CORPORACIÓN UNIVERSITARIA UNITEC	**RESUMEN ANALÍTICO DE INVESTIGACIÓN (RAI)**		
	Código:	**Fecha:**	**Versión No.**

Fecha de elaboración: 10.04.2023			
Tipo de documento	TID: X	Obra Creación:	Proyecto Investigación:
Título	Análisis de seguridad de la solución de Teletrabajo de la empresa CREASISTEMAS S.A.S		
Autor(es)	Augusto Ortega Molina, John Henry Herrera, Raúl Esteban León.		
Tutor(es)	Fabio Antonio González Mendieta		
Fecha de finalización	10.04.2023		
Temática	Seguridad de la Información		
Tipo de investigación	Trabajo final de seminario de investigación		

Resumen

La empresa CREASISTEMAS S.A.S. está formalizando el teletrabajo como una solución de conexión remota de sus colaboradores, desde diferentes regiones del país, y se desea evaluar el estado de la seguridad de la misma, la cual debeestar alineada a las políticas de seguridad de la organización. Por medio de esta investigación, se realiza un proceso de auditoría interna la cual permite identificar el estado del arte y las recomendaciones del mismo, unafotografía actual relacionada al ecosistema presente se sugiere que estos ejercicios se realicen de manera periódica para mantener actualizados los documentos y controles de seguridad de acuerdo a la realidad de la organización, con una periodicidad de anual, la cual permita mantenerse por medio de un ciclo de mejora continua.

Palabras clave

Ciberseguridad, Protección De Punto Final, Riesgo, Mejora, Continua, Seguridad Informática, Teletrabajo, Vulnerabilidad.

Planteamiento del problema

Los colaboradores de CREASISTEMAS S.A.S. usan diferentes dispositivos tecnológicos para acceder a los recursos corporativos y por medio de diferentescanales de comunicación, como son: acceso Internet, redes privadas virtuales, escritorios virtuales, aplicaciones de mensajería, colaboración, teléfonos inteligentes, tabletas, computadores personales y computadores asignados por la organización; estos equipos y mecanismos de comunicación pueden generar vulnerabilidad de seguridad al momento de usar los servicios corporativos, dadoque no se tiene un control para estos dispositivos externos.

En la actualidad no es difícil determinar la confianza que cada persona pretendetener cuando accede a servicios de tecnología desde la comodidad del hogar, se podría decir que se debe gracias a que el entorno que lo rodea es conocido ycon ello se determina que las actividades normales como: consulta de correo, acceso a redes sociales o por citar otro ejemplo realizar pagos de servicios financieros; son actividades sin ningún peligro o se precisa que tantas noticias de brechas de inseguridad se presentan en empresas con gran envergadura, indudablemente son los más buscados, pero a nivel del hogar se han evidenciado un alto crecimiento en el consumo de la Internet y adquisición de dispositivos para conectarse a él, datos que se pueden evidenciar en los enlaces que se relacionan con información respecto a situaciones que se han presentado en el ámbito de los hogares.

Pregunta

¿Cuáles son los riesgos de seguridad de la información específicos asociados con los colaboradores que trabajan en la modalidad de teletrabajo en CREASISTEMAS S.A.S., teniendo en cuenta la variedad de dispositivos y redes utilizados, y cuáles son las soluciones técnicas que se pueden implementar para mitigar estos riesgos y garantizar que se cumplan las políticas de seguridad de la información establecidas por la empresa en este entorno?

Objetivos

El objetivo general de este trabajo de investigación es diseñar e implementar un plan de seguridad de la información efectivo para los colaboradores que trabajanen la modalidad de teletrabajo en CREASISTEMAS S.A.S, que permita mitigar los riesgos específicos asociados con esta modalidad de trabajo y garantizar el cumplimiento de las políticas de seguridad de la información establecidas por la empresa.

Marco teórico

Resuma únicamente los principales referentes teóricos o artísticos que siguió sutrabajo. Señale los números de las páginas de su documento en los que se encuentra la información completa.

En la actualidad, la seguridad de la información es un tema importante para cualquier empresa que maneje datos confidenciales. Con el aumento del trabajoremoto es necesario implementar medidas de seguridad adecuadas para garantizar la protección de la información sensible de la empresa y de sus clientes.

En este marco teórico se explorarán los conceptos fundamentales de la seguridad de la información, el teletrabajo y los riesgos asociados a la seguridadde la información en el teletrabajo.

Seguridad de la información: La seguridad de la información es un conjunto de medidas que se toman para garantizar la confidencialidad, integridad y disponibilidad de la información. Se refiere a la protección de la información de cualquier tipo de amenaza, incluyendo el acceso no autorizado, la modificación,la divulgación y la destrucción.

La ISO 27001 es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información y proporciona un marco parala implementación de medidas de seguridad de la información. Esta norma es utilizada por muchas empresas como guía para la implementación de sus sistemas de seguridad de la información (ISO, 2013).

Teletrabajo: El teletrabajo es una modalidad de trabajo en la que los empleadosrealizan sus tareas desde un lugar diferente a la oficina de la empresa. Esto puede ser desde casa, un café, una biblioteca, entre otros lugares. Esta modalidad de trabajo se ha vuelto cada vez más común debido a los avances tecnológicos y la necesidad de flexibilidad en el trabajo.

Riesgos de seguridad en el teletrabajo: El teletrabajo también presenta riesgosde seguridad para las empresas, ya que los datos pueden estar expuestos a amenazas en un ambiente no controlado. Algunos de estos riesgos incluyen:

Acceso no autorizado: Puede haber personas que no sean empleados de laempresa que tengan acceso a la información confidencial, como amigos, familiares u otras personas en el hogar del teletrabajador.
Dispositivos no seguros: Los dispositivos utilizados por los teletrabajadores pueden no estar actualizados con los parches de seguridad más recientes, loque puede permitir la entrada de virus y malware.

Redes no seguras: Las redes utilizadas por los teletrabajadores pueden serpúblicas o no estar seguras, lo que aumenta el riesgo de que los datos seaninterceptados.

Amenazas y vulnerabilidades en el teletrabajo: Se debe analizar las posibles amenazas y vulnerabilidades en el teletrabajo, como, por ejemplo, ataques dephishing, malware, robo de información, y la falta de actualizaciones de seguridad.

Tecnologías de seguridad para el teletrabajo: Se deben investigar las tecnologías de seguridad disponibles para proteger la información en el teletrabajo, como soluciones de VPN, firewalls, antivirus, y herramientas deencriptación.

Políticas y procedimientos de seguridad en el teletrabajo: Se deben considerarlas políticas y procedimientos de seguridad necesarios para garantizar la protección de la información en el teletrabajo, como, por ejemplo, la definición de reglas de uso de dispositivos y aplicaciones, la gestión de contraseñas y la autenticación de usuarios.

Cumplimiento de normativas y estándares: Se debe analizar el cumplimiento delas normativas y estándares de seguridad de la información, como ISO 27001, NIST, HIPAA, GDPR, y cómo se aplican al teletrabajo.

Capacitación y concientización en seguridad: Se debe considerar la capacitacióny concientización en seguridad para los trabajadores que realizan teletrabajo, para que estén informados y preparados para evitar amenazas de seguridad y adoptar medidas de seguridad adecuadas.

Método

Resuma únicamente los principales elementos metodológicos que empleó en su investigación. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Para el desarrollo de este proyecto de investigación se utilizó ISO / IEC 27001:2013. Para seguir evidenciado el proceso a realizar diríjase a la página 36

Resultados, hallazgos u obra realizada

Presente el resumen de los principales resultados o hallazgos de su investigación o una sinopsis de la obra creada. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Basándonos en las evidencias identificadas, el contexto de la organización y el estado actual de los riesgos de seguridad de la información, se realizó la entrega de un informe final a la gerencia de CREASISTEMAS, con el objetivo de dar continuidad a la mejora continua de sus procesos de seguridad de la información y la implementación de controles que permitan en el tiempo mantener un estado deseable y aceptable, para abordar los retos actuales. Para seguir evidenciado el proceso a realizar diríjase a la página 55.

Conclusiones

Presente el resumen de las conclusiones a las que llegó. Señale los números delas páginas de su documento en los que se encuentra la información completa.

El trabajo de investigación propuesto, soluciono los objetivos planteados y resolvió la pregunta problema; la empresa CREASISTEMAS S.A.S. ha estado madurando su postura de seguridad y ha venido con el tiempo implementando los controles de seguridad pertinentes para migrar sus conexiones de VPN Cliente a Sitio, por herramientas integradas a esquemas de seguridad más robustos y a adecuado al contexto de actual, mediante la gestión de accesos basados en roles, y la reducción de permisos basados en servicios y protocolos, la implementación múltiples factores de autenticación para la identificación de los usuarios en las aplicaciones, monitoreo y control de las vulnerabilidades de seguridad a nivel de servidores y estaciones de trabajo de punto final, han logrado mitigar los riesgos en el Teletrabajo. Para seguir evidenciado el proceso a realizar diríjase a la página 56.

Productos derivados

Referencie los artículos, libros, capítulos de libro, ponencias, etc., que fueronresultado de su proceso investigativo.

Análisis de seguridad de la solución de Teletrabajo de la empresa CREASISTEMAS S.A.S

Augusto Ortega Molina Cod. 12226009

John Henry Herrera Cod. 12226020

Raúl Esteban Peña León Cod. 12226017

Corporación Universitaria UNITEC

Escuela de Posgrados

Especialización en Seguridad de la Información

Bogotá, Distrito Capital

13 de abril de 2023.

Análisis de seguridad de la solución de Teletrabajo de la empresa CREASISTEMAS S.A.S

Augusto Ortega Molina Cod. 12226009

John Henry Herrera Cod. 12226020

Raúl Esteban Peña León Cod. 12226017

Fabio Antonio González Mendieta director

Corporación Universitaria UNITEC

Escuela de Posgrados

Especialización en Seguridad de la Información

Bogotá, Distrito Capital

13 de abril de 2023.

TABLA DE CONTENIDO

1 Planteamiento del problema 7
1.1 Justificación 10
1.2 Pregunta de investigación 11
1.3 Objetivos 12
1.3.1 Objetivo General 12
1.3.2 Objetivos Específicos 12
2 Marco Teórico y estado del arte 13
2.1 Marco conceptual 13
2.2 Teletrabajo 13
2.2.1 Adopción del teletrabajo 14
2.2.2 Modalidades de Teletrabajo 15
2.2.3 Herramientas TIC 16
2.2.4 Ventajas y Desventajas 19
2.3 Seguridad de la Información 20
2.3.1 Norma ISO/IEC 27001:2013 24
2.3.2 Tipos de amenazas 34
2.3.3 Riesgos de seguridad en el teletrabajo 36
2.3.4 Protección de Punto Final 36
3 Desarrollo Metodológico 40
3.1 Contexto Organizacional 40
3.2 Tipo y Diseño Metodológico 40
3.3 Participantes y Fuentes de Datos 43
3.4 Análisis Encuestas y Estadísticas 44
3.5 Cronograma y Presupuesto 54
4 Resultados y Discusiones 59
5 Conclusiones 60
6 Referencias 63
7 Anexos 68

Tablas e Ilustraciones

Tabla 1. Tipos de Amenazas 35
Tabla 2. Cronograma ejecución proyecto de investigación 56
Tabla 3. Presupuesto ejecución proyecto investigación 58

Ilustración 1. Pilares de la seguridad de la información 21
Ilustración 2. Riesgo, Amenaza y Vulnerabilidades 22
Ilustración 3. La Evolución del Teletrabajo 23
Ilustración 4. Utilización Servicio Teletrabajo en CREASISTEMAS 44
Ilustración 5. En qué tipo de dispositivos accede al servicio de teletrabajo 45
Ilustración 6. Conexiones seguras para el ingreso al servicio de teletrabajo 45
Ilustración 7. Comparte el equipo con otras personas cercanas 46
Ilustración 8. Ha compartido su contraseña 46
Ilustración 9. Ha instalado alguna solución de seguridad en el dispositivo 47
Ilustración 10. CREASISTEMAS cuenta con políticas claras de seguridad para el teletrabajo 47
Ilustración 11. Se realizan actualizaciones de seguridad en los equipos para el teletrabajo 48
Ilustración 12. Se realizan copias de seguridad de los datos en el teletrabajo 48
Ilustración 13. Se han producido incidentes de seguridad relacionados con el teletrabajo 49
Ilustración 14. La empresa proporciona formación en seguridad 49
Ilustración 15. Ha recibido alguna comunicación de nuevas amenazas 50
Ilustración 16. Cuál es tu opinión sobre la seguridad de la solución del teletrabajo 50
Ilustración 17. Considera que se debe de implementar medidas de seguridad adicionales 51
Ilustración 18. Que medidas de seguridad sugeriría para mejorar el teletrabajo 51
Ilustración 19. Cree que existen suficientes medidas de seguridad para el teletrabajo 52
Ilustración 20. Alguna vez han detectado un incidente mientras utilizan el teletrabajo 53
Ilustración 21. Medidas adicionales para implementar en el teletrabajo 53
Ilustración 22. Tiene definida una política de seguridad para el uso de dispositivos en el teletrabajo 54

Resumen

Con la creciente adopción del trabajo remoto en la organización posterior a la pandemia, se hace más evidente la necesidad de implementar medidas de seguridad adecuadas para garantizar la protección de la información empresarial sensible y de los empleados, reflejados en la realidad actual y sus riesgos.

Este trabajo de investigación se centra en la evaluación de los riesgos y desafíos asociados con la seguridad de la información en el teletrabajo para la empresa CREASISTEMAS S.A.S., se aborda desde la evaluación de las políticas y documentación existente de seguridad de la información, la evaluación de riesgos, la implementación de soluciones técnicas y la planificación de la concientización y capacitación para los teletrabajadores.

El objetivo de este trabajo es proporcionar una guía práctica para ayudar a las organizaciones a implementar medidas efectivas de seguridad de la información en la modalidad de teletrabajo, mitigando los riesgos y garantizando la protección de los datos empresariales sensibles, normatividad vigente y de acuerdo con la norma ISO 27001:2013 implementar procesos de mejora continua para mantener vigentes los controles de seguridad acorde a las necesidades actuales.

Palabras claves: Ciberseguridad, Mejora Continua, Protección de punto Final, Riesgo, Seguridad Informática, Teletrabajo, Vulnerabilidad.

1 Planteamiento del problema

Los colaboradores de la empresa CREASISTEMAS S.A.S., usan diferentes recursos tecnológicos para acceder a la red corporativa, como canales de comunicación con acceso internet, redes privadas virtuales, escritorios virtuales, aplicaciones de mensajería, colaboración, dispositivos como teléfonos inteligentes, tabletas, computadores personales y computadores propios asignados por la organización.

Estos equipos y mecanismos de comunicación pueden generar vulnerabilidades de seguridad al momento de usar los servicios corporativos; esto generó la necesidad de revisar el modelo de teletrabajo, modificar políticas, procedimientos e implementar mecanismo de control que permitan gestionar los riesgos de la organización. En la actualidad no es difícil determinar la confianza que cada persona pretende tener cuando accede a servicios de tecnología desde la comodidad del hogar, se podría decir que se debe gracias a que el entorno que lo rodea es conocido y con ello se determina que las actividades normales como: consulta de correo, acceso a redes sociales, visualización de contenidos, o por citar otro ejemplo, realizar pagos de servicios financieros; son actividades sin ningún peligro o se precisa que tantas noticias de brechas de inseguridad se presentan en empresas con gran envergadura, indudablemente son los más buscados, pero a nivel del hogar se han evidenciado un alto crecimiento en el consumo de la Internet y adquisición de dispositivos para conectarse a él, datos que se pueden evidenciar en los enlaces que se relacionan con información respecto a situaciones que se han presentado en el ámbito de los hogares.

Con ello debemos preguntarnos ¿Cuáles son los riesgos a los que me encuentro expuesto al realizar estas actividades?, la respuesta a esta pregunta puede causar confusión, pero es la clave, ya que la mayor causa de exposición

a estas actividades sonlos eventos asociados debido a conductas inadecuadas; al final las personas seguimos siendo el eslabón más débil. Se podrán implementar controles y desplegar herramientas.

Con la más alta tecnología siendo conocedores en el tema, pero si en el entorno no siempre somos quienes usan el acceso a la red de internet, ese conocimiento queda aún lado si las conductas que nosotros aplicamos no son retroalimentadas a toda persona que conviven en nuestro mismo entorno.

Dados estos casos se evidencia que una persona del común puede ser atacada en su hogar, a raíz de esto se ha generado la necesidad de ayudar a un sector de personas en un inicio, pero con la gran certeza que podría ser difundida para que la seguridad sea parte de todos, impactando de buena manera cualquier nicho poblacional.

Los antecedentes del desarrollo actual coinciden con los acontecimientos de la sociedad de la información, las redes entre computadoras y el fenómeno “Internet”, cuya expansión ha configurado la quinta dimensión de la guerra moderna y ha afectado sensiblemente la vida cotidiana de los diversos actores en el mundo global. De hecho, su estudio se convierte en una tarea obligada para la conducción político-estratégica de la defensa de las naciones. Armadas (2017).

También se toma la siguiente referencia, en primer lugar, estudiamos el nacimiento de un nuevo espacio delictivo el “ciberespacio” y todas sus amenazas, en una segunda parte se ve la reacción que este fenómeno ha provocado en las naciones y organizaciones internacionales en dirección a determinar y estudiar todos estos delitos, sus causas, métodos y reacciones, para poder combatirlos desde el aspecto legal (legislación española, europea e internacional) y a partir de aquí finalizar mostrando la visión estratégica de

defensa de los estados, estudiando como ejemplos las líneas de actuación que utiliza España y Europa para contrarrestar su efecto destructivo en la sociedad actual. España (2017).

1.1 Justificación

Realizar una investigación del estado actual de la seguridad de la información de la solución de teletrabajo de CREASISTEMAS S.A.S. radica en la necesidad de identificar la postura de la organización y las medidas implementadas en la actualidad para garantizar la protección de los activos de información de la empresa en un entorno de trabajo remoto.

El teletrabajo ha permitido mayor flexibilidad de acceso para los colaboradores de las empresas en Colombia, es fundamental implementar procesos de mejora continua que permitan gestionar las medidas de seguridad de la información de a las necesidades de las empresas, que se mantengan vigentes, actuales y sean efectivas para proteger los activos de información de los riesgos de ciberseguridad que se encuentran en constante evolución.

Como resultado de esta investigación, permitirá identificar por medio del análisis del entorno actual, las vulnerabilidades y riesgos asociados, propone soluciones para mitigarlos y mejorar la postura de seguridad de las organizaciones, para con sus clientes, proveedores y comunidad en nuestro país.

1.2 Pregunta de investigación

¿Cómo identificar vulnerabilidades sobre los dispositivos tecnológicos usados por el personal de TI de la empresa CREASISTEMAS S.A.S, que desarrollan sus actividades laborales en la modalidad de teletrabajo, para tomar decisiones y minimizar riesgos que afecten la seguridad de la información y su continuidad operativa, mediante la evaluación de los controles del anexo A de ISO 27001:2013, para el teletrabajo?

1.3 Objetivos

1.3.1 Objetivo General

Diseñar e implementar un plan de seguridad de la información efectivo para los colaboradores que trabajan en la modalidad de teletrabajo en CREASISTEMAS S.A.S, que permita mitigar los riesgos específicos asociados con esta modalidad de trabajo y garantizar el cumplimiento de las políticas de seguridad de la información establecidas por la empresa.

1.3.2 Objetivos Específicos

- Evaluar las políticas de seguridad de la información actuales de CREASISTEMAS

  S.A.S. y determinar si están adaptadas a la modalidad de teletrabajo, identificandoposibles brechas o lagunas en la política de seguridad actual de la empresa.

- Realizar una evaluación de riesgos para la seguridad de la información de los dispositivos utilizados por los colaboradores que trabajan en la modalidad de teletrabajo, analizando la seguridad de los sistemas operativos, la configuración delsoftware y la presencia de software malicioso.

- Elaborar un plan de concientización y capacitación en seguridad de la informaciónpara los colaboradores que trabajan en la modalidad de teletrabajo, enfocado en laimportancia de la seguridad de la información, la identificación de amenazas y la implementación de buenas prácticas de seguridad.

2 Marco Teórico y estado del arte

"En la actualidad los sistemas de información, la internet y la computación en la nube son el soporte para el almacenamiento, gestión y aplicación de información personal y organizacional, convirtiéndose en el blanco para quienes la quieren robar, manipular o dañar, o desean afectar a sus propietarios. Esto se presenta porque las personas y las organizaciones soportan su rutina en esta información, de manera que cualquier manipulación o fallo termina afectándolos notoriamente, a nivel individual y colectivo." (Ospina y Sanabria 2020).

2.1 Marco conceptual

Para abordar el tema investigación sobre el teletrabajo es necesario tener claridad en los conceptos sobre:

2.2 Teletrabajo

El teletrabajo en Colombia es un método laboral que permite a los empleados trabajar desde un lugar diferente a la oficina tradicional, normalmente desde sus hogares, utilizando las tecnologías de la información y la comunicación TIC (Tecnologías de la Información y Comunicaciones) para realizar sus tareas y comunicarse con sus compañeros de equipo de trabajo y lideres.

En Colombia, el teletrabajo ha ganado popularidad en los últimos años, especialmente a raíz de la pandemia de COVID-19 en 2020, cuando muchas empresas tuvieron que adaptarse a esta modalidad de trabajo para seguir funcionando. De acuerdo con la ley 1221 de 2008, se establecieron las normas para la promoción del teletrabajo en Colombia, abordando temas como los

beneficios y responsabilidades, promoviendo su adopción en el sector público y privado, adicionalmente reglamentado por el decreto 1072 de 2015, en el Decreto 1072 de 2015 establece disposiciones para la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) en Colombia (Presidencia de la República, 2015).

2.2.1 Adopción del teletrabajo

Colombia ha experimentado un aumento en la adopción del teletrabajo en los últimos años, especialmente debido a la pandemia de COVID-19, que ha llevado a las empresas y empleados a adaptarse rápidamente a nuevas formas de trabajar, de acuerdo con lo mencionado por Morales y Ropero (2022).

El Decreto 884 de 2012 es una norma emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, que regula el teletrabajo en el país. Entre las disposiciones más relevantes del decreto, se encuentran las siguientes:

Se define el teletrabajo como una forma de trabajo que se realiza de manera parcial o total desde la residencia del trabajador o desde cualquier otro lugar fuera de las instalaciones del empleador, utilizando tecnologías de la información y la comunicación. Se establecen los requisitos para que un contrato laboral incluya la modalidad de teletrabajo, incluyendo la necesidad de que se acuerde por escrito y que se especifiquen las condiciones en que se realizará el trabajo.

