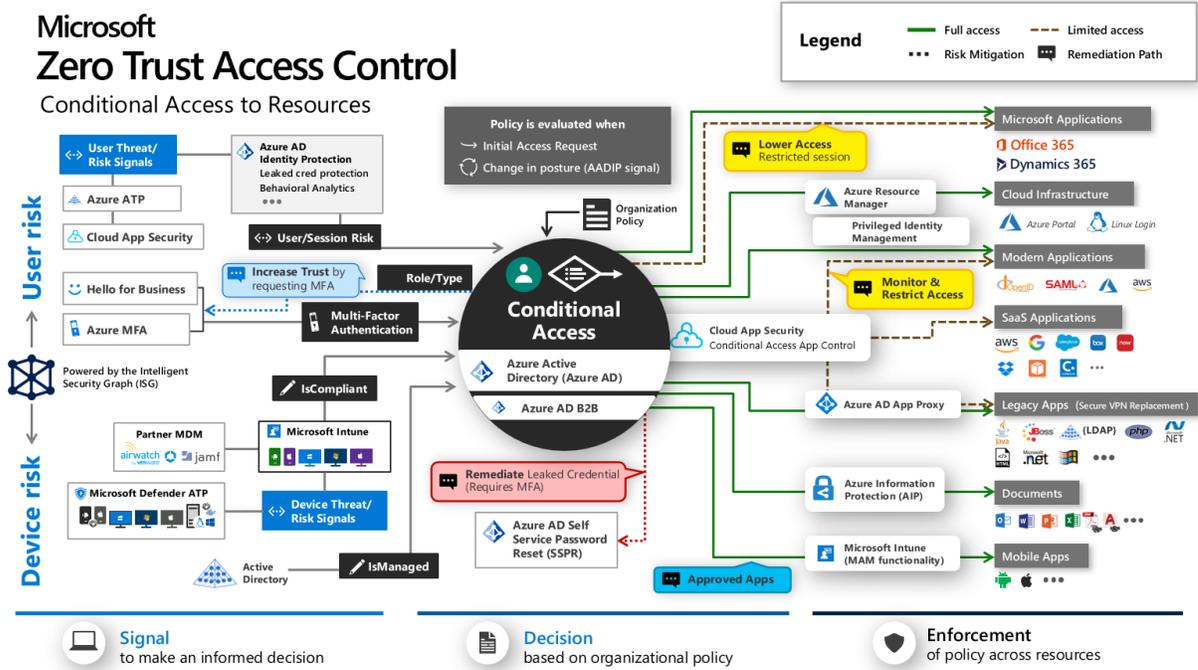


Ilustración 36

Azure Active Directory: Zero Trust Access Control