Se establece la obligación del empleador de proporcionar los recursos tecnológicos necesarios para que el teletrabajador pueda desempeñar sus

funciones en condiciones de seguridad y salud ocupacional. Se establecen las responsabilidades del empleador y del teletrabajador en cuanto a la protección de la información confidencial de la empresa y de terceros, y se señala que el empleador debe implementar medidas de seguridad adecuadas para garantizar la protección de dicha información.

Se establece la obligación del empleador de velar por la protección de la integridad psicológica del teletrabajador, mediante la promoción de un ambiente de trabajo saludable y el cumplimiento de las normas laborales aplicables. MINTIC (2020).

2.2.2 Modalidades de Teletrabajo

La Ley 1221 de 2008 y el Decreto 884 de 2012 establecen las siguientes modalidades de teletrabajo en Colombia:

Teletrabajo autónomo: Esta modalidad se refiere a los empleados que trabajan de manera remota en su propia residencia o en un lugar diferente a las instalaciones de la empresa. Los empleados en esta modalidad tienen un contrato laboral y realizan sus actividades de manera regular y autónoma sin necesidad de una supervisión directa del Congreso de la República de Colombia (2008).

Teletrabajo suplementario: En esta modalidad, los empleados trabajan de manera remota por fuera de su horario laboral normal. Por ejemplo, un empleado que trabaja en la oficina durante el día y realiza tareas adicionales desde su hogar por la noche o los fines de semana. Esta modalidad permite a los empleados aumentar sus ingresos o mejorar su productividad al complementar su trabajo presencial con actividades realizadas de manera remota descrito en la normatividad emitida por el Congreso de la República de Colombia, (2008).

Teletrabajo móvil: Los empleados en esta modalidad trabajan de manera remota utilizando dispositivos móviles, como teléfonos inteligentes, tabletas o computadoras portátiles y se desplazan frecuentemente entre diferentes lugares para realizar sus actividades laborales. Este tipo de teletrabajo es común en profesionales de ventas, técnicos de campo y consultores que necesitan estar en constante movimiento para cumplir con sus responsabilidades laborales, Congreso de la República de Colombia (2008).

Las modalidades de teletrabajo en Colombia proporcionan diferentes opciones para que las organizaciones y empleados adapten sus prácticas laborales a las necesidades y preferencias individuales, así como a los requerimientos organizacionales y de acuerdo al contexto, así lo menciona Chávez (2020), en su presentación ante la OIT donde menciona toda la evolución del teletrabajo y como se ha fortalecido después de la pandemia.

Según Benjumea-Arias, M. L., Villa-Enciso, E. M., & Valencia-Arias, J. (2016)., el teletrabajo en Colombia se ha convertido en una opción importante para las organizaciones y los empleados, ya que proporciona diferentes modalidades de trabajo remoto que se adaptan a las necesidades y preferencias de cada individuo y a los requerimientos del negocio.

2.2.3 Herramientas TIC

Existen varias herramientas que facilitan la implementación del teletrabajo en las organizaciones. Estas herramientas ayudan a mejorar la comunicación, colaboración, productividad y seguridad mientras se trabaja de forma remota, Kaivanto (2021).

- **Tecnologías de seguridad para el teletrabajo:** Se deben investigar las tecnologías de seguridad disponibles para proteger la información en el teletrabajo, como soluciones de VPN, firewalls, antivirus, y herramientas de encriptación.

- **Políticas y procedimientos de seguridad en el teletrabajo**: Se deben considerar las políticas y procedimientos de seguridad necesarios para garantizar la protección de la información en el teletrabajo, como, por ejemplo, la definición de reglas de uso de dispositivos y aplicaciones, la gestión de contraseñas y la autenticación de usuarios.

- **Cumplimiento de normativas y estándares**: Se debe analizar el cumplimiento de las normativas y estándares de seguridad de la información, como ISO 27001, NIST (National Institute of Standards and Technology), HIPAA, GDPR, y cómo se aplican al teletrabajo.

- **Capacitación y concientización en seguridad**: Se debe considerar la capacitación y concientización en seguridad para los trabajadores que realizan teletrabajo, para que estén informados y preparados para evitar amenazas de seguridad y adoptar medidas de seguridad adecuadas.

A continuación, se presenta una lista de categorías de herramientas tecnológicas usadas de manera común en las organizaciones:

- **Comunicación y mensajería:**

Slack: Es una plataforma de comunicación basada en canales que permite a los equiposmantener conversaciones organizadas y accesibles.
Microsoft Teams: Es una plataforma de comunicación y colaboración que integra chat,videollamadas, y compartición de archivos.
Google Chat: Es una herramienta de mensajería segura para equipos que forma parte de Google Workspace.

- **Reuniones y conferencias virtuales:**

Zoom: Plataforma de videoconferencia y reuniones virtuales con opciones de grabación ycompartición de pantalla.
Google Meet: Es una herramienta de videoconferencia que permite a los usuarios unirse areuniones mediante un enlace o código de acceso.
Cisco Webex: Solución empresarial de videoconferencia y reuniones virtuales confunciones avanzadas de seguridad y colaboración.

- **Colaboración y gestión de proyectos:**

Trello: Herramienta de gestión de proyectos basada en tarjetas y tableros que permite alos equipos organizar y priorizar tareas.
Asana: Plataforma de gestión de proyectos y colaboración que permite a los equiposplanificar, organizar y hacer seguimiento del trabajo.
Monday.com: Plataforma de gestión del trabajo y colaboración que ayuda a los equipos acoordinar proyectos y tareas.

- **Compartición y almacenamiento de archivos:**

Google Drive: Es un servicio de almacenamiento en la nube que permite a los usuariosguardar, compartir y acceder a archivos desde cualquier dispositivo.
Dropbox: Es una plataforma de almacenamiento en la nube y compartición de archivosque facilita la colaboración en documentos y carpetas.
Microsoft OneDrive: Es un servicio de almacenamiento en la nube que forma parte deMicrosoft 365 y permite a los usuarios almacenar y compartir archivos.

- **Seguridad y privacidad:**

LastPass: un administrador de contraseñas que ayuda a los usuarios a generar y almacenarcontraseñas seguras en un único lugar.
NortonLifeLock: una suite de seguridad que ofrece protección antivirus, antimalware yotras funciones de seguridad para dispositivos.
ExpressVPN: Es una red privada virtual (VPN) que cifra las conexiones a Internet yprotege la privacidad de los usuarios.

- **Herramientas de productividad y organización:**

Todoist: Es una aplicación de lista de tareas que permite a los usuarios organizar y priorizar tareas y proyectos.

Evernote: Aplicación de toma de notas que permite a los usuarios capturar y organizarideas, notas y listas en un único lugar.
RescueTime: Es una herramienta de seguimiento del tiempo que ayuda a los usuarios acomprender cómo invierten su tiempo en dispositivos y aplicaciones.

Estas herramientas, cuando se utilizan de manera efectiva, pueden facilitar la implementación del teletrabajo en las organizaciones y mejorar la experiencia de trabajo remoto para empleados y empleadores.

2.2.4 Ventajas y Desventajas

A continuación, se presentan algunas ventajas y desventajas del teletrabajo en Colombia, con citas y referencias recientes.

Ventajas:

Ahorro de tiempo y costos: El teletrabajo permite a los empleados

evitar los largos tiempos de desplazamiento y los costos asociados con el transporte público o privado (Rodriguez, 2021).

Flexibilidad laboral: El teletrabajo ofrece una mayor flexibilidad en cuanto a horarios y espacios de trabajo, lo que puede mejorar el equilibrio entre la vida laboral y personal Camacho et al. (2020).

Desventajas:

Brecha digital: El acceso limitado a tecnologías de información y comunicación(TIC) y a una conexión a internet de calidad en algunas áreas de Colombia puede dificultar la adopción y el éxito del teletrabajo Ramirez y et al., (2019).

Aislamiento social: El teletrabajo puede generar sentimientos de aislamiento y disminución de la interacción social, lo que podría afectar la salud mental y emocional delos empleados Quintero et al., (2021).

Dificultades para desconectar: El teletrabajo puede provocar que los empleados tengan problemas para desconectar del trabajo, lo que puede aumentar el estrés y afectarsu bienestar Camacho et al., (2020).

2.3 Seguridad de la Información

De acuerdo con Álvarez (2013), en su trabajo de grado "Diseño de una Metodología para el Análisis de Riesgo en los Sistemas de Gestión de Seguridad de Información (Marisgsi)", presentado en la Universidad Centro-occidental "Lisandro Alvarado" para optar al título de Magister Scientiarum en Ciencias de la Computación, se ofrece una perspectiva global sobre seguridad informática, específicamente en el aseguramiento de recursos de la empresa,

tomando como base los tres pilares: confidencialidad, integridad y disponibilidad. Dicho trabajo se relaciona con este proyecto aplicado, dado que proporciona pasos para la planificación y el establecimiento de medidas para el aseguramiento de la información dentro de una empresa.

Ilustración 1. Pilares de la seguridad de la información

Fuente**:** Elaboración Propia

Según Vásquez (2013), en su tesis de grado titulada "Aplicación de la metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información Aplicado a la Empresa Pesquera e Industrial Bravito S. A. en la Ciudad de Machala", presentada en la Universidad Politécnica Salesiana, sede Cuenca, para optar al título de Ingeniera de Sistemas, se definen aspectos importantes en la identificación y valoración de los riesgos a los que puede estar sujeta la información si no se toman medidas tendientes a protegerlos de ataques que afecten su integridad. Dicha investigación se relaciona con este trabajo, ya que coincide en el establecimiento de una metodología que proporcione los elementos de juicio necesarios encaminados a la protección de la información, mitigando las amenazas a las que pueden estar expuestas.

Ilustración 2. Riesgo, Amenaza y Vulnerabilidades

Fuente**:** Elaboración Propia

De acuerdo con Martínez (2019). Diseño de políticas de seguridad de la información para la unidad de tecnología de la Cámara de Comercio de Cúcuta (Tesis de grado, Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia)., define a partir de la gestión de riesgos, las salvaguardas necesarias para maximizar las condiciones de seguridad tendientes a proteger la información de amenazas que afecten la integridad, disponibilidad y confidencialidad. Dicho trabajo se relaciona con este proyecto ya que en ambos se pretende suministrar los controles que permitan asegurar los activos de información y la infraestructura tecnológica de una empresa.

En la actualidad, la seguridad de la información es un tema importante para cualquier empresa que maneje datos confidenciales. Con el aumento del trabajo remoto, es necesario implementar medidas de seguridad adecuadas para garantizar la protección de la información sensible de la empresa y de sus clientes concuerda con lo mencionado por Amin (2017). En este marco teórico se explorarán los conceptos fundamentales de la seguridad de la información, el teletrabajo y los riesgos asociados a la seguridad de la información en el teletrabajo.

De acuerdo con lo mencionado en la revista Innovation at Work. (2020), en la era digital actual, la seguridad de la información es un tema crítico para cualquier organización que maneje datos sensibles. Con el aumento del trabajo remoto debido a la pandemia del COVID-19, es aún más importante implementar medidas de seguridad adecuadas para garantizar la protección de la información confidencial de la empresa y de sus clientes. En este contexto, se deben explorar los conceptos fundamentales de la seguridad de la información y los riesgos asociados al teletrabajo para poder aplicar medidas de seguridad efectivas.

Ilustración 3. La Evolución del Teletrabajo

Fuente: Messenger Gschwind (2016)

Seguridad de la información

La seguridad de la información es un conjunto de medidas que se toman para garantizar la confidencialidad, integridad y disponibilidad de la información. Se refiere a la protección de la información de cualquier tipo de amenaza, incluyendo el acceso no autorizado, la modificación, la divulgación y la destrucción.

La ISO 27001 es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información y proporciona un marco para la implementación de medidas de seguridad de la información. Esta norma es utilizada por muchas empresas como guía para la implementación de sus sistemas de seguridad de la información ISO (2013).

Teletrabajo

El teletrabajo es una modalidad de trabajo en la que los empleados realizan sus tareas desde un lugar diferente a la oficina de la empresa. Esto puede ser desde casa, un café, una biblioteca, entre otros lugares. Esta modalidad de trabajo se ha vuelto cada vez más común debido a los avances tecnológicos y la necesidad de flexibilidad en el trabajo.

La seguridad de la información es un aspecto clave que debe estar inmerso en laimplementación de cualquier tipo de solución organizacional, tanto tecnológica o no el análisis del estado de la seguridad de la información permite evaluar la madurez de la organización frente a la gestión de riesgos y su responsabilidad en el entorno social.

El teletrabajo dinamiza los modelos de conexión de los dispositivos de punto final, a las organizaciones dentro del país, como fuera del país, y abordar los temas seseguridad de la información deben tener un contexto más amplio cuando se trata de activos de información que se encuentran fuera de las organizaciones.

2.3.1 Norma ISO/IEC 27001:2013

Existen en la actualidad diferentes metodologías y herramientas que apoyan la gestión de riesgos de seguridad de la información abordando así

temas como políticas,procedimientos, herramientas de gestión de activos de punto final, que abordan los aspectos desde la mejora continua, para abordar las necesidades de las organizaciones acorde al contexto.

Algunos autores, Roy (2020), comparan las normas ISO 27001, NIST SP 800-53 y CIS CSC como estándares de seguridad de la información para el desarrollo de una línea base de seguridad. Los autores concluyen que ISO 27001 es una de las normas más ampliamente adoptadas y reconocidas internacionalmente, y que ofrece una estructura sólida y sistemática para la gestión de la seguridad de la información. Además, la norma es compatible con otras normas y regulaciones relacionadas con la seguridad de la información, y permite una mejora continua de los procesos de seguridad de la información.

La norma ISO/IEC 27001:2013 es un estándar internacional para la gestión de la seguridad de la información que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de una organización, lo que permite garantizar la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2013). En la norma ISO/IEC 27001:2013, se establecen 14 dominios de control de seguridad de la información en el Anexo A.

Estos dominios de control son:

- A.5: Política de seguridad de la información
- A.6: Organización de la seguridad de la información
- A.7: Seguridad en los recursos humanos
- A.8: Gestión de activos A.9: Control de acceso
- A.10: Criptografía
- A.11: Seguridad física y del entorno
- A.12: Seguridad en las operaciones
- A.13: Seguridad en las comunicaciones

- A.14: Adquisición, desarrollo y mantenimiento de sistemas de información
- A.15: Relaciones con proveedores
- A.16: Gestión de incidentes de seguridad de la información
- A.17: Continuidad del negocio y seguridad de la información
- A.18: Cumplimiento

Comparación de modelos de seguridad de la información (Ramirez 2016), ISO 27001:2013 es una metodología recomendada para pequeñas y grandes empresas, teniendo en cuenta que esta norma comparte con la mayoría de los estándares de la ISO, una estructura basada en el ciclo PHVA (Planear, Hacer, Verificar, Actuar) ,

Cada dominio aborda diferentes aspectos de la seguridad de la información y proporciona controles específicos para gestionar los riesgos asociados. Algunos de los controles sugeridos por la norma ISO/IEC 27001:2013 que pueden ser relevantes para elteletrabajo incluyen los siguientes dominios:

Política de seguridad de la información (A.5.1.1): Establecer y comunicar políticas de seguridad de la información específicas para el teletrabajo, que incluyan requisitos y responsabilidades para empleados y terceros. Para evaluar el estado de implementación y madurez de este control, se pueden abordar las siguientes preguntas:

- ¿Existe una política de seguridad de la información documentada yactualizada en la organización?
- ¿La política de seguridad de la información incluye objetivos y principiosclaros relacionados con la seguridad de la información?
- ¿La alta dirección ha aprobado y respaldado explícitamente la política deseguridad de la información?

- ¿Se comunica la política de seguridad de la información a todos los empleadosy partes interesadas relevantes?
- ¿Se capacita a los empleados sobre la política de seguridad de la informacióny sus responsabilidades en relación con la seguridad de la información?
- ¿Se revisa y actualiza periódicamente la política de seguridad de lainformación para garantizar que siga siendo relevante y efectiva?
- ¿Se monitorea y mide el cumplimiento de la política de seguridad de lainformación y se toman acciones correctivas cuando sea necesario?

Una organización con un estado de madurez alto en el dominio A.5 demuestra unsólido compromiso con la seguridad de la información, respaldado por una política bien definida, alineada con los objetivos de negocio y comunicada de manera efectiva a todaslas partes interesadas. Además, la política es revisada y actualizada periódicamente para garantizar su relevancia y eficacia, y se realizan auditorías para asegurar el cumplimientoy la mejora continua.

Control de acceso (A.9): Se enfoca en garantizar que el acceso a los activos de información esté restringido a usuarios autorizados y se realice de manera controlada. Este dominio contiene varios controles de seguridad de la información, como políticas yprocedimientos de control de acceso, autenticación de usuarios y gestión de privilegios.

- ¿Existe una política de control de acceso documentada y actualizada en la organización que defina los requisitos de acceso a los sistemas y activos deinformación?

- ¿Se asignan roles y responsabilidades a los empleados en función de

su función y se restringe el acceso a la información según el principio de mínimoprivilegio?

- ¿Se implementan medidas de autenticación de usuarios, como contraseñasseguras y autenticación multifactor, para garantizar que solo los usuarios autorizados tengan acceso a los sistemas y la información?

- ¿Se establecen procedimientos formales para otorgar, modificar y revocar el acceso a los sistemas y la información en función de las necesidades del negocio y los cambios en las funciones y responsabilidades de los empleados?

- ¿Se controla y registra el acceso a los sistemas e información crítica para detectar actividades sospechosas o no autorizadas y tomar medidas correctivascuando sea necesario?

- ¿Se realiza una revisión periódica de los derechos de acceso de los empleadospara garantizar que sigan siendo apropiados y se ajusten a las políticas y normas de control de acceso de la organización?

- ¿Se implementan medidas de seguridad para proteger las redes y sistemas de la organización, como firewalls y sistemas de detección de intrusiones, para garantizar que solo los usuarios autorizados tengan acceso a los recursos de lared?

Una organización con un estado de madurez alto en el dominio A.9 demuestra un enfoque sólido y completo para el control de acceso a la información y a los sistemas.

Esto incluye políticas y procedimientos basados en los requisitos de negocio y en los riesgos de seguridad de la información, así como procesos formales para la asignación y revocación de derechos de acceso. Además, se lleva a cabo un monitoreo y una revisión regular de los derechos de acceso otorgados, y se aplican controles de acceso físico y lógico a áreas, sistemas y dispositivos seguros.

Seguridad en entornos de trabajo móvil (A.11.1.5): Establecer políticas y medidas específicas para garantizar la seguridad de la información en entornos de trabajo móvil, incluyendo el uso de dispositivos personales (BYOD (Bring Your Own Device)) y conexiones de red no seguras. Este control se enfoca en asegurar que solo las personas autorizadas tengan acceso a áreas donde se procesa o almacena información sensible.

- ¿Se han identificado y delimitado las áreas de trabajo seguras donde seprocesa o almacena información confidencial o crítica?
- ¿Se han implementado controles de acceso físico, como tarjetas de acceso, cerraduras electrónicas o biométricas, para restringir el acceso a las áreas detrabajo seguras únicamente a personas autorizadas?

- ¿Se han establecido políticas y procedimientos claros para la autorización, elregistro y la revocación del acceso a las áreas de trabajo seguras?

- ¿Se proporciona información y capacitación a los empleados y otras partes interesadas sobre la importancia de mantener un acceso seguro a las áreas detrabajo y las responsabilidades relacionadas?

- ¿Se realizan auditorías y revisiones periódicas de los registros de

acceso a lasáreas de trabajo seguras para garantizar la conformidad con las políticas y procedimientos de la organización?

- ¿Se monitorean y registran las actividades en las áreas de trabajo seguras, como mediante cámaras de seguridad o sistemas de detección de intrusión,para detectar y responder a incidentes de seguridad física?

- ¿Se revisan y actualizan periódicamente las políticas, procedimientos y controles de acceso a áreas de trabajo seguras para garantizar que sigan siendoefectivos y estén alineados con los objetivos de seguridad de la organización?

Una organización con un estado de madurez alto en el control A.11.1.5 demuestraun enfoque sólido y completo para la eliminación segura de equipos que contienen información almacenada. Esto incluye políticas y procedimientos documentados, la identificación y registro de equipos, la realización de procedimientos de eliminación segura, la capacitación del personal responsable y el seguimiento y auditoría de las actividades de eliminación segura.

Adquisición, desarrollo y mantenimiento de sistemas de información (A.14): Se centra en garantizar que la seguridad de la información se integre en todo el ciclo de vidade los sistemas de información, desde su adquisición o desarrollo hasta su mantenimientoy eliminación. Este dominio contiene varios controles de seguridad de la información, como requisitos de seguridad en el desarrollo de sistemas, gestión de vulnerabilidades y protección contra malware.

- ¿Se definen e integran requisitos de seguridad de la información en el procesode adquisición o desarrollo de nuevos sistemas de información?

- ¿Se realiza una evaluación de riesgos para identificar y abordar los riesgos deseguridad de la información asociados con el desarrollo y la adquisición de sistemas de información?

- ¿Se aplican prácticas de desarrollo seguro y se siguen estándares y guías deseguridad en el desarrollo de sistemas de información?

- ¿Se realizan pruebas de seguridad en los sistemas de información durante eldesarrollo y antes de la implementación para identificar y remediar vulnerabilidades y defectos de seguridad?

- ¿Se implementan medidas de protección contra malware, como antivirus,actualizaciones de software y capacitación de empleados para prevenir y detectar ataques de malware?

- ¿Se establecen procedimientos para el mantenimiento y la actualización de lossistemas de información, incluida la aplicación de parches de seguridad y la mitigación de vulnerabilidades conocidas?

- ¿Se monitorizan y registran los eventos de seguridad de la información en lossistemas de información para detectar y responder a incidentes de seguridad de la información?

- ¿Se realizan revisiones periódicas de la efectividad y la adecuación de los controles de seguridad de la información en el dominio A.14 para identificaráreas de mejora y garantizar la madurez continua?

Una organización con un estado de madurez alto en el dominio A.14 demuestra un enfoque sólido y completo para la adquisición, desarrollo y mantenimiento de sistemas de información. Esto incluye políticas y

procedimientos basados en los requisitos de seguridad de la información, evaluaciones de riesgos y análisis de impacto en el negocio, aplicación de controles y técnicas de seguridad, pruebas de seguridad y auditorías, y monitoreo y gestión efectiva de los cambios en los sistemas de información.

Gestión de incidentes de seguridad de la información (A.16): Implementar un proceso eficaz para gestionar y responder a incidentes de seguridad de la información en entornos de teletrabajo, que incluya la identificación, evaluación, respuesta y seguimientode incidentes. Este dominio contiene varios controles de seguridad de la información, como la notificación y clasificación de incidentes, la gestión y la comunicación de incidentes, y la revisión y mejora de la respuesta a incidentes.

- ¿Existe una política de gestión de incidentes de seguridad de la informacióndocumentada y actualizada en la organización que defina los roles, responsabilidades y procedimientos para manejar incidentes?

- ¿Se han establecido procedimientos claros para la notificación y clasificaciónde incidentes de seguridad de la información por parte de los empleados y otras partes interesadas?

- ¿Se ha asignado un equipo o función responsable de la gestión de incidentesde seguridad de la información que tenga la autoridad, el conocimiento y lashabilidades necesarias para abordar incidentes de manera efectiva?

- ¿Se capacita a los empleados sobre la importancia de la notificación de incidentes y sus responsabilidades en la gestión de incidentes de seguridad dela información?
- ¿Se comunican los incidentes de seguridad de la información de

manera adecuada a las partes interesadas internas y externas, según sea necesario, incluyendo la notificación a las autoridades reguladoras cuando corresponda?

- ¿Se implementan medidas para contener, erradicar y recuperarse de incidentesde seguridad de la información, minimizando el impacto y restaurando la operación normal de la organización?

- ¿Se llevan a cabo revisiones y análisis post-incidente para identificar las causas de los incidentes, evaluar la efectividad de la respuesta y mejorar lagestión de incidentes en el futuro?

- ¿Se monitoriza, mide y revisa periódicamente la efectividad y la madurez delproceso de gestión de incidentes de seguridad de la información para garantizar una mejora continua?

Una organización con un estado de madurez alto en el dominio A.16 demuestra un enfoque sólido y completo para la gestión de incidentes de seguridad de la información. Esto incluye políticas y procedimientos documentados, un proceso estructurado y formal para la gestión de incidentes, un equipo de respuesta a incidentes deseguridad de la información (CSIRT) con personal capacitado y recursos adecuados, análisis y evaluaciones periódicas de los incidentes, e implementación de acciones correctivas y preventivas basadas en las lecciones aprendidas.

La adopción de la norma ISO/IEC 27001:2013 en un entorno de teletrabajo puede ayudar a las organizaciones a abordar los riesgos de seguridad de la información de manera proactiva y sistemática, al tiempo que proporciona un marco para la mejora continua de las prácticas de seguridad de la información, este puede aplicarse de manera abierta, es decir a pesar que las organizaciones no estén enfocadas a procesos de certificaciones de la norma, pueden usar

libremente la documentación para implementar parcialmente los controles de seguridad que sean pertinentes a las necesidades y contexto de la organización.

2.3.2 Tipos de amenazas

Las amenazas pueden clasificarse en dos tipos:

Intencionales: en caso de que deliberadamente se intente producir un daño (por ejemplo, el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).

No intencionales: en donde se producen acciones u omisiones de acciones que, si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo, las amenazas relacionadas con fenómenos naturales), (Whitman & Mattord, 2018).

Tabla 1. Tipos de Amenazas

Nombre de los atacantes	Definición
Hackers	Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas, pero sin motivación económica o dañina.
Crackers	Un hacker que, cuando rompe la seguridad de un sistema, lo hace con intención maliciosa, bien para dañarlo o para obtener un beneficio económico.
Phreakers	Crackers telefónicos, que sabotean las redes de telefonía para conseguir llamadas gratuitas.
Sniffers	Expertos en redes que analizan el tráfico para obtener información extrayéndola de los paquetes que se transmiten por la red.
Lammers	Chicos jóvenes sin grandes conocimientos de informática pero que se consideran a sí mismos hackers y se vanaglorian de ello.
Newbie	Hacker novato.
Ciberterrorista	Expertos en informática e intrusiones en la red que trabajan para países y organizaciones como espías y saboteadores informáticos.
Programadores de virus	Expertos en programación, redes y sistemas que crean programas dañinos que producen efectos no deseados en los sistemas o aplicaciones.
Carders	Personas que se dedican al ataque de los sistemas de tarjetas, como los cajeros automáticos.

Fuente**:** Elaboración propia

2.3.3 Riesgos de seguridad en el teletrabajo

El teletrabajo también presenta riesgos de seguridad para las empresas, ya que los datos pueden estar expuestos a amenazas en un ambiente no controlado. Algunos de estos riesgos incluyen, de acuerdo con Kaivanto (2021):

- Acceso no autorizado: Puede haber personas que no sean empleados de laempresa que tengan acceso a la información confidencial, como amigos, familiares u otras personas en el hogar del teletrabajador.

- Dispositivos no seguros: Los dispositivos utilizados por los teletrabajadores pueden no estar actualizados con los parches de seguridad más recientes, lo quepuede permitir la entrada de virus y malware.

- Redes no seguras: Las redes utilizadas por los teletrabajadores pueden serpúblicas o no estar seguras, lo que aumenta el riesgo de que los datos seaninterceptados.

- Amenazas y vulnerabilidades en el teletrabajo: Se debe analizar las posibles amenazas y vulnerabilidades en el teletrabajo, como, por ejemplo, ataques dephishing, malware, robo de información, y la falta de actualizaciones de seguridad.

2.3.4 Protección de Punto Final

Una herramienta de gestión de equipos de punto final (Endpoint Management Tool) es un software o solución que ayuda a las organizaciones a administrar, controlar y proteger de manera centralizada los dispositivos de

punto final, como computadoras portátiles, teléfonos móviles, tabletas y servidores, dentro de una red empresarial. Estas herramientas permiten a las empresas garantizar la seguridad, mantener la conformidad y mejorar la eficiencia operativa al abordar las necesidades de administración y seguridad de una amplia variedad de dispositivos de acuerdo con lo mencionado por Gartner, (2023).

Las herramientas de gestión de equipos de punto final pueden incluir funciones como:

- Administración de dispositivos: Monitoreo, control y actualización de dispositivosde punto final en la red empresarial.

- Gestión de políticas: Implementación y aplicación de políticas de seguridad yconfiguraciones en todos los dispositivos de punto final.

- Administración de aplicaciones: Distribución, actualización y eliminación deaplicaciones en los dispositivos de punto final.

- Seguridad de datos: Protección de datos confidenciales y personales en losdispositivos de punto final.

- Gestión de parches: Actualización de software y aplicaciones en dispositivos depunto final para corregir vulnerabilidades y garantizar la seguridad.

El uso de herramientas de gestión de equipos de punto final es especialmente importante en entornos de teletrabajo, donde los empleados pueden utilizar una variedad de dispositivos personales y corporativos para acceder a la información y los sistemas de la empresa, ENISA, (2020).

La adopción de herramientas de gestión de equipos de punto final puede mejorar la ciberseguridad y la eficiencia operativa en organizaciones que implementan políticas de teletrabajo, permitiendo un control centralizado de dispositivos y la aplicación de políticas de seguridad adecuadas.

Las mejores herramientas de EndPoint Security son aquellas que ofrecen protección completa, facilidad de uso y alta tasa de detección de amenazas. La clasificación de las mejores soluciones puede variar según los criterios utilizados y los estudios realizados, pero aquí hay algunas de las herramientas de EndPoint Security más reconocidas y recomendadas por expertos y organizaciones en ciberseguridad, con citas y referencias recientes:

- CrowdStrike Falcon: CrowdStrike Falcon es una plataforma de protecciónde endpoint basada en la nube que utiliza inteligencia artificial y machine learning para detectar y prevenir amenazas en tiempo real de Gartner (2023).

- Microsoft Defender for Endpoint: Anteriormente conocido como Windows Defender ATP, Microsoft Defender for Endpoint es una solución de seguridad integral que proporciona protección contra malware, vulnerabilidades y amenazasen línea para dispositivos Windows, de acuerdo con la evaluación de Gartner (2023).

- Sophos Intercept X: Sophos Intercept X es una solución de seguridad de endpointque combina técnicas de detección basadas en firmas y machine learning para proteger contra malware, exploits y ransomware, de acuerdo con la evaluación de Forrester (2021).

- Symantec Endpoint Security (SES) de Broadcom: Symantec Endpoint Security esuna solución completa de protección de endpoint que ofrece prevención, detección y respuesta a amenazas a través de una única

plataforma, de acuerdo con la evaluación de Gartner, (2023).

- Trend Micro Apex One: Trend Micro Apex One es una solución de seguridad de endpoint que utiliza técnicas de aprendizaje automático y análisis de comportamiento para proteger contra malware, ransomware y amenazas avanzadas, de acuerdo con la evaluación de Gartner (2023).

- VMware Carbon Black Cloud: VMware Carbon Black Cloud es una plataforma de seguridad de endpoint basada en la nube que ofrece protección en tiempo realcontra malware, exploits y otras amenazas cibernéticas, de acuerdo con la evaluación de Gartner (2023).

Es importante tener en cuenta que la efectividad y las capacidades de las herramientas de EndPoint Security pueden variar según el entorno y las necesidades específicas de cada organización. Por lo tanto, es fundamental evaluar cuidadosamente las características, el rendimiento y la compatibilidad de cada solución antes de seleccionar la más adecuada para su entorno de TI, concordando con lo mencionado por Kshetri (2013).

En relación a estas herramientas, y basados en la experiencia nos alineamos siguiente argumento "Este tipo de herramientas tienen sus ventajas y desventajas las cuales deben ser abordadas de acuerdo al contexto de la organización, su conocimiento puede brindar apoyo a soluciones que tengan un valor en relación costo/beneficio que estén alineados a los objetivos de la organización y las políticas de seguridad establecidas" (Amin, 2017).

3 Desarrollo Metodológico

3.1 Contexto Organizacional

CREASISTEMAS S.A.S., es una empresa que ofrece servicios de tecnología orientados a la consultoría, diseño, desarrollo e implementación de soluciones para la gestión de información enfocados en sistemas de apoyo a la toma de decisiones, gestión de sistemas de bases de datos servicios de outsourcing y fábrica de software.

Cuenta con más de 20 años de trayectoria en el sector de las TIC y actualmente es reconocida por Microsoft como un socio estratégico en el apoyo de implementaciones, soporte y gestión de tecnologías de la misma, por su gran experiencia y confianza. Según Gómez y Contreras (2021), la empresa ABC tiene más de dos décadas de experiencia en el sector de las TIC y es reconocida por su amplio conocimiento y experiencia en el soporte, la implementación y la gestión de tecnologías, siendo un socio estratégico para Microsoft en la región.

Actualmente cuenta con contratos con diferentes organizaciones para apoyar a las áreas de tecnología de diferentes organizaciones y sectores económicos los cuales apoyan a su vez los objetivos organizaciones de estas empresas.

Como se pueden identificar dentro del enfoque de esta investigación, CREASISTEMAS S.A.S. es un referente en la comunidad y apoya con responsabilidad social el desarrollo del sector.

3.2 Tipo y Diseño Metodológico

De acuerdo con el autor Saunders (2019), en un proyecto de

investigación de seguridad de la información, se puede aplicar una metodología de investigación mixta que combine tanto el análisis cualitativo como cuantitativo.

En el análisis cuantitativo, se pueden utilizar herramientas como encuestas o cuestionarios para recopilar datos numéricos y estadísticas sobre la seguridad de la información de los teletrabajadores, lo que ayuda a comprender la seguridad de la información en la empresa.

En el análisis cualitativo, se pueden utilizar técnicas como entrevistas en profundidad y grupos focales para obtener información detallada sobre las experiencias y percepciones de los teletrabajadores con respecto a la seguridad de la información. Una vez obtenidos los datos, se pueden analizar y comparar los resultados de ambas metodologías para obtener una imagen completa de la seguridad de la información en la empresa y hacer recomendaciones para mejorarla, para el desarrollo de estar análisis nos apoyaremos en le norma ISO27001:2013 y las recomendaciones que se proponen en el Anexo A, para establecer la madurez y el estado de implementación de los controles más relevantes asociados al Teletrabajo.

Plan de trabajo para llevar a cabo el análisis de seguridad de la información para los teletrabajadores de CREASISTEMAS:

- **Investigación inicial:** Realizar una revisión de la documentación actual de seguridad de la información de CREASISTEMAS y recopilar información sobrela modalidad de teletrabajo utilizada por la empresa y los dispositivos y redes utilizados por los colaboradores.

- **Identificación de riesgos**: Realizar una evaluación de riesgos para la seguridad dela información de los dispositivos utilizados por los colaboradores en la modalidad de teletrabajo, identificando los posibles vectores de ataque y las vulnerabilidades de seguridad. Documentar y

priorizar los riesgos identificados.

- **Evaluación de políticas de seguridad:** Realizar una evaluación de las políticas deseguridad de la información actuales de CREASISTEMAS y determinar si estánadaptadas a la modalidad de teletrabajo, identificando posibles brechas o lagunasen la política de seguridad actual de la empresa.

- **Diseño e implementación de soluciones técnicas**: Diseñar e implementar medidastécnicas de seguridad de la información, como el uso de soluciones de endpoint protección, la implementación de políticas de acceso y autenticación, y la configuración de redes privadas virtuales (VPN), que permitan mitigar los riesgosidentificados y garantizar el cumplimiento de las políticas de seguridad de la información establecidas por la empresa.

- **Plan de concientización y capacitación:** Elaborar un plan de concientización y capacitación en seguridad de la información para los colaboradores que trabajanen la modalidad de teletrabajo, enfocado en la importancia de la seguridad de la información, la identificación de amenazas y la implementación de buenasprácticas de seguridad.

- **Evaluación y seguimiento**: Realizar evaluaciones periódicas para medir la efectividad de las medidas implementadas y hacer ajustes según sea necesario.Documentar el progreso y el impacto de las medidas de seguridad de la información implementadas.

- **Informe final**: Elaborar un informe final que incluya una descripción detallada delos riesgos identificados, las medidas de seguridad de la información implementadas, los resultados de las evaluaciones periódicas y cualquier recomendación para futuras mejoras. Presentar el

informe a los responsables de laempresa y discutir los próximos pasos.

3.3 Participantes y Fuentes de Datos

De acuerdo con las reuniones previas con la Gerencia de CREASISTEMAS S.A.S. se determinó que el alcance de la presente investigación abordara a uno de los equipos de trabajo de uno de los proyectos más importantes de la empresa, como muestrarepresentativa de sus actividades.

El equipo de trabajo de este proyecto está compuesto por:

- Gerente de CREASISTEMAS.A.S.
- Responsable de Seguridad de la Información
- Responsable de Tecnología
- Equipo Administrativo y Apoyo Operativo
- Coordinador Líder Equipo de Desarrollo Soluciones de Software
- Coordinador Líder de Soporte Base de Datos
- Coordinador Líder de Soporte Administración de Plataforma
- Administradores de Plataforma Nube y Local
- Administradores de Base de Datos
- Analistas de Desarrollo

La población está compuesta de aproximadamente 45 colaboradores, de áreasadministrativas y de apoyo. Otras fuentes de datos que se usaran para el desarrollo del proyecto se basaran:

- Entrevistas personales
- Encuesta formato MS FORMS “Estado Seguridad de la Información SoluciónTeletrabajo CREASISTEMAS S.A.S”
- Lista de Chequeo ISO27001:2013 Anexo A.

3.4 Análisis Encuestas y Estadísticas

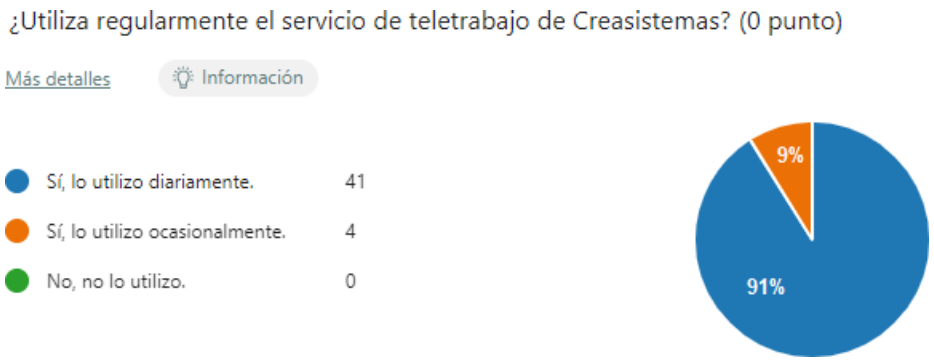
La población total es de 200 colaboradores y deseamos un nivel de confianza del 95%.

El margen de error para una encuesta de 45 personas de una población total de 200 colaboradores es del 14% con un nivel de confianza del 95%. Esto significa que los resultados de la encuesta pueden variar en ± 14% en relación con la proporción real en la población total.

Si desea reducir el margen de error, puede aumentar el tamaño de la muestra o disminuir el nivel de confianza. Sin embargo, esto puede requerir más tiempo y recursospara llevar a cabo la encuesta. Por otro lado, si está dispuesto a aceptar un margen de error mayor, podría disminuir el tamaño de la muestra o aumentar el nivel de confianza.

De acuerdo con la encuesta realizada a continuación presentamos los resultadostabulados.

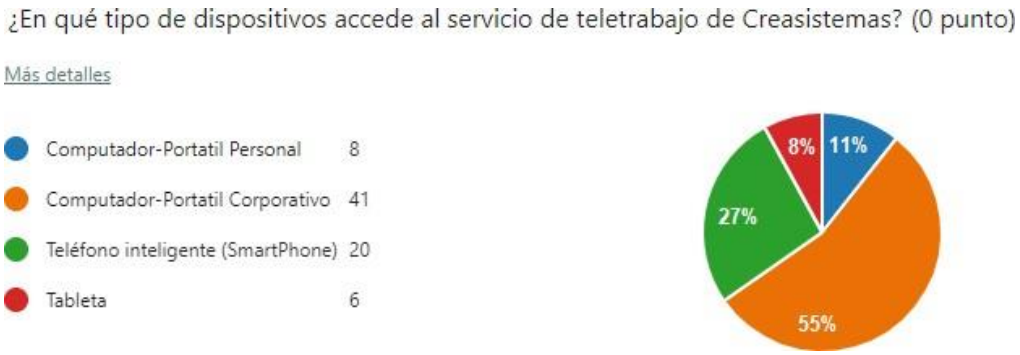
Ilustración 4. Utilización Servicio Teletrabajo en CREASISTEMAS



Fuente: Elaboración Propia

Según los resultados el 91% de los colaboradores si utilizan diariamente elservicio de teletrabajo contra un solo 9% de colaboradores que si lo utilizan ocasionalmente.

Ilustración 5. En qué tipo de dispositivos accede al servicio de teletrabajo



Fuente: Elaboración propia

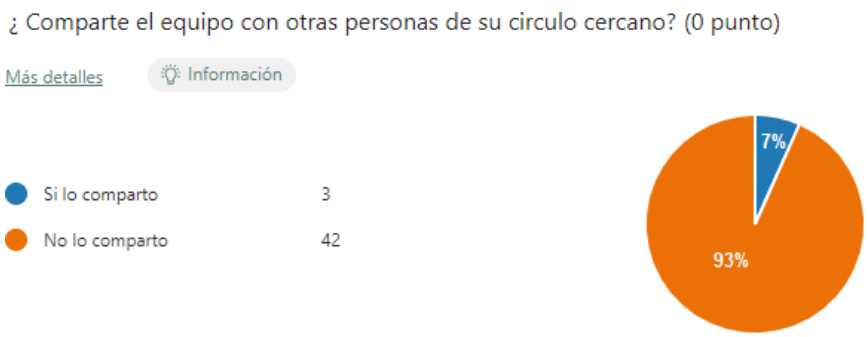
En respuesta al tipo de dispositivo con el que mayor frecuencia acceden al servicio de teletrabajo los colaboradores en CREASISTEMAS es el Computador- PortátilCorporativo con un 55%, después continua con un 27% el Teléfono inteligente (Smartphone), le sigue con un 11% el Computador-Portátil Personal y finalmente el dispositivo Tableta con un 8%.

Ilustración 6. Conexiones seguras para el ingreso al servicio de teletrabajo

Fuente: Elaboración Propia

En el uso de las conexiones seguras muestra una tendencia a ser manejadas todas casi por igual, iniciando con la más utilizada con un 29% el escritorio virtual, seguida con un 28% la herramienta de colaboración digital y después seguimos con un 24% la VPN corporativa, finalmente con un 19% las herramientas de gestión remota web.

Ilustración 7. Comparte el equipo con otras personas cercanas



Fuente**:** Elaboración Propia

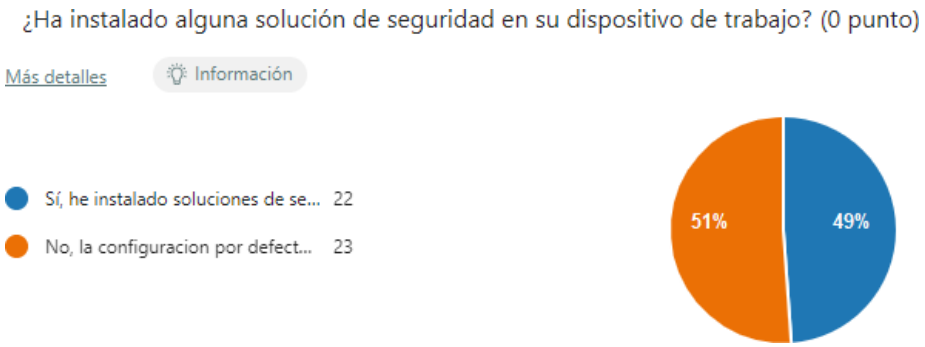
Se ha encontrado un buen proceder de los colaboradores de no utilizar los equipos de trabajo para realizar funciones personales y con un resultado del 93% que no comparten su dispositivo de trabajo y un 7% que si lo comparten.

Ilustración 8. Ha compartido su contraseña

Fuente**:** Elaboración Propia.

En esta pregunta se evidencia que tienen casi todos muy clara las políticas de seguridad de la información ya que el 93% de los colaboradores nunca han compartido su contraseña contra un 7% que si la han compartido.

Ilustración 9. Ha instalado alguna solución de seguridad en el dispositivo



Fuente: Elaboración Propia.

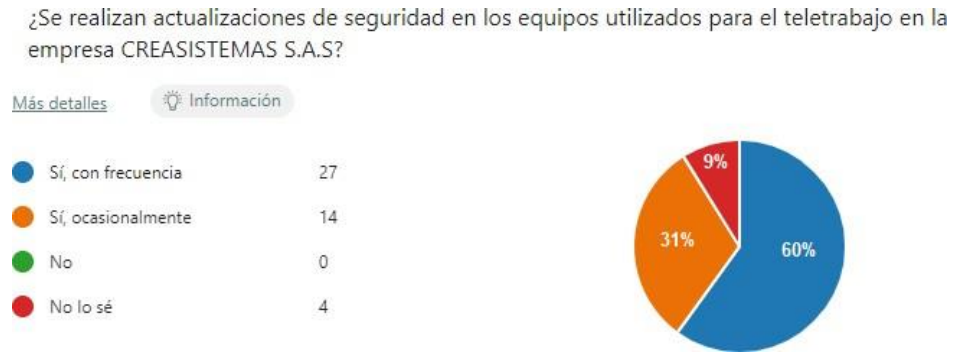
Según el resultado el 51% de los colaboradores utilizan la solución de seguridad que les brinda la empresa y un 49% si han instalado alguna otra solución adicional.

Ilustración 10. CREASISTEMAS cuenta con políticas claras de seguridad para el teletrabajo

Fuente: Elaboración Propia

La percepción de la mayoría de los colaboradores es de un 71% ante si la empresa tiene políticas claras de seguridad contra un 22% que no lo sabe y un 7% dicen que no.

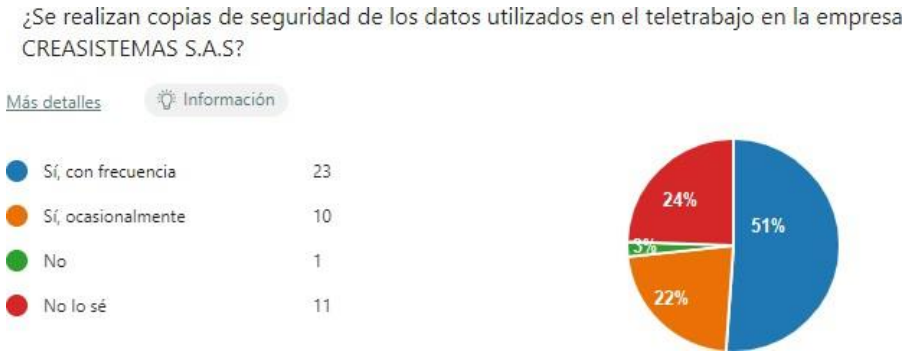
Ilustración 11. Se realizan actualizaciones de seguridad en los equipos para el teletrabajo



Fuente**:** Elaboración Propia

En esta pregunta se evidencia que un alto número de colaboradores se preocupan de realizar las actualizaciones de seguridad en sus equipos con un 60% de afirmación contra un 31% que lo hace ocasionalmente y 9 que no lo sabe.

Ilustración 12. Se realizan copias de seguridad de los datos en el teletrabajo



Fuente: Elaboración Propia

Con los resultados obtenidos el 51% de los colaboradores realizan copias de seguridad de sus datos, el 24% no lo saben, un 22 lo hacen ocasionalmente y un 3% no lo hacen.

Ilustración 13. Se han producido incidentes de seguridad relacionados con el teletrabajo

Fuente**:** Elaboración Propia

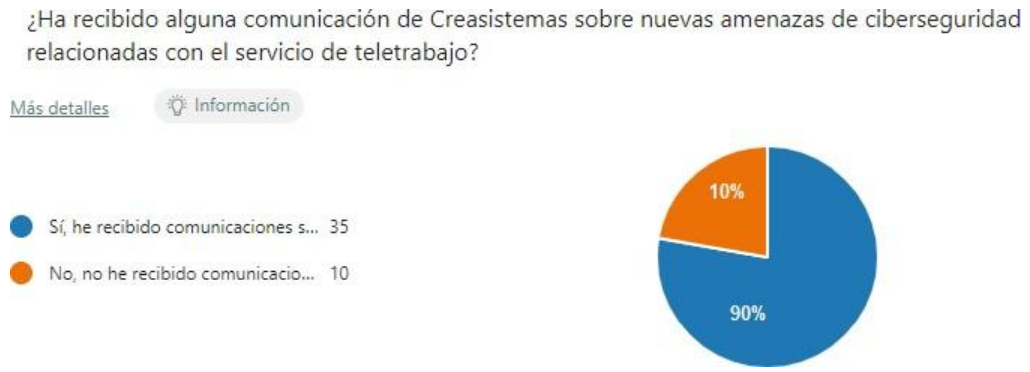
El 36% de los colaboradores aseguran haber tenido un incidente de seguridad en el teletrabajo contra 38% que asegura que no han tenido un incidente de seguridad y finalmente un 26% que no lo saben.

Ilustración 14. La empresa proporciona formación en seguridad

Fuente**:** ElaboraciónPropia

En esta respuesta tenemos el 47% de los colaboradores que dicen que han recibido con frecuencia una formación en seguridad para el teletrabajo, y otro 47% de ellos dicen que si la han recibido ocasionalmente y un 6% no lo saben.

Ilustración 15. Ha recibido alguna comunicación de nuevas amenazas



Fuente**:** Elaboración Propia.

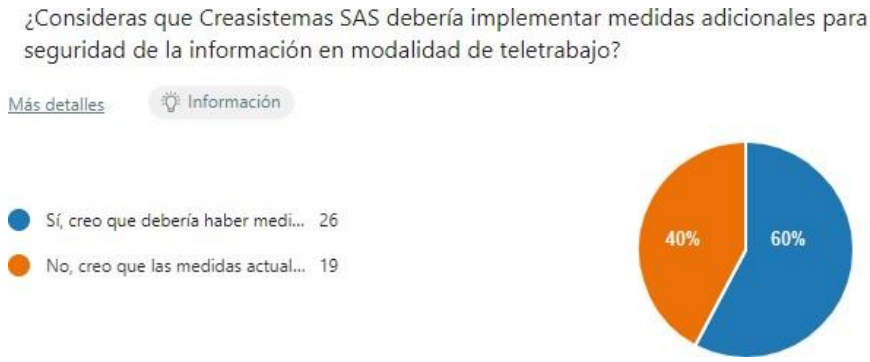
Según la encuesta el 90% de los colaboradores han recibido comunicaciones sobre nuevas amenazas por parte de CREASISTEMAS contra un 10% que asegura que no han recibido un comunicado.

Ilustración 16. Cuál es tu opinión sobre la seguridad de la solución del teletrabajo

Fuente**:** Elaboración Propia

Se puede evidenciar que un 58% de los colaboradores piensan que la seguridad que ofrece CREASISTEMAS para la solución del Teletrabajo es buena, y un 40% están algo seguros de que es buena la seguridad contra un 2% que dicen que es poca segura.

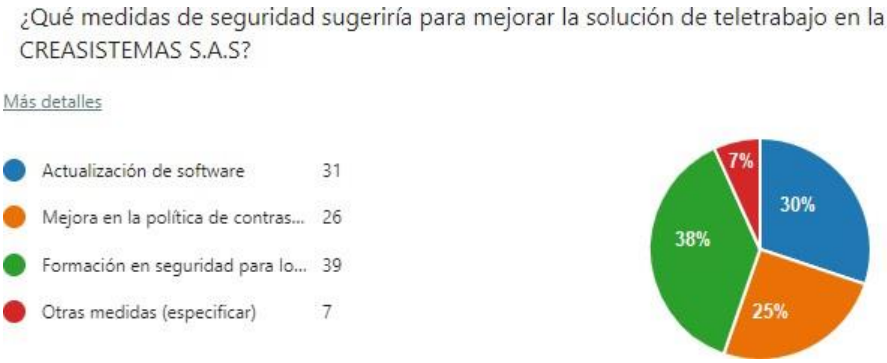
Ilustración 17. Considera que se debe de implementar medidas de seguridad adicionales



Fuente**:** Elaboración Propia

Un 60% de los colaboradores consideran que se debe de implementar nuevas medidas de seguridad en la modalidad de teletrabajo contra un 40% que considera que las medidas que tiene CREASISTEMAS son suficientes para el ámbito de teletrabajo.

Ilustración 18. Que medidas de seguridad sugeriría para mejorar el teletrabajo



Fuente**:** Elaboración Propia

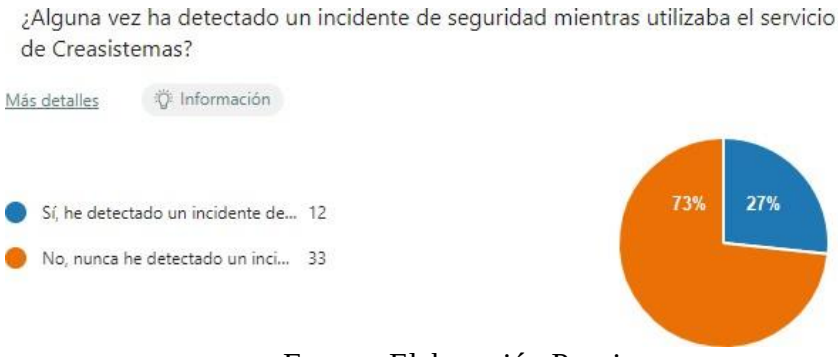
En respuesta a esta pregunta un 38% de los colaboradores consideran que la mejor medida que se puede mejorar para la seguridad en el teletrabajo es la formación en seguridad para los trabajadores, seguido del 30% que consideran que la actualización de software se puede mejorar y no se puede dejar con un 25% la mejora de la política de contraseñas y finalizando con un 7% otras medidas.

Ilustración 19. Cree que existen suficientes medidas de seguridad para el teletrabajo

Fuente: Elaboración Propia.

La percepción del 90% de los colaboradores es de que la empresa CREASISTEMAS cuenta con suficientes medidas de seguridad para el teletrabajo contra un 10% que dicen creer que es necesario más medidas de seguridad.

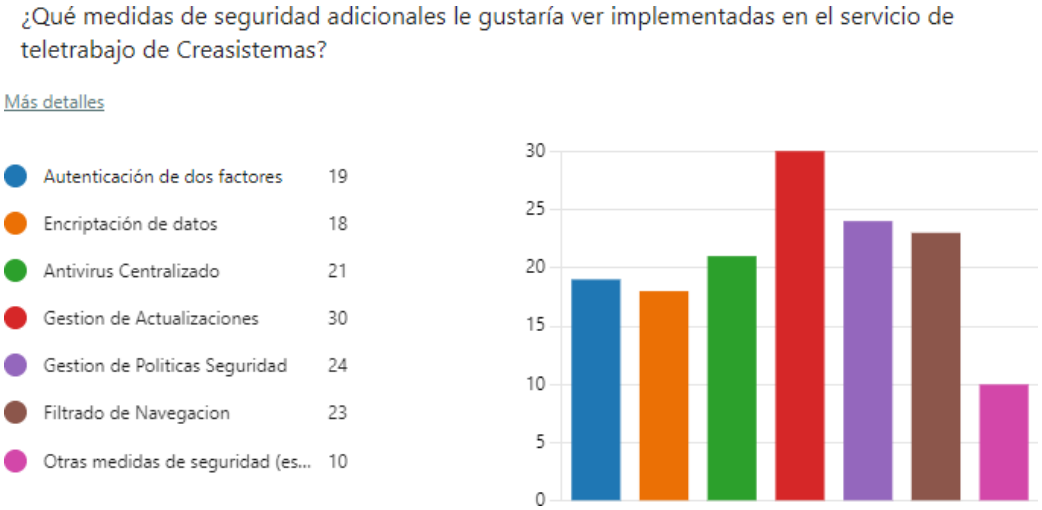
Ilustración 20. Alguna vez han detectado un incidente mientras utilizan el teletrabajo



Fuente**:** Elaboración Propia.

Se evidencia que un 73% de los colaboradores no han detectado un incidente de seguridad mientras utilizan el teletrabajo contra un 27% que si lo han detectado.

Ilustración 21. Medidas adicionales para implementar en el teletrabajo



Fuente**:** ElaboraciónPropia

Analizando las respuestas de los colaboradores ellos evidencian que se debe mejorar las medidas sobre la gestión de actualizaciones de los equipos seguido de la gestión de políticas de seguridad y el filtrado de navegación, siendo estas las 3 medidas más calificadas.

Ilustración 22. Tiene definida una política de seguridad para el uso de dispositivos en el teletrabajo

Fuente**:** Elaboración Propia

Y como última pregunta de la encuesta tenemos un 78% de los colaboradores tienen bien definida la política de seguridad que implementa CREASISTEMAS para el uso de los dispositivos en el teletrabajo.

3.5 Cronograma y Presupuesto

Para realizar el desarrollo del proyecto de investigación se realizó una estimación de recursos basados en la triple restricción costo, tiempo y alcance.

Se determinó una estructura de desglose de trabajo para realizar la gestión del desarrollo del proyecto, y las dependencias de las tareas, de acuerdo con cada entregable establecido, de acuerdo con cada una de las etapas definidas para la ejecución del mismo.

Se acordó con la gerencia de CREASISTEMAS que la participación de los colaboradores del equipo de trabajo sería parcial, debido a que estaría enfocado a momentos específicos en los cuales serían consultados y

entrevistados para no afectar sus asignaciones diarias de trabajo. Facilitando así con el compromiso de la organización los espacios de trabajo acotados para alcanzar los objetivos del proyecto.

Tabla 2. Cronograma ejecución proyecto de investigación

Nombre de tarea	Duración	Comienzo	Fin
Hito 1 - Planificación de la auditoría	**15 días**	**lun 12/12/22**	**vie 30/12/22**
Identificación de objetivos y alcance de laauditoría	3 días	lun 12/12/22	mié 14/12/22
Selección del equipo auditor y asignación de roles	3 días	jue 15/12/22	lun 19/12/22
Revisión de normativas y estándares aplicables (ISO27001)	3 días	mar 20/12/22	jue 22/12/22
Desarrollo del cronograma y asignación de recursos	3 días	vie 23/12/22	mar 27/12/22
Comunicación a las partes interesadas sobre laauditoría	3 días	mié 28/12/22	vie 30/12/22
Hito 2: Evaluación preliminar y recolección de información	**16 días**	**lun 2/01/23**	**lun 23/01/23**
Revisión de políticas y procedimientos de la organización	3 días	lun 2/01/23	mié 4/01/23
Identificación de sistemas, aplicaciones y procesoscríticos	3 días	vie 6/01/23	mar 10/01/23
Realización de entrevistas y cuestionarios alpersonal clave	3 días	mié 11/01/23	vie 13/01/23
Recopilación de evidencia documental y registros	3 días	lun 16/01/23	mié 18/01/23
Análisis preliminar de riesgos y vulnerabilidades	3 días	jue 19/01/23	lun 23/01/23
Hito 3: Pruebas de auditoría y evaluación decontroles	**18 días**	**mar 24/01/23**	**jue 16/02/23**
Evaluación de controles de seguridad física yambiental	3 días	mar 24/01/23	jue 26/01/23
Pruebas de acceso, autenticación y autorización ensistemas y aplicaciones	3 días	vie 27/01/23	mar 31/01/23
Evaluación de la gestión de parches y actualizaciones de software	3 días	mié 1/02/23	vie 3/02/23
Análisis de cumplimiento de políticas y procedimientos de la organización	3 días	lun 6/02/23	mié 8/02/23
Pruebas de resiliencia y continuidad del negocio	3 días	jue 9/02/23	lun 13/02/23
Evaluación de protección de datos y privacidad	3 días	mar 14/02/23	jue 16/02/23
Hito 4: Análisis de resultados y elaboración deinformes	**15 días**	**vie 17/02/23**	**jue 9/03/23**
Análisis y clasificación de hallazgos y riesgos identificados	3 días	vie 17/02/23	mar 21/02/23
Elaboración de recomendaciones y planes deacción	3 días	mié 22/02/23	vie 24/02/23
Redacción del informe de auditoría preliminar	3 días	lun 27/02/23	mié 1/03/23
Revisión y validación del informe con las partesinteresadas	3 días	jue 2/03/23	lun 6/03/23
Elaboración del informe de auditoría final	3 días	mar 7/03/23	jue 9/03/23
Hito 5: Presentación de resultados y seguimiento	**15 días**	**vie 10/03/23**	**jue 30/03/23**
Presentación de resultados a la dirección y partesinteresadas	3 días	vie 10/03/23	mar 14/03/23

Definición de responsables y plazos para implementar acciones correctivas	3 días	mié 15/03/23	vie 17/03/23
Establecimiento de un plan de seguimiento ymonitoreo	3 días	lun 20/03/23	mié 22/03/23
Comunicación de conclusiones y leccionesaprendidas al equipo auditor	3 días	jue 23/03/23	lun 27/03/23
Cierre formal de la auditoría	3 días	mar 28/03/23	jue 30/03/23

Fuente: Elaboración propia

Adicionalmente se determinaron unos costos relativos, a la ejecución de las actividades basados un presupuesto, basado en horas para la documentación y ejecución de las actividades de los investigadores, tomando como valor de referencia por hora de $20.000 pesos, moneda corriente.

Estos costos solo se tienen encuentra dentro de la estimación de ejecución, no implica compromisos contractuales o prestaciones económicas por ninguna de las partes, porque hacer parte de un ejercicio de estimación.

Tabla 3. Presupuesto ejecución proyecto investigación

ACTIVIDADES	Detalle	Horas	Pers.	Valor
Cronograma y presupuesto	Definición del cronograma con cada una de sus actividades.	5	1	$ 100.000
Marco de referencia	Definición del marco de referencia.	12	2	$ 480.000
Estado del arte	Realizar la definición del estado del arte.	30	2	$ 1.200.000
Enfoque y estudio de investigación		10	3	$ 600.000
Recolección de datos y aplicaciónde herramientas	Realizar la recolección de los datos a realizar en la ejecución del proyecto.	40	1	$ 800.000
Análisis de información	Realizar el análisis de los hallazgos durante la recolección de datos.	15	1	$ 300.000
Revisión de riesgos y estándares de seguridad para los servidores	Analizar los riesgos detectados.	10	2	$ 400.000
Evaluación de las vulnerabilidades encontradas	Realizar la evaluación de las vulnerabilidades.	15	2	$ 600.000
Estructuración esquema de seguridad	Estructurar el esquema de seguridad para de las vulnerabilidades detectadas.	15	3	$ 900.000
Resultados de la aplicación de la metodología.		10	2	$ 400.000
Conclusiones y recomendaciones		10	1	$ 200.000
Entrega de trabajo y entregables		3	3	$ 180.000
		175		$ 6.160.000

Fuente: Elaboración propia.

4 Resultados y Discusiones

Basándse en las evidencias identificadas, el contexto de la organización y el estado actual de los riesgos de seguridad de la información, se realizó la entrega de un informe final a la gerencia de CREASISTEMAS, con el objetivo de dar continuidad a la mejora continua de sus procesos de seguridad de la información y la implementación de controles que permitan en el tiempo mantener un estado deseable y aceptable, para abordar los retos actuales.

Es importante resaltar que el estado actual, es cambiante en relación al tiempo, los desarrollos tecnológicos, nuevas vulnerabilidades de seguridad de la información, características por que determinan que este ejercicio debe realizarse periódicamente, se sugiere que por lo menos 2 veces al año, o máximo una vez al año se actualicen los documentos, procedimientos, controles, evidencias y herramientas asociadas, al ejercicio con el fin de estar preparados frente a una situación de riesgo que permita abordar de una manera adecuada la gestión de los riesgos de seguridad de la información.

CREASISTEMAS S.A.S. en el marco del proceso de certificación para la norma ISO27001:2013, establecerá internamente los planes de trabajo necesarios para abordar los hallazgos entregados en el informe, y estará comprometido en fortalecer su posición frente a las vulnerabilidades de seguridad identificadas, y la gestión de riesgos asociados sobre las mismas.

5 Conclusiones

El trabajo de investigación propuesto, soluciono los objetivos planteados y resolvió la pregunta problema; la empresa CREASISTEMAS S.A.S. ha estado madurando su postura de seguridad y ha venido con el tiempo implementando los controles de seguridad pertinentes para migrar sus conexiones de VPN Cliente a Sitio, por herramientas integradas a esquemas de seguridad más robustos y a adecuado al contexto de actual, mediante la gestión de accesos basados en roles, y la reducción de permisos basados en servicios y protocolos, la implementación múltiples factores de autenticación para la identificación de los usuarios en las aplicaciones, monitoreo y control de las vulnerabilidades de seguridad a nivel de servidores y estaciones de trabajo de punto final, han logrado mitigar los riesgos en el Teletrabajo.

Con este investigación CREASISTEMAS S.A.S. ha logrado identificar nuevos riesgos y herramientas que puede contribuir a su postura de seguridad, al igual que la actualización de la documentación requerida para su proceso de certificación a ISO / IEC 27001:2013, procedimientos, políticas, procedimientos, es un camino por recorrer y de mejora continua, el estado actual será una instantánea para comparar a futuro con nuevos procesos de auditorías internas, que permitan identificar de manera correcta si el modelo de mejora continua ha permitido evolucionar sus procesos de seguridad de la información y alcanzar el proceso de certificación a corto plazo, se recomendó a la empresa CREASISTEMAS S.A.S. realizar este proceso de manera periódica, de manera interna, teniendo en cuenta que los riesgos de hoy continuaran evolucionando al igual que las tecnologías, y requiere de la misma forma de la mejora continua en el plan de seguridad de la información.

Es importante resaltar que se han incorporado de manera correcta los factores claves para la implementación de la norma ISO/IEC 27001:2013, como lo mencionamos en el desarrollo de nuestra investigación, es una responsabilidad social y de ejemplo desarrollar este tipo de investigaciones, aplicadas a las empresas en Colombia, con el fin de contribuir en la construcción del conocimiento y el desarrollo de una cultura de seguridad informática y ciberseguridad, entendiendo que todo hacemos parte de un ecosistema social y fortalecer la postura personal, de las organizaciones del sector privado y sus interacciones permitan un ecosistema más seguro para todos.

Desde nuestra perspectiva como investigadores, podemos evidenciar que la seguridad de la información en las organizaciones debe abordarse desde diferentes frentes de trabajo, no es suficiente abordar la gestión de riesgos dejando atrás los procesos de gestión general de la seguridad de la información. Si bien es cierto que el área de TI abandera en las organizaciones muchas actividades de seguridad, por la implementación de las soluciones de TI de Seguridad Informática, es importante el apoyo del equipo de seguridad de la información que facilite la interacción con los procesos de la organización para tener una mayor visual de la gestión de riesgos, y asi mismo abordar los procesos de mejora continua pertinentes que le den vida a la misma gestión, realizando actividades de monitoreo, control, mejora continua, actualización de políticas, procedimiento, mejora continua. La norma ISO/IEC 27001:2013 facilita la implementación y el control de las actividades de gestión de riesgos, entre más detallado se tenga en una organización cada uno de los procesos y controles, facilitara determinar de una mejor forma la madurez de la organización frente a su postura de seguridad.

Consideramos que el factor más importante en seguridad de la información, no solo debe basarse en la triada de la información, la confidencialidad, integridad, y disponibilidad de nuestros sistemas de información, y la continuidad de la operación de los mismos, debe ser

apalancada por seres humanos que realizan a gestión de los riesgos, que identifican y reconocen las necesidades de las organizaciones, y dando cierre a nuestra ponencia, la formación continua de las personas, habilitan nuevas capacidades, las cuales no son estáticas y generan una dinámica en el entorno. Cada día las tecnologías van avanzando, nuevas herramientas, y nuevos servicios que implican que de manera responsable estemos continuamente informándonos y participando en esa dinámica continua de aprendizaje, de gestión de los riesgos, basados en los objetivos de la organización, apoyados en la mejora continua se puede garantizar el éxito para abordar las nuevas necesidades.

Como profesionales en seguridad de la seguridad de la información el teletrabajo es una preocupación que cobra mayor relevancia debido a la creciente tendencia de las empresas a adoptar esta modalidad de trabajo y cómo la llegada de la pandemia del COVID-19 aceleró esta tendencia, lo que significa que muchas empresas se vieron obligadas a adoptar la modalidad de teletrabajo sin tener políticas de seguridad debidamente establecidas, procedimientos adecuados, infraestructura, capacidad operativa y recurso humano para garantizar la continuidad del negocio y asegurar la protección de la información confidencial, y con la variedad de dispositivos que permiten interconectarnos es un foco de atención importante al cual se le debe prestar mucha atención así como resguardamos nuestras redes internas.

6 Referencias

Álvarez Sosa, Y. M. (2013). Diseño de una Metodología para el Análisis de Riesgo en los Sistemas de Gestión de Seguridad de Información (Marisgsi) [Tesis de maestría, Universidad Centroccidental "Lisandro Alvarado"].

Amin, M. B., Malik, H., & Amin, M. B. (2017). Security Challenges and Solutions in the Internet of Things (IoT): A Comprehensive Review. Journal of Network and Computer Applications, 88, 10-28. https://www.researchgate.net/publication/365349394_Security_Challenges_and_Solutions_in_Internet_of_Things_IoT_A_Review

Arévalo Morales, A. D., & Buitrago Ropero, C. A. (2022). Análisis de ciberseguridad sobre las vulnerabilidades que se pueden presentar con el teletrabajo.

Benjumea-Arias, M. L., Villa-Enciso, E. M., & Valencia-Arias, J. (2016). Beneficios e impactos del teletrabajo en el talento humano. Resultados desde una revisión de literatura (Benefits and Impacts of Telework in Human Talent Results from a Literature Review). Revista Cea, 2(4).

Camacho, J., Castañeda, J., & Navarro, A. (2020). "Impacto del teletrabajo en la satisfacción laboral de los empleados en Bogotá durante la pandemia COVID-19". Revista Espacios, 41(48). Recuperado de: http://www.revistaespacios.com/a20v41n48/a20v41n48p14.pdf

Chavez, S (s/f). El trabajo en casa: Su evolución en la crisis por la covid-19. Oas.org. Recuperado el 14 de abril de 2023, de https://www.oas.org/en/sedi/dhdee/labor_and_employment/documentos/TRABAJO/20CIMT/VMWGS/Presentacion_Colombia.pdf

Congreso de la República de Colombia. (2008). "Ley 1221 de 2008". Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1221_2008.html

ENISA (European Union Agency for Cybersecurity). (2020). " Tips for cybersecurity when working from home". Recuperado de: https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

Forrester. (2021). "The Forrester Wave: Endpoint Security Software as a Service, Q2 2021". Recuperado de: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE53ZzH

Gartner. (2023). "Market Guide for Unified Endpoint Management Tools". Recuperado de: https://www.gartner.com/reviews/market/unified-endpoint-management-tools

Gómez, A., & Contreras, J. (2021). Gestión de riesgos en la seguridad de la información de las pymes. En M. Hernández & S. Sánchez (Eds.), Ciberseguridad y protección de datos personales en el ámbito empresarial (pp. 47-62). Editorial Universidad de Granada.

Innovation at Work. (2020, noviembre 23). How the COVID-19 pandemic is impacting cyber security worldwide. IEEE Innovation at Work; IEEE. https://innovationatwork.ieee.org/how-the-covid-19-pandemic-is-impacting-cyber-security-worldwide/

ISO/IEC. (2013). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. Recuperado de: https://www.iso.org/standard/54534.html

Kim Kaivanto: Autor del estudio "Telework cybersecurity risks and risk management" (2021), que examina los riesgos de seguridad en el teletrabajo y cómo pueden abordarse a través de políticas y tecnologías de seguridad.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 38(9), 817-834. https://ideas.repec.org/a/eee/telpol/v37y2013i4p372-386.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). "Estudio de Teletrabajo en Colombia 2020". Recuperado de: https://www.mintic.gov.co/portal/715/articles-179742_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). "Estudio de Teletrabajo en Colombia 2020". Recuperado de: https://www.teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf

Ramirez, M.B., (2016). “Medición de madurez de CiberSeguridad en MiPymes colombianas” Recuperado de: https://repositorio.unal.edu.co/bitstream/handle/unal/57956/80245271.2016.pdf?sequence=1&isAllowed=y

Ramírez Velásquez, J. C., Vega Abad, C. R., & Narcisa Villagómez, M. (2022). Ventajas y desventajas del teletrabajo en Sudamérica frente a la pandemia del covid-19. Civilizar Ciencias Sociales y Humanas, 22(42).

Morales, Ropero, (2022). Análisis De Ciberseguridad Sobre Las Vulnerabilidades Que Se Pueden Presentar Con El Teletrabajo Recuperado de :

https://repository.libertadores.edu.co/bitstream/handle/11371/5405/Arevalo_Buitrago_2022.pdf?sequence=1&isAllowed=y

Ospina Díaz, M. R., & Sanabria Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad, 62(2), 199-217. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

Presidencia de la República. (2015). Decreto 1072 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=72173

Rodríguez, M. A. (2021). El Teletrabajo en tiempos de la pandemia por Covid-19 en Colombia, una alternativa que llego para quedarse. Recuperado de: https://repository.ucatolica.edu.co/entities/publication/f7b86a8e-2964-4f7c-ad25-9f69f64e08b7

Roy, P. P. (2020). A High-Level comparison between the NIST cyber security framework and the ISO 27001 information security standard. 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 1–3.

Sánchez Castillo, C. R., Gavilán Ordóñez, M. C., & Mateus Gutiérrez, M. Á. (2022). Buenas prácticas en seguridad de la información para el teletrabajo en Colombia.

Saunders, M. N., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students (8th ed.). Pearson Education Limited.

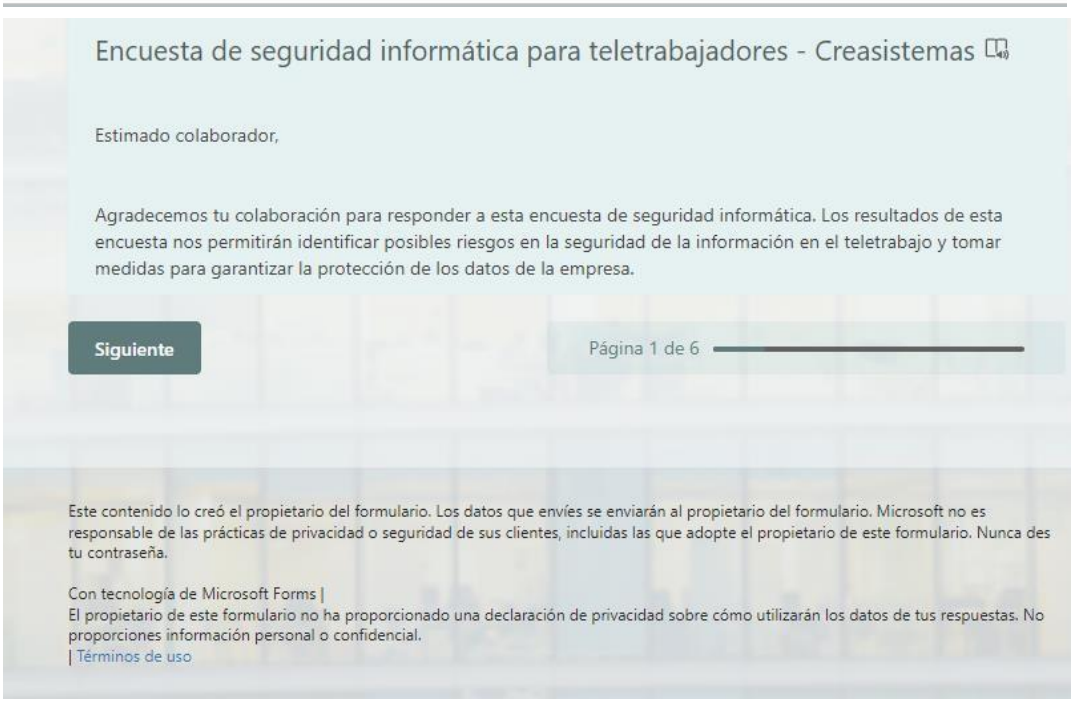
Souppaya, M., & Scarfone, K. (2016). "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security". NIST Special Publication 800-46 Revision 2. Recuperado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

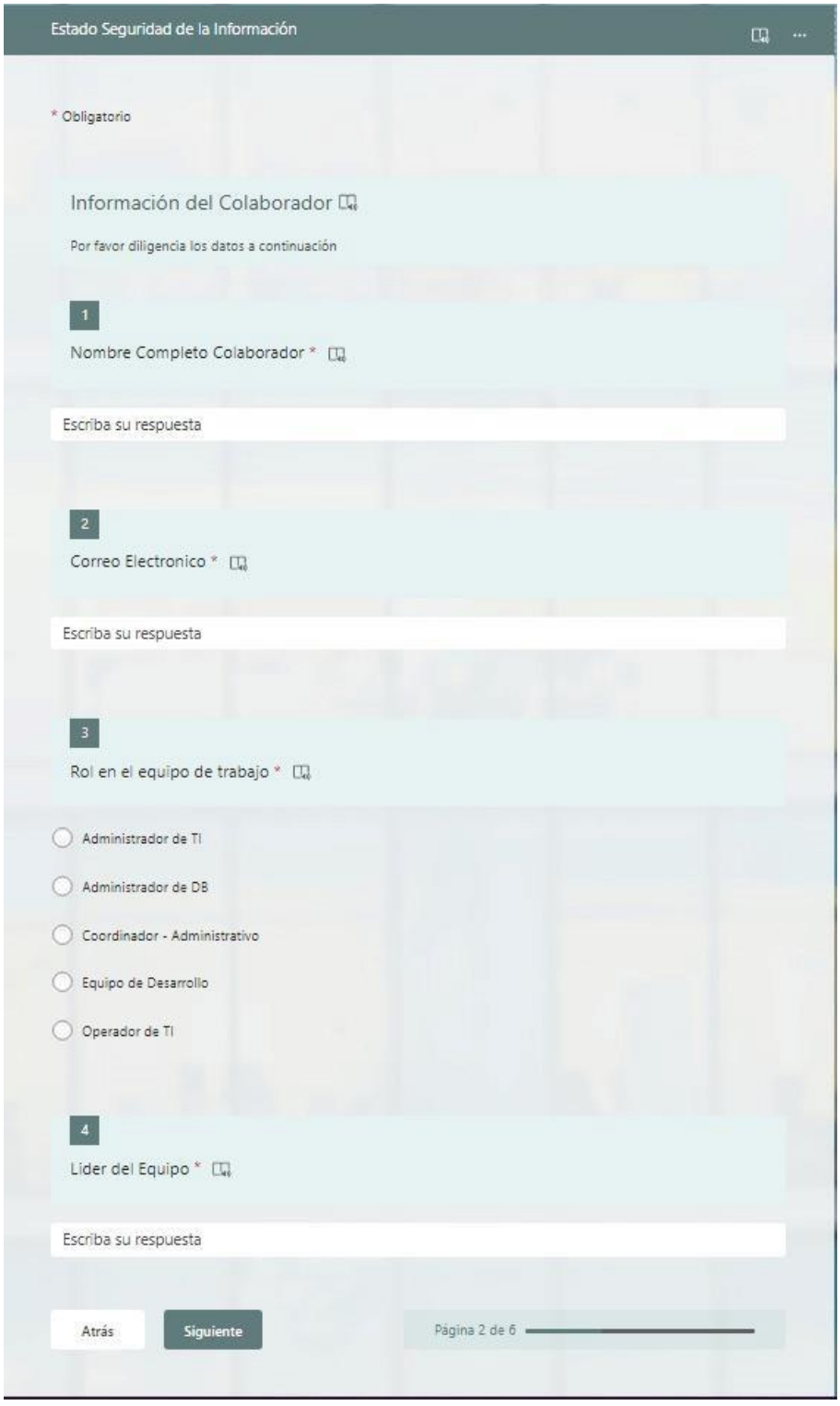
Vásquez Gaona, K. del R. (2013). Aplicación de la metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información Aplicado a la Empresa Pesquera e Industrial Bravito S. A. en la Ciudad de Machala [Tesis de pregrado, Universidad Politécnica Salesiana].

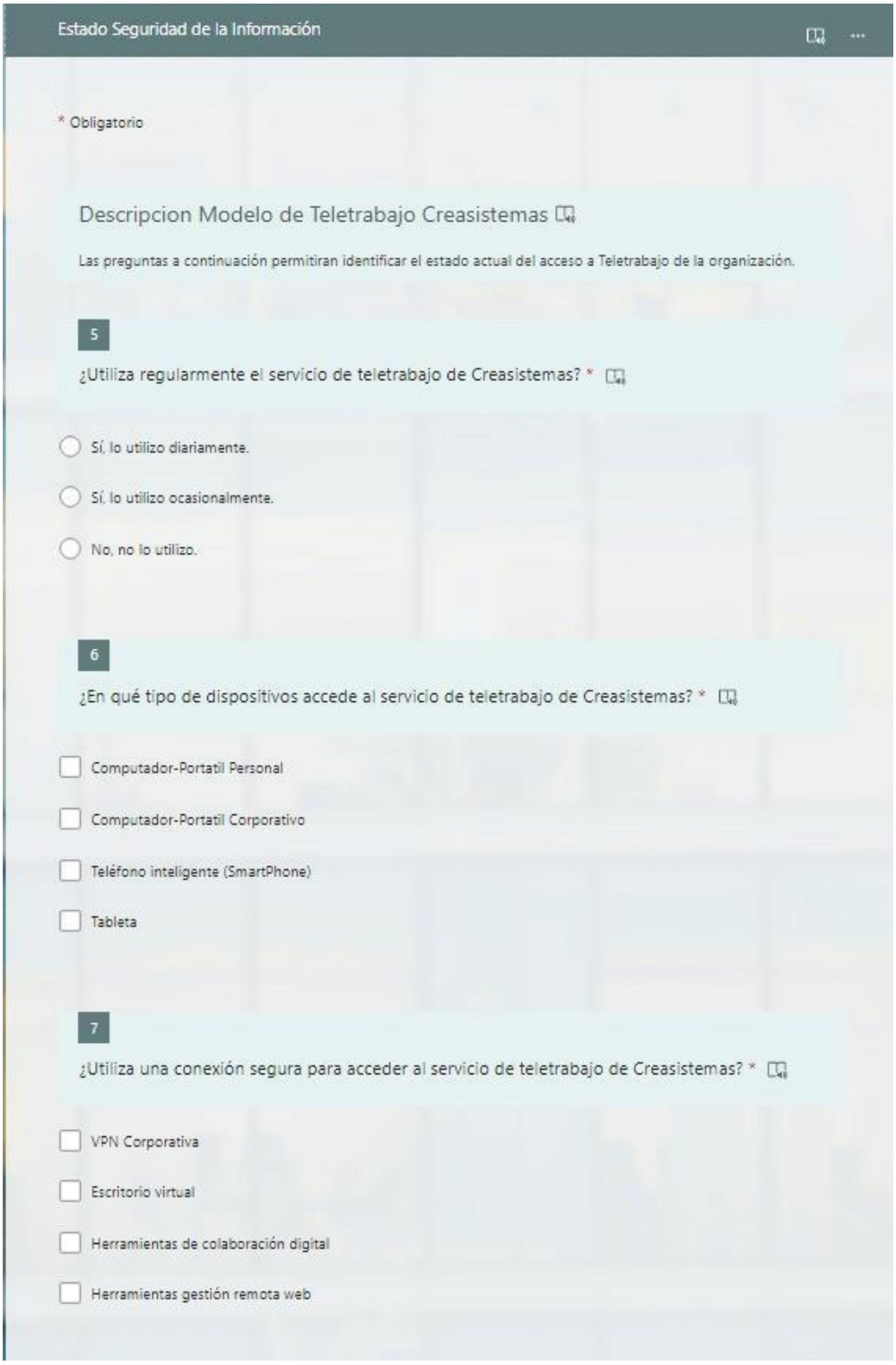
Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.

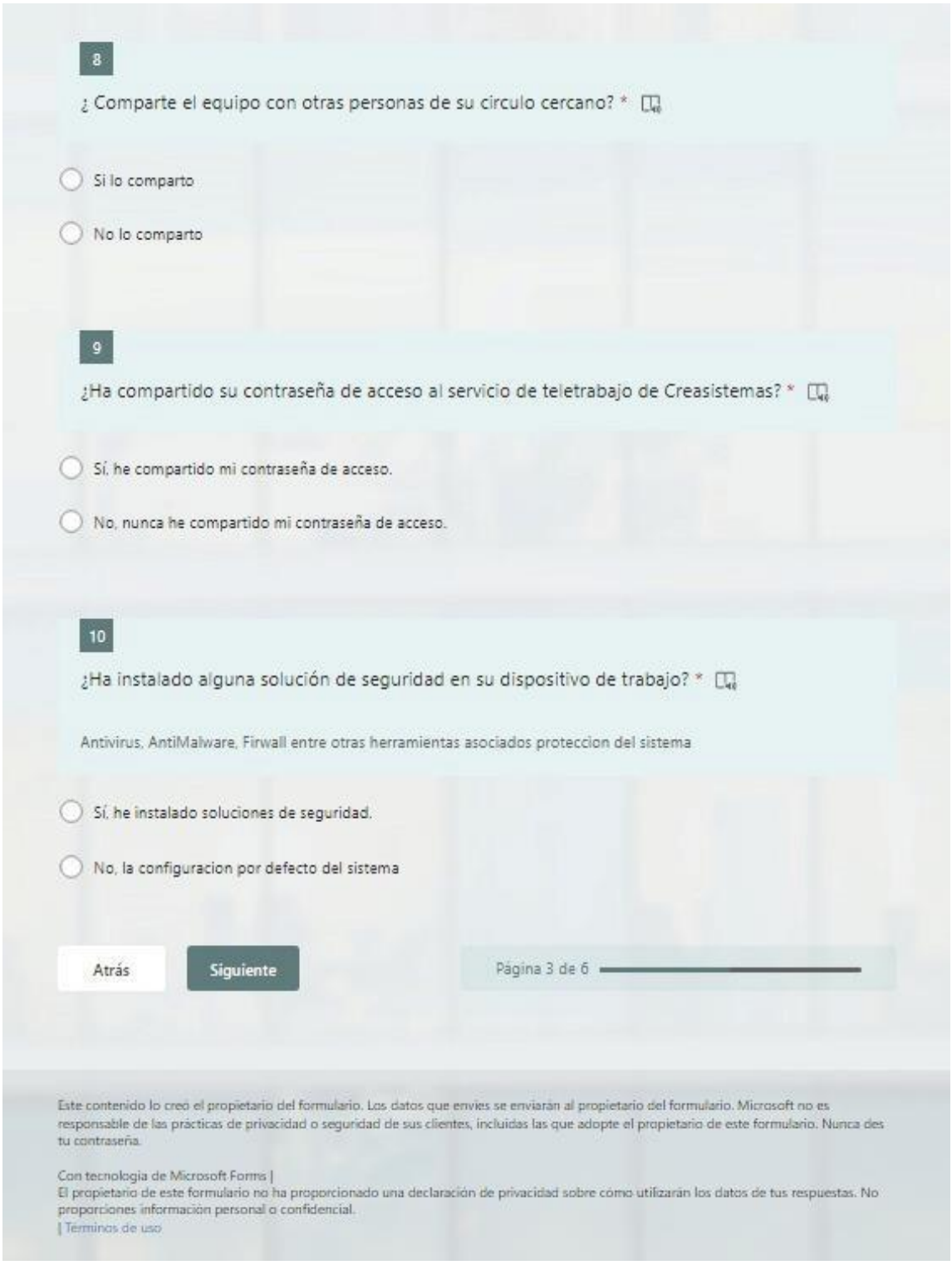
7 Anexos

ANEXO A – Diseño Encuestas




Estado Seguridad de la Información
* Obligatorio
Información del Colaborador
Por favor diligencia los datos a continuación
1
Nombre Completo Colaborador *
Escriba su respuesta
2
Correo Electronico *
Escriba su respuesta
3
Rol en el equipo de trabajo *
Administrador de TI
Administrador de DB
Coordinador - Administrativo
Equipo de Desarrollo
Operador de TI
4
Lider del Equipo *
Escriba su respuesta
Atrás
Siguiente
Página 2 de 6


Estado Seguridad de la Información
* Obligatorio
Descripcion Modelo de Teletrabajo Creasistemas
Las preguntas a continuación permitiran identificar el estado actual del acceso a Teletrabajo de la organización.
5
¿Utiliza regularmente el servicio de teletrabajo de Creasistemas? *
Sí, lo utilizo diariamente.
Sí, lo utilizo ocasionalmente.
No, no lo utilizo.
6
¿En qué tipo de dispositivos accede al servicio de teletrabajo de Creasistemas? *
Computador-Portatil Personal
Computador-Portatil Corporativo
Teléfono inteligente (SmartPhone)
Tableta
7
¿Utiliza una conexión segura para acceder al servicio de teletrabajo de Creasistemas? *
VPN Corporativa
Escritorio virtual
Herramientas de colaboración digital
Herramientas gestión remota web



8

¿ Comparte el equipo con otras personas de su circulo cercano? *

- Si lo comparto
- No lo comparto

9

¿Ha compartido su contraseña de acceso al servicio de teletrabajo de Creasistemas? *

- Sí, he compartido mi contraseña de acceso.
- No, nunca he compartido mi contraseña de acceso.

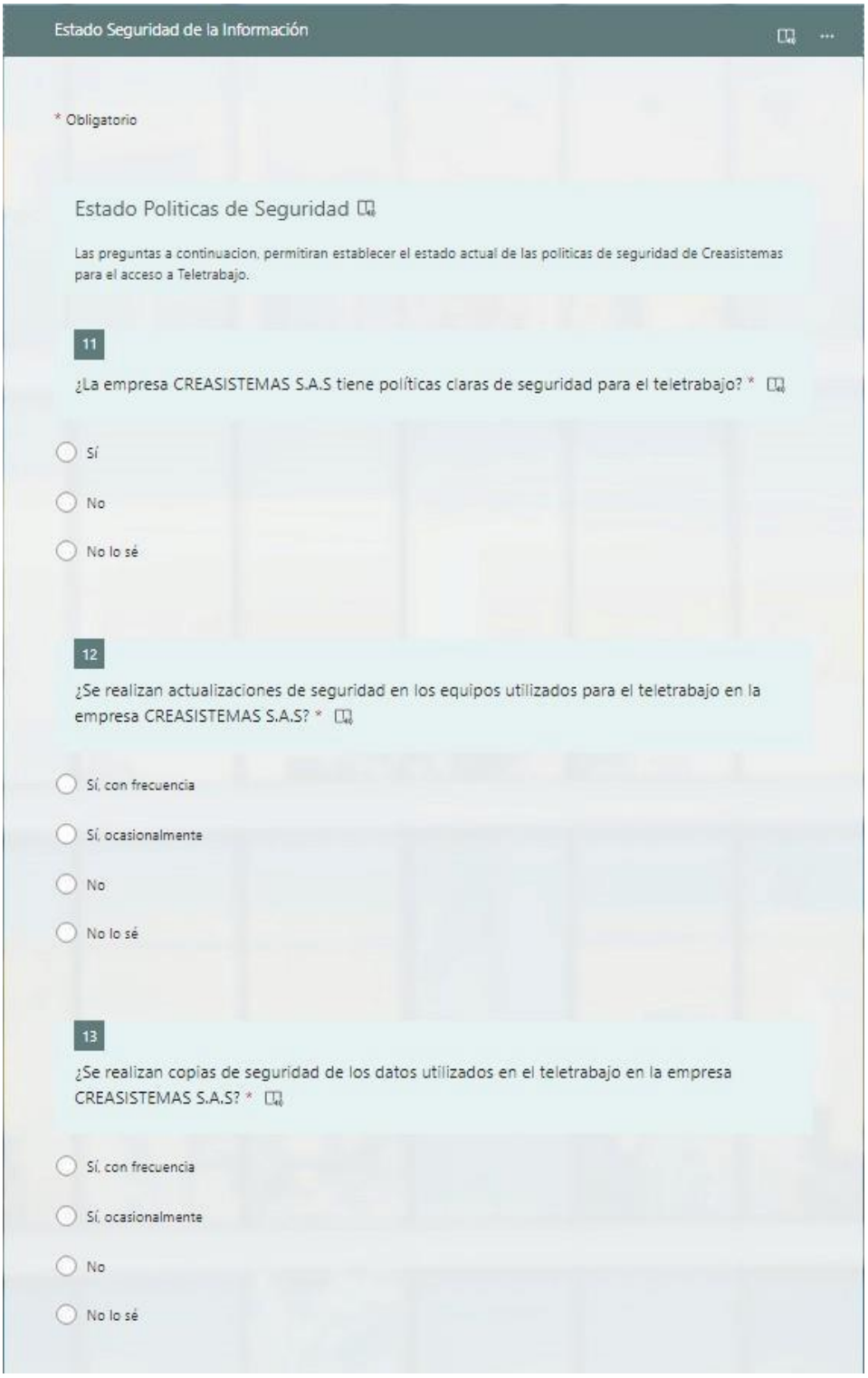
10

¿Ha instalado alguna solución de seguridad en su dispositivo de trabajo? *

Antivirus, AntiMalware, Firwall entre otras herramientas asociados proteccion del sistema

- Sí, he instalado soluciones de seguridad.
- No, la configuracion por defecto del sistema

Atrás | Siguiente | Página 3 de 6



Estado Seguridad de la Información

* Obligatorio

Estado Politicas de Seguridad

Las preguntas a continuacion, permitiran establecer el estado actual de las politicas de seguridad de Creasistemas para el acceso a Teletrabajo.

11

¿La empresa CREASISTEMAS S.A.S tiene políticas claras de seguridad para el teletrabajo? *

- Sí
- No
- No lo sé

12

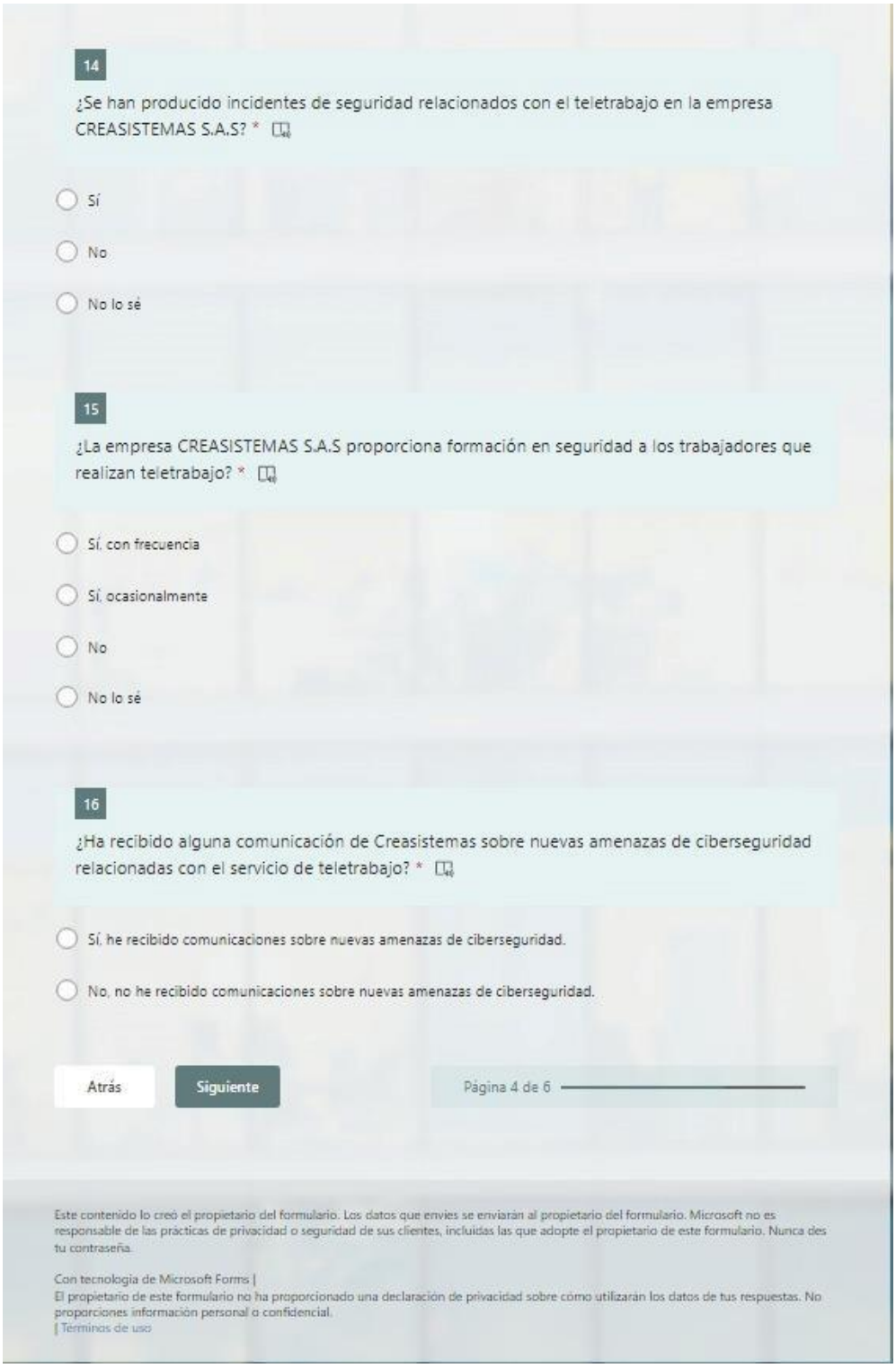
¿Se realizan actualizaciones de seguridad en los equipos utilizados para el teletrabajo en la empresa CREASISTEMAS S.A.S? *

- Sí, con frecuencia
- Sí, ocasionalmente
- No
- No lo sé

13

¿Se realizan copias de seguridad de los datos utilizados en el teletrabajo en la empresa CREASISTEMAS S.A.S? *

- Sí, con frecuencia
- Sí, ocasionalmente
- No
- No lo sé



14

¿Se han producido incidentes de seguridad relacionados con el teletrabajo en la empresa CREASISTEMAS S.A.S? *

- Sí
- No
- No lo sé

15

¿La empresa CREASISTEMAS S.A.S proporciona formación en seguridad a los trabajadores que realizan teletrabajo? *

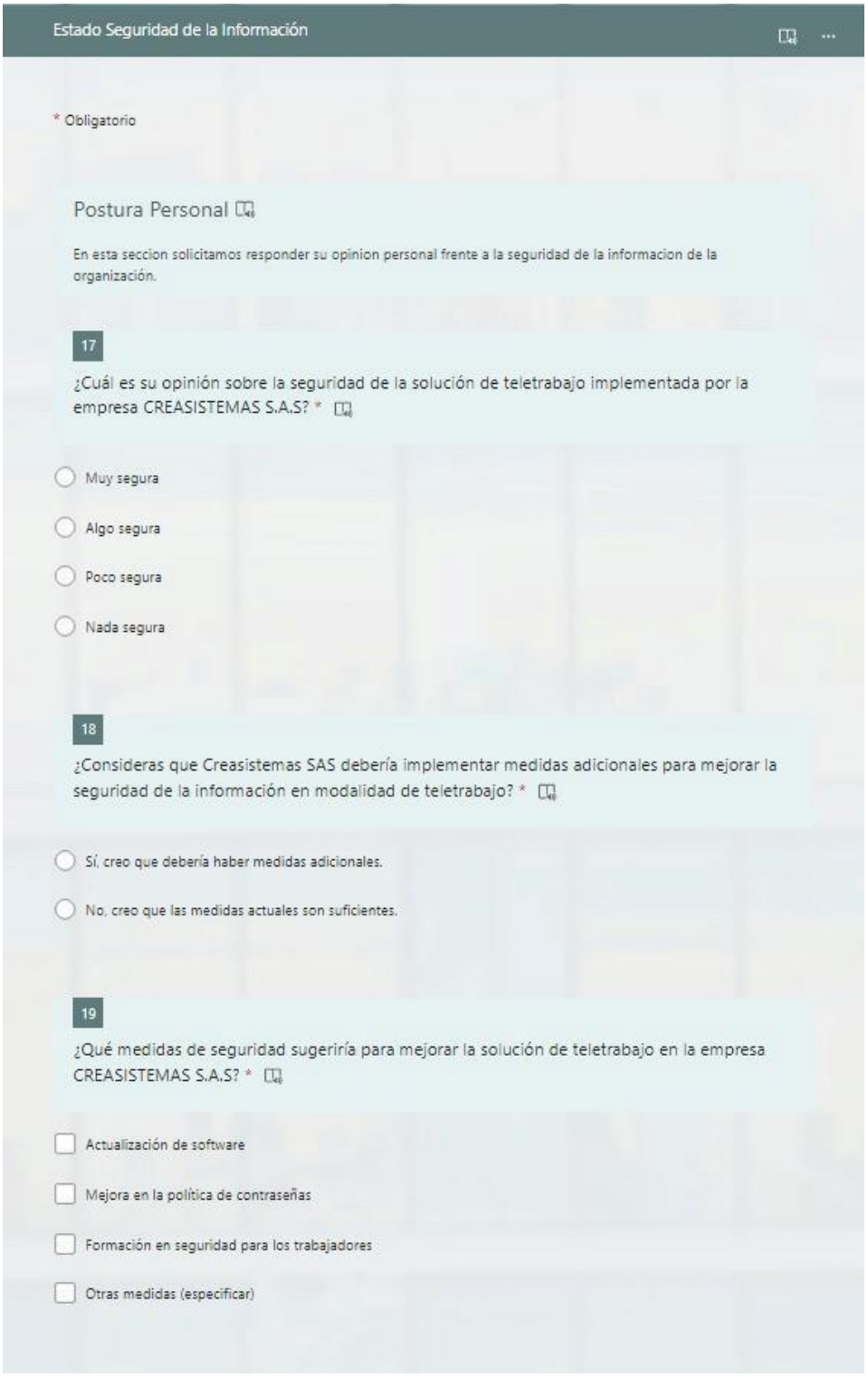
- Sí, con frecuencia
- Sí, ocasionalmente
- No
- No lo sé

16

¿Ha recibido alguna comunicación de Creasistemas sobre nuevas amenazas de ciberseguridad relacionadas con el servicio de teletrabajo? *

- Sí, he recibido comunicaciones sobre nuevas amenazas de ciberseguridad.
- No, no he recibido comunicaciones sobre nuevas amenazas de ciberseguridad.

Atrás | Siguiente | Página 4 de 6


Estado Seguridad de la Información
* Obligatorio
Postura Personal
En esta seccion solicitamos responder su opinion personal frente a la seguridad de la informacion de la organización.
17
¿Cuál es su opinión sobre la seguridad de la solución de teletrabajo implementada por la empresa CREASISTEMAS S.A.S? *
Muy segura
Algo segura
Poco segura
Nada segura
18
¿Consideras que Creasistemas SAS debería implementar medidas adicionales para mejorar la seguridad de la información en modalidad de teletrabajo? *
Sí, creo que debería haber medidas adicionales.
No, creo que las medidas actuales son suficientes.
19
¿Qué medidas de seguridad sugeriría para mejorar la solución de teletrabajo en la empresa CREASISTEMAS S.A.S? *
Actualización de software
Mejora en la política de contraseñas
Formación en seguridad para los trabajadores
Otras medidas (especificar)

20

¿Cree que existen suficientes medidas de seguridad implementadas en el servicio de teletrabajo de Creasistemas? *

- ○ Sí, creo que hay suficientes medidas de seguridad implementadas.
- ○ No, creo que se necesitan medidas adicionales de seguridad.

21

¿Alguna vez ha detectado un incidente de seguridad mientras utilizaba el servicio de teletrabajo de Creasistemas? *

- ○ Sí, he detectado un incidente de seguridad.
- ○ No, nunca he detectado un incidente de seguridad.

22

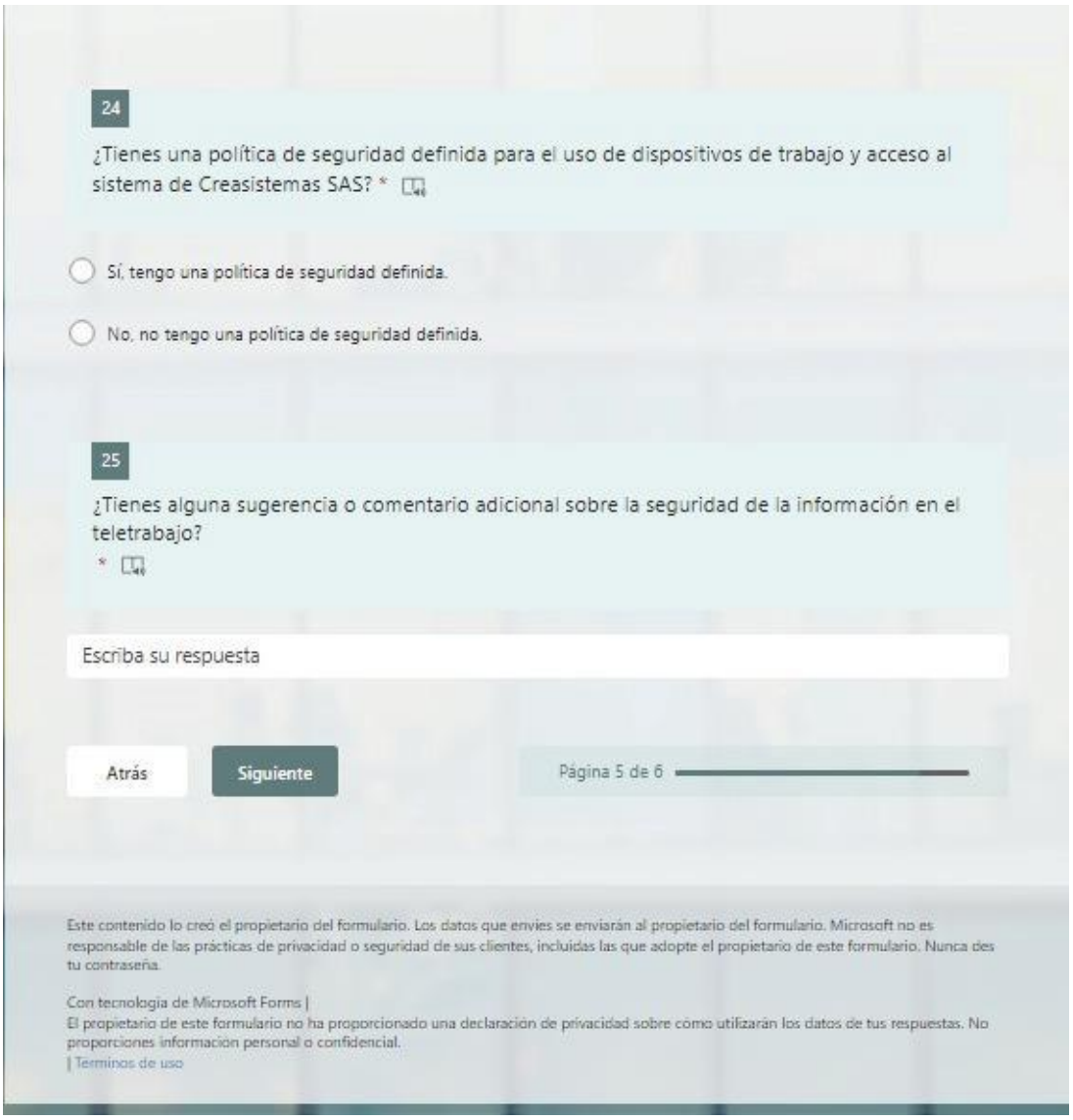
¿Qué medidas de seguridad adicionales le gustaría ver implementadas en el servicio de teletrabajo de Creasistemas? *

- ☐ Autenticación de dos factores
- ☐ Encriptación de datos
- ☐ Antivirus Centralizado
- ☐ Gestion de Actualizaciones
- ☐ Gestion de Politicas Seguridad
- ☐ Filtrado de Navegacion
- ☐ Otras medidas de seguridad (especificar)

23

¿Cree que existen suficientes medidas de seguridad implementadas en el servicio de teletrabajo de Creasistemas? *

- ○ Sí, creo que hay suficientes medidas de seguridad implementadas.
- ○ No, creo que se necesitan medidas adicionales de seguridad.


24
¿Tienes una política de seguridad definida para el uso de dispositivos de trabajo y acceso al sistema de Creasistemas SAS? *
Sí, tengo una política de seguridad definida.
No, no tengo una política de seguridad definida.
25
¿Tienes alguna sugerencia o comentario adicional sobre la seguridad de la información en el teletrabajo?
*
Escriba su respuesta
Atrás
Siguiente
Página 5 de 6
Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.
Con tecnología de Microsoft Forms |
El propietario de este formulario no ha proporcionado una declaración de privacidad sobre cómo utilizarán los datos de tus respuestas. No proporciones información personal o confidencial.
| Términos de uso

ANEXO B – Repuestas Encuestas

Estado Seguridad de la Información

45	04:57	Activo
Respuestas	Tiempo medio para finalizar	Estado

1. Nombre Completo Colaborador (0 punto)

45
Respuestas

Respuestas más recientes
"Yeffer Aguirre"
"Sebastian Aguirre"
"Edgar Aguirre"

2 encuestados (4%) respondieron **Sergio Bernal Romero** para esta pregunta.

2. Correo Electronico (0 punto)

45
Respuestas

Respuestas más recientes
"yaguirre@creasistemas.com"
"saguirre@creasistemas.com"
"eaguirre@creasistemas.com"

43 encuestados (**96%**) respondieron **creasistemas** para esta pregunta.

3. Rol en el equipo de trabajo (0 punto)

Administrador de TI	9
Administrador de DB	6
Coordinador - Administrativo	10
Equipo de Desarrollo	11
Operador de TI	9

4. Lider del Equipo (0 punto)

45
Respuestas

Respuestas más recientes
"Edgar Aguirre"
"Edgar Aguirre"
"N/A"

10 encuestados (22%) respondieron **Jeime Maldonado** para esta pregunta.

5. ¿Utiliza regularmente el servicio de teletrabajo de Creasistemas? (0 punto)

6. ¿En qué tipo de dispositivos accede al servicio de teletrabajo de Creasistemas? (0 punto)

7. ¿Utiliza una conexión segura para acceder al servicio de teletrabajo de Creasistemas? (0 punto)

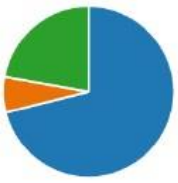
8. ¿ Comparte el equipo con otras personas de su circulo cercano? (0 punto)

9. ¿Ha compartido su contraseña de acceso al servicio de teletrabajo de Creasistemas? (0 punto)

10. ¿Ha instalado alguna solución de seguridad en su dispositivo de trabajo? (0 punto)

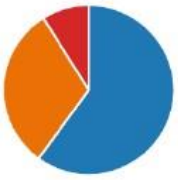
11. ¿La empresa CREASISTEMAS S.A.S tiene políticas claras de seguridad para el teletrabajo? (0 punto)

Sí	32
No	3
No lo sé	10



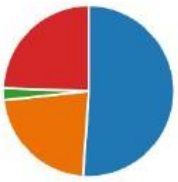
12. ¿Se realizan actualizaciones de seguridad en los equipos utilizados para el teletrabajo en la empresa CREASISTEMAS S.A.S? (0 punto)

Sí, con frecuencia	27
Sí, ocasionalmente	14
No	0
No lo sé	4



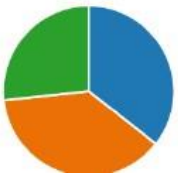
13. ¿Se realizan copias de seguridad de los datos utilizados en el teletrabajo en la empresa CREASISTEMAS S.A.S? (0 punto)

Sí, con frecuencia	23
Sí, ocasionalmente	10
No	1
No lo sé	11



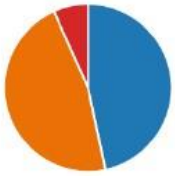
14. ¿Se han producido incidentes de seguridad relacionados con el teletrabajo en la empresa CREASISTEMAS S.A.S? (0 punto)

Sí	16
No	17
No lo sé	12



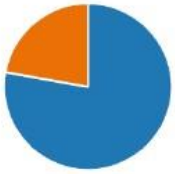
15. ¿La empresa CREASISTEMAS S.A.S proporciona formación en seguridad a los trabajadores que realizan teletrabajo? (0 punto)

Sí, con frecuencia	21
Sí, ocasionalmente	21
No	0
No lo sé	3



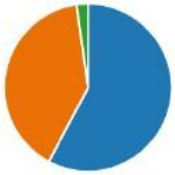
16. ¿Ha recibido alguna comunicación de Creasistemas sobre nuevas amenazas de ciberseguridad relacionadas con el servicio de teletrabajo? (0 punto)

Sí, he recibido comunicaciones s...	35
No, no he recibido comunicacio...	10



17. ¿Cuál es su opinión sobre la seguridad de la solución de teletrabajo implementada por la empresa CREASISTEMAS S.A.S? (0 punto)

Muy segura	26
Algo segura	18
Poco segura	1
Nada segura	0



18. ¿Consideras que Creasistemas SAS debería implementar medidas adicionales para mejorar la seguridad de la información en modalidad de teletrabajo? (0 punto)

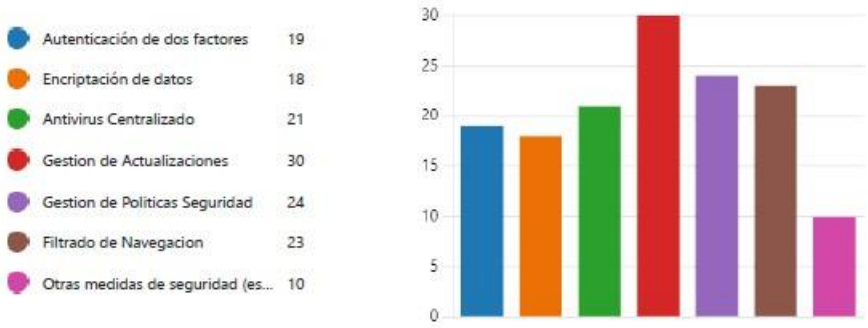
Sí, creo que debería haber medi...	26
No, creo que las medidas actual...	19

19. ¿Qué medidas de seguridad sugeriría para mejorar la solución de teletrabajo en la empresa CREASISTEMAS S.A.S? (0 punto)

20. ¿Cree que existen suficientes medidas de seguridad implementadas en el servicio de teletrabajo de Creasistemas? (0 punto)

21. ¿Alguna vez ha detectado un incidente de seguridad mientras utilizaba el servicio de teletrabajo de Creasistemas? (0 punto)

22. ¿Qué medidas de seguridad adicionales le gustaría ver implementadas en el servicio de teletrabajo de Creasistemas? (0 punto)



23. ¿Cree que existen suficientes medidas de seguridad implementadas en el servicio de teletrabajo de Creasistemas? (0 punto)

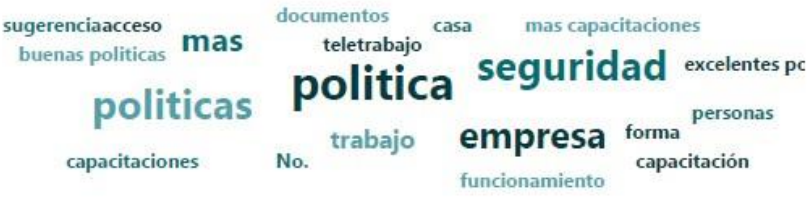
24. ¿Tienes una política de seguridad definida para el uso de dispositivos de trabajo y acceso al sistema de Creasistemas SAS? (0 punto)

25. ¿Tienes alguna sugerencia o comentario adicional sobre la seguridad de la información en el teletrabajo? (0 punto)

45
Respuestas

Respuestas más recientes
"No."
"Ninguna."
"No"

11 encuestados (**24%**) respondieron **politica** para esta pregunta.



ANEXO C – INFORME DE GERENCIAL

Después de realizar una investigación en la empresa CREASISTEMAS, he observado que la organización tiene un nivel de madurez medio en términos de seguridadde la información. A continuación, presento conclusiones detalladas y acciones de mejorarecomendadas para cada punto, teniendo en cuenta este nivel de madurez:

Políticas, procedimientos y controles de seguridad:

- Acción de mejora: Establecer políticas y procedimientos de seguridad más completosy detallados, que aborden aspectos específicos de la seguridad de la información, como la clasificación de datos, el acceso a la información y la protección de dispositivos y sistemas.

Enfoque reactivo para identificar y abordar vulnerabilidades y riesgos:

- Acción de mejora: Pasar de un enfoque reactivo a uno proactivo, mediante la implementación de un programa de gestión de riesgos de seguridad de la informaciónque permita identificar, evaluar y mitigar riesgos de forma sistemática y anticipada.

Capacitación y concientización en seguridad de la información:

- Acción de mejora: Diseñar e implementar un programa de capacitación y concientización en seguridad de la información más estructurado y exhaustivo, queincluya evaluaciones periódicas del conocimiento y la efectividad de la formación.

Revisión y actualización de políticas, procedimientos y controles:

- Acción de mejora: Establecer un proceso formal de revisión y actualización de políticas, procedimientos y controles de seguridad de la información, que se realice demanera regular y esté alineado con las necesidades y prioridades de la organización.

Implementación de un marco de gestión de seguridad de la información, como ISO/IEC27001:

- Acción de mejora: Comenzar el proceso de implementación del marco ISO/IEC 27001, lo cual incluye la realización de un análisis de brechas para identificar áreas demejora y desarrollar un plan de acción para abordarlas.

Evaluaciones y auditorías de seguridad de la información periódicas:

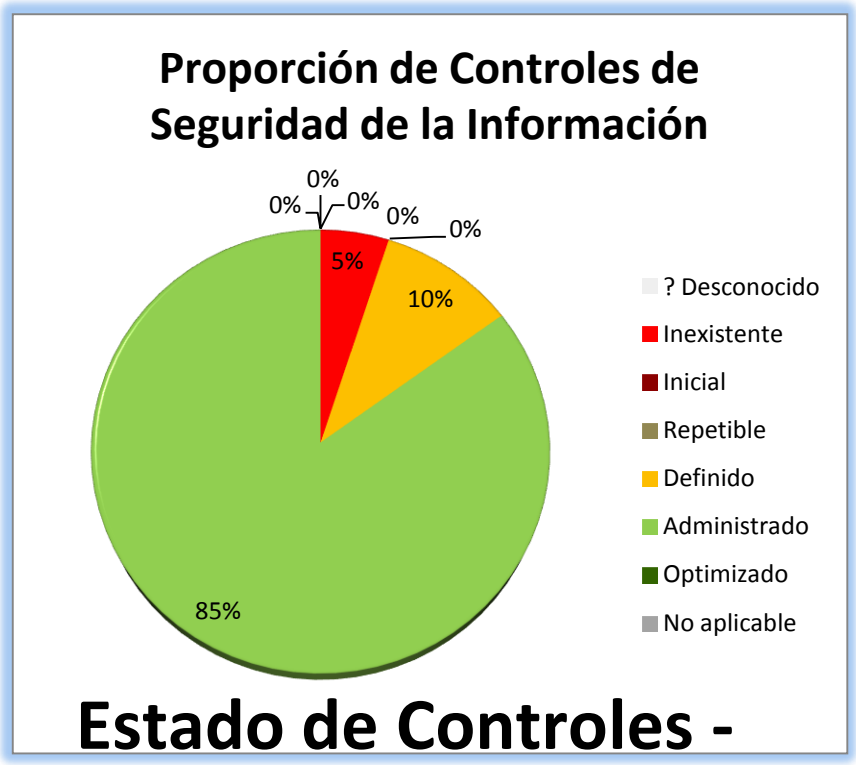
- Acción de mejora: Establecer un programa de evaluaciones y auditorías internas yexternas de seguridad de la información, que permita identificar áreas de mejora ygarantizar el cumplimiento de políticas y regulaciones aplicables.

Utilización de tecnologías y soluciones básicas de seguridad de la información:

- Acción de mejora: Realizar un análisis de las necesidades tecnológicas de la organización en términos de seguridad de la información, e invertir en soluciones yherramientas más avanzadas que permitan mejorar la protección y la detección de amenazas, así como la automatización de procesos de seguridad.

Al abordar estas acciones de mejora, CREASISTEMAS podrá elevar su nivel demadurez en seguridad de la información, pasar de un enfoque reactivo a uno proactivo ygarantizar la protección efectiva de sus activos de información en el futuro.

Estado	Significado	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	**0%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**5%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**0%**
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**0%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.	**10%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**85%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**0%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**0%**
	Total	100%


Proporción de Controles de Seguridad de la Información
0%
0%
0%
0%
0%
5%
10%
85%
? Desconocido
Inexistente
Inicial
Repetible
Definido
Administrado
Optimizado
No aplicable
Estado de Controles -

ANEXO D – Informe Detallado CheckList ISO 27001:2013

CONTROLES PARA ELTELETRABAJO

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A5	Políticas de seguridad de la información			
A5.1	Directrices de gestión de la seguridad de la información			
A5.1.1	Políticas para la seguridad de la información	Administrado	Sí, la organización cuenta con una política de seguridad de la información documentada, aprobada por la dirección y comunicada de manera efectiva a todos los empleados y partes interesadas relevantes. Sí, la política de seguridad de la información incluye un claro compromiso de la dirección y está alineada con los objetivos y estrategias de negocio de la organización. Sí, la política de seguridad de la información proporciona un marco sólido para establecer y revisar los objetivos de seguridad de la información, asegurando la mejora continua en este aspecto.	¿Existe una política de seguridad de la información documentada, aprobada por la dirección y comunicada a todos los empleados y partes interesadas relevantes? ¿La política de seguridad de la información incluye una declaración de compromiso de la dirección y está alineada con los objetivos y estrategias de negocio de la organización? ¿La política de seguridad de la información proporciona un marco para establecer y revisar los objetivos de seguridad de la información?
A5.1.2	Revisión de las políticas para la seguridad de la información	Administrado	Sí, la política de seguridad de la información es revisada y actualizada de manera periódica y sistemática, lo que garantiza su pertinencia y eficacia en función de las necesidades y circunstancias cambiantes de la organización. Sí, la organización lleva a cabo auditorías internas y externas de manera regular para verificar el cumplimiento de la política de seguridad de la información y evaluar la efectividad de su implementación en la organización.	¿La política de seguridad de la información es revisada y actualizada periódicamente para garantizar su pertinencia y eficacia en función de las cambiantes necesidades y circunstancias de la organización? ¿Se realizan auditorías internas y externas para verificar el cumplimiento de la política de seguridad de la información y la efectividad de su implementación?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A9	Control de acceso			
A9.1	Requisitos de negocio para el control de acceso			
A9.1.1	Política de control de acceso	Administrado	Si existe, la política de seguridad de informacion lo contempla. Se complementa con la Matriz de Cargos en doden se detallan los roles y las responsabilidades de los colaboradores.	¿La organización ha implementado políticas y procedimientos de control de acceso para garantizar que el acceso a la información y los sistemas se limite a personal autorizado? ¿Se basa el control de acceso en los requisitos de negocio y los riesgos de seguridad de la información identificados previamente? ¿Se ha establecido un proceso formal para la asignación y revocación de derechos de acceso a la información y a los sistemas? ¿Se monitorea y revisa el uso de los derechos de acceso otorgados y se realiza una auditoría de accesos periódicamente? ¿Se aplican controles de acceso físico y lógico a las áreas seguras, sistemas y dispositivos de la organización?
A9.1.2	Acceso a las redes y a los servicios de red	Definido	Si existen controles como MFA para establecer el acceso a servicios como Correo Electronico, acceso a recursos como escrtiroiso vrituales, erramientas de colaboracion, tanto por dispositivos fijos, moviles, tanto internos como externos a la organizaicon Se tiene configuradas reglas de notificacion en caso de deteccion de comportamientos indevidos sobre el Firewall. Esta en proceso de documentacion interna el manejod e incidents de seguridad, ya se encuentran idetificasos los actores en las atencion, reporte seguimiento, comunicacion frente a un incidente de segurdad, pero estos deben ser actualizados.	¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado? ¿Se utiliza autenticación de múltiples factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A11.1	Áreas seguras			
A11.1.1	Perímetro de seguridad física	Administrado	La sede en la cual nos encontramos esta en un sector de transtito medio vehicular y peatonal debio que en las instalaciones se presentan servicios de salud y recreacion. Se cuenta con un sistema centralizado de gestion de accesos, con cantoneras que habilitan el acceso por medio del registro del carnet de cada colaborador, y areas de trabajo. Todos los puntos de acceso estan monitoreados con camara de vigilancia, con sensores de movimiento, y con personal de vigilancia 24x7, intercomunicado con la centralde vigilancia de la organizacion.	¿Las instalaciones se encuentran en una zona de riesgo? ¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)? ¿El techo exterior, las paredes y el suelo son de construcción sólida? ¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado? ¿Las puertas y ventanas son fuertes y con cerradura? ¿Se monitorea los puntos de acceso con cámaras? ¿Existe un sistema de detección de intrusos y se prueba periódicamente?
A11.1.2	Controles físicos de entrada	Administrado	Si se cuentan con estos controles. Las unicas puertas que tienen codigo de acceso son las que dan acceso a la gerencia, como contingencia se tiene acceso con tarjeta, y as claves se vencen de manera periodica. Se lleva una bitacora de registro del acceso	¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)? ¿Hay procedimientos que cubran las siguientes áreas? • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas) ¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)? ¿Se requiere para las áreas críticas? ¿Existe un registro de todas las entradas y salidas?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A11.1.3	Seguridad de oficinas, despachos y recursos	Administrado	Si se cuentan, el DataCenter principal se encuentra en las instalaciones de un proveedor de servicios, que cuenta con certificacion TIER 3.0 que contempla todas las medidas correspondientes. En la sede principal, se tiene un Mini DataCnter, con la proteccion de acceso al cuarto de servidores y Rack de Telecomunicaciones.	¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)? ¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos? ¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?
A11.1.4	Protección contra las amenazas externas y ambientales	Administrado	Se cuenta con un sistema HoneyWell integrado al sistema de vigilancia centraizado con sensores de humo, y sistema de esparcion de agua en caso de presentarse alguna emergencia.	¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.? ¿Existe un procedimiento de recuperación de desastres? ¿Se contemplan sitios remotos?
A11.1.5	El trabajo en áreas seguras	Administrado	Se cuentan con procedimientos documentados, y controles periodicos para validar el estado de los elementos, adicionalmente la gestion de servicios administrativos se tiene incluido supervision de los servicios prestados por las compañias de vigilancia y mantenimiento. Diariamente se encuentran asignados recorredores que inspeccionan as areas de trabajo y reporte de actividad sospechosa. Estos procesos de documentos se encuentran registrados en la politica de seguridad de la informacion, el equipo de seguridad recolecta dispositivos USB abandonados, para su inspeccion por parte del equipo de	¿Se verifican al final del dia las oficinas, las salas de informática y otros lugares de trabajo? ¿Se hace un análisis para evaluar que los controles adecuados están implementados? Controles de acceso físico Alarmas de intrusión Monitoreo de CCTV (verificar la retención y frecuencia de revisión) Se prohibe el uso de equipos fotográficos, video, audio u otro tipo de grabación Políticas, procedimientos y pautas ¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?
A11.1.6	Áreas de carga y descarga	Administrado	Se cuentan documentados los procesos, y se realiza seguimiento continuo al registro de las minutas de las areas.	¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado? ¿Se verifica que el material recibido coincide con un número de pedido autorizado? ¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A11.2.3	Seguridad del cableado	Administrado	Periodicamente se realiza inspeccion y recorrido del cableado electroc y de telecomunicaciones de las diferentes sedes. Los colabroadores cuentan con un aherramienta de gestion de solicitudes para brindar apoyo y mantenimiento a las redes	¿Hay protección física adecuada para cables externos, cajas de conexiones? ¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias? ¿Se controla el acceso a los paneles de conexión y las salas de cableado? ¿Existen procedimientos adecuados para todo ello?
A11.2.4	Mantenimiento de los equipos	Administrado	Se encuentra documentado y especificado en los contratos de servicios, con las validaciones periodicas de los mismos. El personal de Servicios Administrativos designa el personal adecuado para estas actividades de gestion.	¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)? ¿Hay programas de mantenimiento y registros / informes actualizados? ¿Se aseguran los equipos?
A11.2.5	Retirada de materiales propiedad de la empresa	Administrado	Se encuentra documentado y especificado en los contratos de servicios, con las validaciones periodicas de los mismos. El personal de Servicios Administrativos designa el personal adecuado para estas actividades de gestion.	¿Existen procedimiento relativos al traslado de activos de información? ¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados? ¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo? ¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Administrado	La politica de seguridad contiene aspectos asociados a la asignacion de activos, y el buen suo de las herramientas tecnologicas.	¿Existe una "politica de uso aceptable" que cubra los requisitos de seguridad y "obligaciones" con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas? ¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras? ¿Existen controles para asegura todo esto? ¿Cómo se les informa a los trabajadores sobre sus obligaciones? ¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?
A11.2.7	Reutilización o eliminación segura de equipos	Administrado	El equipo de tecnologia designa al persona de gestion de activos herramientas de eliminacion segura de los datos de los equipos, en cada acceso a la bodega, para que en los proceso de asignacion y retiro de activos los equipos sean reinstalados sobre estas condiciones, se genera minuta de cada formato en baja.	¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación? ¿Se utiliza cifrado fuerte o borrado seguro? ¿Se mantienen registros adecuados de todos los medios que se eliminan? ¿La política y el proceso cubren todos los dispositivos y medios de TIC?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos	Administrado	Se encuenran divididos los espacios de trabajo y areas comunes por divisiones en vidrio con puertas de control de acceso a zonas clasificadas. Las pantallas cuentan con bloqueo de pantana por inactividad despues de 5minutos. Periodicamete se realizar inspeccion de las areas de trabajo y plan de emergencia de acuerdo a los riesgos identificados por la organizacion, se cuenta con un procedimiento establecido para atencion de incidentes de seguridad fisica. Anualmente se realizan simulacros con la brigada de emergencias.	¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas? ¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada? ¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales? • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal ¿Se prueban estos controles periódicamente y después de cambios importantes?
A11.2.2	Instalaciones de suministro	Administrado	El equipo de servicios Administrativos se encuengra de supervisar el contrato de mantenimiento con el proveedor de servicios para temas Electricos, periodiamente se relaiza las pruebas de carga, y mantenimientos de la UPS. Se cuenta con sistema de deteccion de temperatura, en las areas criticas, de negocio.	¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad? ¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente? ¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante? ¿Son probados con regularidad? ¿Hay una red de suministro eléctrico redundante? ¿Se realizan pruebas de cambio? ¿Se ven afectados los sistemas y servicios? ¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos? ¿Están ubicados apropiadamente? ¿Hay una capacidad adecuada de A / C para soportar la carga de calor? ¿Hay unidades redundantes, de repuesto o portátiles disponibles? ¿Hay detectores de temperatura con alarmas de temperatura?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A11.2.8	Equipo de usuario desatendido	Administrado	Por medio de directorio activo, y azure active directory se gestionan politicas de configuracion de estaciones de trabajo y dispositivos moviles para el control y acceso a la informacion.	¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción? ¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado? ¿Se protegen los bloqueos de pantalla con contraseña? ¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC? ¿Cómo se verifica el cumplimiento?
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Administrado	La politica de seguridad contiene aspectos asociados a la asignacion de activos, y el buen suo de las herramientas tecnologicas.	¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas? ¿Funciona en la práctica? ¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos? ¿Se activa automáticamente tras de un tiempo inactivo definido? ¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.1	Procedimientos y responsabilidades operacionales			
A12.1.1	Documentación de procedimientos operacionales	Administrado	El equipo de operaciones y servicios tiene documentado en el sistema de gestion de calidad, la especificacion de sus actividades y roles dentro del equipo. La politica de seguridad de la informacion, es generada desde el gobierno corporativo para realizar definir las directrices de seguridad vigentes de acuerdo al contxtos de la organizacion, Desde el equipo de Gestion Humana, se definen con el apoyo de la Gerencia de Tecnologia, la matriz de cargos y responsabilidades de los colaboradores de acuerdo a su rol. Para las actividades asociadas a la gestion de los sistemas de informacion definidos como implementacion, operacion, mantenimiento y mejora continua, cuentan con los procedimientos definidos, con los controls de cada proceso enmarcados en ITIL v3.	¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.? ¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez? ¿Los procesos son razonablemente seguros y están bien controlados? ¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal? ¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)? ¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?
A12.1.2	Gestión de cambios	Administrado	Para las actividades asociadas a la gestion de los sistemas de informacion definidos como implementacion, operacion, mantenimiento y mejora continua, cuentan con los procedimientos definidos, con los controls de cada proceso enmarcados en ITIL v3.	¿Existe una política de gestión de cambios? ¿Existen registros relacionados a la gestión de cambios? ¿Se planifican y gestionan los cambios? ¿Se evalúan los riesgos potenciales asociados con los cambios? ¿Los cambios están debidamente documentados, justificados y autorizados por la administración?
A12.1.3	Gestión de capacidades	Administrado	Para las actividades asociadas a la gestion de los sistemas de informacion definidos como implementacion, operacion, mantenimiento y mejora continua, cuentan con los procedimientos definidos, con los controls de cada proceso enmarcados en ITIL v3.	¿Existe una política de gestión de capacidad? ¿Existen registros relacionados a la gestión de capacidad? ¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante? ¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Administrado	Para las actividades asociadas a la gestion de los sistemas de informacion definidos como implementacion, operacion, mantenimiento y mejora continua, cuentan con los procedimientos definidos, con los controls de cada proceso enmarcados en ITIL v3. Loas Ambientes de Desarollo, pruebas, Preproduccion y produccion s eneucnetran aislados por politicas de seguridad a nivel de Firewall, apoyados porla segmentacion de red para cada ambiente. Los perfiles de acceso a los ambientes se encuentra segmentados adicionalmente por permisos a niveld e active directory, azure active directoru, basados en RBAC, incluyendo el perfilamiento de roles y Licenicas y herramientas de Sowftare para el desarrollo de las actividades. Sobre los ambientes de desarollo y pruebas, cuentan con ofuscamiento de datos, para dar cumplimiento con los requsitisos de privacidad de pacientes y clientes de la organizacion.	¿Se segregan entornos de TIC de desarrollo, prueba y operacionales? ¿Cómo se logra la separación a un nivel de seguridad adecuado? ¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)? ¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos? ¿Cómo se promueve y se lanza el software? ¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección? ¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros? ¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.2.1	Controles contra el código malicioso	Administrado	Se tiene asigna una politica corporativa de acceso a dispositiovos de almacenamiento masivo USB, que bloquean o habilitan de acuerdo al perfiles definidos en la organización el acceso a los mismos. Se cuenta con un Proxy el cual por medio de filtrado de contenido, permite habilitar el acceso a la web, por medio de perfilamiento de roles y funciones, se cuenta con bloqueo por listas blancas y negras de paginas web. Se cuenta con una herramienta centralziada tanto para estaciones de trabajo, como para los servidores de la compañia, que permite realizar tanto el control de las actualizaciones de seguridad, como la revision de comportamiento de Software Malicioso generado reportes y notificaciones de alerta, informativos, asociados a comportamientos inesperados. Periodicamente se realizan escaneo de vulnerabilidades sobre los ambientes de produccion, y pruebas para revisar el estado del plan de actualizaciones de seguridad y administracion de la plataforma, sobre los sitios web se realizan analisis de vulnerabilidades con el objetivo de realizar los ajustes a los procedimientos correspondientes y minimizar los riesgos.	¿Existen políticas y procedimientos asociados a controles antimalware? ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado? ¿Cómo se compila, gestiona y mantiene la lista y por quién? ¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT? ¿Se actualiza el software antivirus de forma automática? ¿Se general alertas accionables tras una detección? ¿Se toma acción de forma rápida y apropiada para minimizar sus efectos? ¿Cómo se gestionan las vulnerabilidades técnicas? ¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte? ¿Existe un mecanismo de escalación para incidentes graves?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.3	Copias de seguridad			
A12.3.1	Copias de seguridad de la información	Administrado	La poltica de seguridad de la informacion, excluye a los equipos de computo y disositivos moviles de las politicas de Backup Corporativos, la informacion de la organización y dmas asociados a la operación debe estar almacenada en los servidores corporativos, y estos estan sujetos a las politicas de Backup de la Organizacion. Teniendo en cuenta que se cuentan con plataforma OnPremise en DataCenter, y Soluciones de Virtualizacion Cloud, se encuenta alineadas las politcas de Backup ,, Transaccional, Diferenciales Diarios, Full Semanal, Full mensual, Full Semestral y Full Anual por la vigencia de los contratos de operacion, y politicas vigentes de almacenaiento de informacion clinica de pacientes. La Gestion de los Backups de las Bases de Datos, se realizan a cinta, y estan bajo el contrato de gestion tecnologica con nuestr proveedor de servicios de DataCenter. Continuamente se envian notificacion por medio de la Intranet para informar a los colaboradores las politcas de sgeuridad y recomendaciones necesarias para mantener los principios de seguridad de la informacion y atender a una cultura resonsable.	¿Existen políticas y procedimientos asociados a las copias de seguridad? ¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio? ¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.? ¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales? ¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido? ¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica? ¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar? ¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.4	Registros y supervisión			
A12.4.1	Registro de eventos	Definido	Las polticas se encuentran definidas, pero no se alamacenan los logs por periodos cortos de tiempo debido al tamañao de los mismos. Se validan que los controels esten activos, pero el seguimiento a las deviaciones de operación estan limitados ala configuracion de alarmas informativas, y de criticdad alta en casos criticos, no se cuenta con un equipo de trabajao asigandoa revision solo de logs.	¿Existen políticas y procedimientos para el registro de eventos? ¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí? ¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web ¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados? ¿Cuál es el periodo de retención de eventos? ¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?
A12.4.2	Protección de la información del registro	Inexistente	No se cuenta con el almacenamiento de los Logs, de los servidores. Los Sistemas de Informacion Critica cuentan con Logs a nivel de aplicación que llevan a tablas del sistema de manera temporal registros sobre las transacciones a nivel de Base de datos. Sin embargo no cobre al 100 % la informacion consultada.	¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no editable? ¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado? ¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos? ¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención? ¿Existen copias de seguridad de los registros?
A12.4.3	Registros de administración y operación	Inexistente	La compañie ano cuenta con un SIEM, los siemtas que contienen los Logs de Eventos, no estan correlacionados. Se cuentan con sistemas de Auditoria de Acceso a los Servidores de Archivos, asociados a la creacion, modificacion, eliminacion de archivos y carpetas, sin embargo no cubre todas las necesidades consultadas	Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)? ¿Cómo se recogen, almacenan y aseguran, analizan los registros? ¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.4.4	Sincronización del reloj	Administrado	La configuracion se relaiza de manea centralziada con los Controladores del Dominio de la Organización.	¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión? ¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)? ¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales? ¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.? ¿Existe una configuración de respaldo para la referencia de tiempo?
A12.5	Control del software en explotación			
A12.5.1	Instalación del software en explotación	Administrado	Dentro del equipode Operaciones y Servicios de TI se cuenta con un proceso de aprobacion de licenciamiento de SW asociado al control de inventario de SW gestionado por la mesa de Servicios, y la recoleccion de informacion por medio de un Sistema Centralizados, para evitar la instalacion de SOftware o Herramientas no licenciadas, o que no esten asignado al rol de los servidores o del los colaboradores de la organizacion.	¿Existe una política acerca de la instalación de software? ¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción? ¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)? ¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.? ¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados? ¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas? ¿Existe un control de cambio y aprobación adecuado para la aprobación de software?
A12.6	Gestión de la vulnerabilidad técnica			
A12.6.1	Gestión de las vulnerabilidades técnicas	Administrado	Dentro del plan de seguridad informatica, se realizan diferentes escenarios de escaneo de vulnerabilidades, y se desarrollan las actividaes para mitigar los riegos identificados, aplicando configuraciones, o instalando los KB de Sofware que minimizen las vulnerabilidades.	¿Existe una política la gestión de vulnerabilidades técnicas? ¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada? ¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes? ¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes? ¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC? ¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo? ¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución? ¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados? ¿Se emplea una administración automatizada de parches? ¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.6.2	Restricción en la instalación de software	Administrado	Los colaboradores no cuentan con privilegios de Administracion sobre los equipos, asi mismo se evita la modificacion ela configuracion de los misos, elevacion de privilegios o instalcion de Software Inseguro	¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados? ¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos? ¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?
A12.7	Consideraciones sobre la auditoria de sistemas de información			
A12.7.1	Controles de auditoría de sistemas de información	Definido	Existen procedimientos asociados a los cambios de los datos por medio de las aplicaciones, y a nivel transaccional de en las bases de Datos, de manera similar temas asociados a correso electronico. Frente a un proceso administrativo se realiza el escalamiento al area de Riesgo Corporativo para su revision y analisis de incidentes que atenten con la operacion y etica de la organizacion.	¿Existe una política que requiera auditorías de seguridad de la información? ¿Existe un programa definido y procedimientos para auditoría? ¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales? ¿Se define el alcance de la auditoría en coordinación con la administración? ¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?
A13	Seguridad de las comunicaciones			
A13.1	Gestión de la seguridad de las redes			
A13.1.1	Controles de red	Administrado	Por medio de los dispositivos de comunicación vertical y horizontal sr relaiza la segmentacion de servicios de red, tanto por reglas de firewall, perfilamiendo de acceso por servicios, como el acceso de los mismos. Se encuentran gestionados los permisos con un enfoque de confianza minima, que permita habilitar solo los acceso requeridos y agurpados en la organziacion de acuerdo a los servicios de red.	¿Existen políticas de redes físicas e inalámbricas? ¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red? ¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella? ¿Hay un sistema de autenticación para todos los accesos a la red de la organización? ¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos? ¿Los usuarios se autentican adecuadamente al inicio de sesión? ¿Cómo se autentican los dispositivos de red? ¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.? ¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?
A13.1.2	Seguridad de los servicios de red	Administrado	El proveedor de servicios como Firewall, Balanceador, WAF, y SOC, envian mensuales informes de gestion sobre la operación de estos servicios para evidenciar la gestion continua de los servicios. Y asi mismo establecer los controles de seguridad adecuados para mantener una plataforma saludable.	¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada? ¿Existe un monitoreo de servicios de red? ¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)? ¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red? ¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A13.1.3	Segregación en redes	Administrado	Por medio de los dispositivos de comunicación vertical y horizontal sr relaiza la segmentacion de servicios de red, tanto por reglas de firewall, perfilamiendo de acceso por servicios, como el acceso de los mismos. Se encuentran gestionados los permisos con un enfoque de confianza minima, que permita habilitar solo los acceso requeridos y agurpados en la organziacion de acuerdo a los servicios de red.	¿Existe una política de segmentación de red? ¿Qué tipo de segmentación existe? ¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)? ¿Cómo se monitorea y controla la segregación? ¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados? ¿Hay controles adecuados entre ellos? ¿Cómo se controla la segmentación con proveedores y clientes? ¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?
A13.2	**Intercambio de información**			
A13.2.1	Políticas y procedimientos de intercambio de información	Definido	Los proceso de clasificacion de la informacion se estaban implementando pero por una segmentacion de actividades en la organización, se separo el area de seguridad informatica del area de seguridad de la informacion, lo cual ha limitado el alcance de los equipos y ha generado cuellos de botella para continuar con procesos asociados a clasificacion de la informacion. Las unidades de negcoio son responsables de la clasificacion de la informacion, y estan apoyados por el equipo de Seguridad dela Informacion. Se encuentra bloquedo el acceso a repositoriso externos de infromacion de acuerdo a los perfiles de navegacion, no esta autorizado copartir informacion en archivos planos sin porteccion.	¿Existen políticas y procedimientos relacionados con la transmisión segura de información? ¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.? ¿Está basado en la clasificación de la información? ¿Existen controles de acceso adecuados para esos mecanismos? ¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)? ¿Se sigue el principio de confidencialidad y privacidad? ¿Existen un programa de concientización, capacitación y cumplimiento?
A13.2.2	Acuerdos de intercambio de información	Administrado	Para el manejo de informacion bancaria y los proceoss de consiliacion respectivos se usa mecanimso de encirpcion PGP para compartir la informacion entre las organizaciones. De manera externa se tiene un filtrado por direccion IP Publica, Usuario, Contraseña de acceso, ruta de almaceniamiento, para el inercambio de datos con provedores externos. Perfilameniento de acceso a Internet y Servicios FTP por el Proxy y por el Firewall.	Más allá de A.13.2.1 ¿Qué tipos de comunicaciones se implementan las firmas digitales? ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos? ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas? ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A13.2.2	Acuerdos de intercambio de información	Administrado	Para el manejo de informacion bancaria y los proceoss de consiliacion respectivos se usa mecanimso de encirpcion PGP para compartir la informacion entre las organizaciones. De manera externa se tiene un filtrado por direccion IP Publica, Usuario, Contraseña de acceso, ruta de almaceniamiento, para el inercambio de datos con provedores externos. Perfilameniento de acceso a Internet y Servicios FTP por el Proxy y por el Firewall.	Más allá de A.13.2.1 ¿Qué tipos de comunicaciones se implementan las firmas digitales? ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos? ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas? ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?
A13.2.3	Mensajería electrónica	Administrado	Para el manejo de informacion bancaria y los proceoss de consiliacion respectivos se usa mecanimso de encirpcion PGP para compartir la informacion entre las organizaciones. De manera externa se tiene un filtrado por direccion IP Publica, Usuario, Contraseña de acceso, ruta de almaceniamiento, para el inercambio de datos con provedores externos. Perfilameniento de acceso a Internet y Servicios FTP por el Proxy y por el Firewall.	¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.? ¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)? ¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?
A13.2.4	Acuerdos de confidencialidad o no revelación	Administrado	Se cuenta con procesos de confidencialidad con proveedores y con colaboradores de la organización.	¿Existen acuerdos de confidencialidad? ¿Han sido revisados y aprobados por el Departamento Legal? ¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)? ¿Han sido aprobados y firmados por las personas adecuadas? ¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?

ANEXO E – Entrevistas CREASISTEMAS S.A.S.

Entrevista Gerente General

- ¿Por qué decidió implementar el teletrabajo en su organización?

Por la característica y objeto de nuestra organización, teníamos un modelo mixto de trabajo donde algunos colaboradores trabajaban de manera remota y otros en las instalaciones de la empresa, pero con la llegada de la pandemia del COVID-19 decidimosimplementar el teletrabajo en todos los niveles como medida preventiva. Una vez terminóla pandemia, hicimos una evaluación a nivel general y dados los buenos índices de productividad y la disminución de los costos de operación, decidimos mantener el modelode teletrabajo en toda la organización.

- ¿Cuáles son los principales desafíos y beneficios que ha experimentado suorganización con el teletrabajo?

Los principales desafíos son mantener la productividad, el compromiso de los empleados y mantener nuestra calidad del servicio con nuestros clientes, mientras que losbeneficios incluyen la reducción de costos de operación, la flexibilidad laboral y la calidad de vida de nuestros colaboradores.

- ¿Ha establecido políticas y procedimientos específicos para la seguridad de lainformación en teletrabajo?

Sí, con el impacto de la pandemia establecimos y reforzamos las políticas yprocedimientos para mejorar la seguridad de la información en la modalidad de teletrabajo.

- ¿Cuáles son las medidas de seguridad que ha implementado para proteger lainformación en teletrabajo?

Implementamos medidas de seguridad como el uso de VPN, múltiple factor deautenticación, encriptación de datos, uso de software licenciado, mantener equipos y dispositivos actualizados, entre otros.

- ¿Qué herramientas y tecnologías utiliza en teletrabajo?

Dentro de la organización hacemos uso de las herramientas de Microsoft como Teams, SharePoint, Onedrive compartir información y como sistemas de colaboración enlínea.

- ¿Realiza pruebas de penetración y evaluaciones de vulnerabilidades para asegurar laseguridad de la información en teletrabajo?

Al inicio de la pandemia no se realizaban, pero debido a que estamos en proceso de certificación y como parte de los requisitos de la misma, debemos realizar pruebas de penetración y evaluaciones de vulnerabilidades regularmente para garantizar la seguridadde la información en teletrabajo.

- ¿Brinda capacitación sobre seguridad de la información a los empleados que trabajanen teletrabajo?

Sí, brindamos capacitación sobre seguridad de la información a nuestros colaboradores que están en el esquema de teletrabajo y propendemos por crear concienciaen ellos para el buen uso de los recursos haciendo uso de mejores prácticas.

- ¿Tiene una política de uso aceptable para el teletrabajo y se ha comunicadoclaramente a los empleados?

Sí, hemos definido algunas políticas de uso aceptable para el teletrabajo, por ejemplo, el uso adecuado de los recursos, medidas de seguridad a tener en cuenta paraproteger la información sensible, protección ante posibles ataques de virus y malware,uso de contraseñas seguras, evitar el uso de redes inseguras, entre otros, y se ha comunicado claramente a los colaboradores.

- ¿Cómo promueve la concientización sobre la seguridad de la información enteletrabajo en su organización?

Mediante capacitaciones y campañas de sensibilización.

- ¿Se tienen establecidos procedimientos para la gestión de incidentes de seguridad enteletrabajo?

Establecimos un procedimiento de gestión de incidentes que incluye el reporte inmediato de los incidentes a la gerencia y al equipo de administración de TI. Se maneja de esta manera porque no se tiene conformado en equipo de seguridad de la información,pero dentro del mismo proceso de certificación que está en curso, se tiene proyectado crearlo.

- ¿Cómo se reportan los incidentes y cómo se investigan y resuelven?

Los incidentes se investigan y se resuelven en colaboración con el equipo de TI, lagerencia y el personal afectado por un incidente de seguridad.

- ¿Tiene registros de incidentes de seguridad en teletrabajo y cómo los utiliza paramejorar la seguridad de la información en su organización?

Sí, llevamos un registro de los incidentes de seguridad de nuestros colaboradoresy de los reportes de nuestros clientes y se realiza de forma manual en teletrabajo y los utilizamos para identificar patrones, mejorar la seguridad de la información y como apoyo para implementar mejores practicas

- Basado en sus respuestas, ¿cuáles son los principales puntos fuertes y débiles en laseguridad de la información en teletrabajo en su organización?

Creemos que nuestros puntos fuertes en seguridad de la información en teletrabajoincluyen nuestras medidas de seguridad, el uso adecuado de los recursos y la creación de conciencia en nuestros colaboradores. Así mismo, nuestro desafío es emitir políticas y

procedimientos claros en seguridad de la información dentro de la organización con el finde que los colaboradores las pongan en práctica para minimizar los riesgos asociados.

- ¿Está interesado en recibir recomendaciones para mejorar la seguridad de lainformación en teletrabajo?

Sí, estoy interesado en recibir recomendaciones para mejorar la seguridad de lainformación en teletrabajo.

Entrevista directora de tecnología

- ¿Qué motivó a su organización a adoptar el teletrabajo?

Indudablemente, lo que nos motivó a adoptar el teletrabajo a nivel general, fue la llegada de la pandemia. Para nosotros no fue tan traumático porque estábamos laborando en un modelo hibrido de trabajo en sitio para gran parte de los empleados y algunos en unesquema de teletrabajo desde diferentes ciudades del país.

- ¿Cuáles son los principales desafíos y beneficios de implementar el teletrabajo desdeuna perspectiva tecnológica?

Los principales desafíos que identificamos estaban relacionados con la seguridadde la información, la conectividad de los empleados, la implementación de sistemas de comunicación y colaboración para que los empleados siguieran trabajando de manera efectiva, el acceso a la información.

Dentro de los beneficios logramos reducir los costos de operación, costos de servicios, desplazamientos, mejorar la productividad de los trabajadores, la flexibilidadde horarios.

- ¿La organización tiene políticas y procedimientos específicos para la seguridad de lainformación en teletrabajo?

Está en proceso de implementación

- ¿Qué medidas de seguridad se han implementado para proteger la información enteletrabajo?

Se han implementado algunas medidas, como el acceso a la red interna medianteel uso de VPNs, implementación múltiple factos de autenticación, encriptación de datos,uso de software licenciado, mantener los equipos y dispositivos actualizados y crear conciencia en los empleados del uso de los recursos asignados.

- ¿Qué herramientas tecnológicas se utilizan para apoyar el teletrabajo y cómo seasegura su seguridad?

Utilizamos plataforma de colaboración y comunicación como Microsoft Teams, SharePoint, uso de las herramientas de nube, acceso remoto a los sistemas de informaciónmediante VPN y se ha reforzado el uso de las herramientas que provee Azure.

- ¿Se brinda capacitación a los empleados sobre seguridad de la información enteletrabajo?

Hacemos especial énfasis en seguridad de la información y en el buen uso de losrecursos que la empresa les asigna, identificación de amenazas para proteger la información.

- ¿Se ha establecido una política de uso aceptable para el teletrabajo?

Sí y actualmente estamos en proceso de construcción de políticas de uso aceptableen teletrabajo para proteger los activos de la empresa.

- ¿Cómo se promueve la concientización sobre la seguridad de la información enteletrabajo?

Aunque no se tiene un proceso formal, se realizan sesiones y comunicaciones paramejorar los temas de seguridad de la información no solamente en teletrabajo y se les brindan las herramientas para que puedan realizar sus labores haciendo uso de las mejoresprácticas.

- ¿Qué procedimientos se tienen en caso de un incidente de seguridad en teletrabajo?

El procedimiento que se tiene es mediante un reporte inmediato porque actualmente no se tiene un procedimiento formal y está en proceso de construcción.

- ¿Cómo se investigan y resuelven los incidentes de seguridad?

En estos momentos no se tiene establecido un procedimiento formal. Cuando se reporta algún incidente, se reúne la gerencia y el equipo de TI para investigar el incidente,identificarlo, recopilar las evidencias, se cita a la persona involucrada en el incidente paraque haga los descargos y con base en la información aportada se realizan los análisis y se toman las medidas que correspondan para solucionarlo.

- ¿Se registran y analizan los incidentes de seguridad para identificar patrones y áreasde mejora?

Los incidentes se registran de forma manual en un archivo y se toma como basepara mejorar la seguridad de la información.

- ¿Cuál considera que son los principales puntos fuertes y desafíos en seguridad de lainformación en teletrabajo para su organización?

Como puntos fuertes están el recurso humano y su alto de grado de compromiso,el buen uso de los recursos y la implementación de buenas prácticas en seguridad de la información. Dentro de los desafíos es continuar en la construcción de las políticas y procedimientos de seguridad de la información.

- ¿Está interesado en recibir recomendaciones para mejorar la seguridad de lainformación en teletrabajo?

Sí porque me interesa poder mejorar en todos los aspectos de seguridad para biende la empresa, los empleados y los clientes.

Entrevista Oficial De Seguridad

Debido a que en CREASISTEMAS no se tienen formalizadas políticas y procedimientos de seguridad de la información y no se tiene un oficial de seguridad, no fue posible llevar a cabo esta entrevista. En su lugar, la información que se aportó es queestán en proceso de certificación en ISO 27001 y dentro de la misma se debe formalizar la política de seguridad de la información.

Entrevista Recursos Humanos

- ¿Con qué frecuencia los empleados de su organización trabajan de forma remota(teletrabajo)?

Después de la pandemia, todo el personal de CREASISTEMAS está en la modalidad de teletrabajo. Antes de pandemia, algunos empleados trabajaban de maneraremota, especialmente algunos recursos lo hacían desde sus ciudades de origen, como, por ejemplo, Barranquilla, Tunja, Neiva y algunos municipios cercanos a Bogotá.

- ¿Qué tipo de datos y sistemas tienen acceso los empleados que trabajan de formaremota?

La mayoría de los empleados de CREASISTEMAS no tienen acceso a lossistemas de información porque están asignados a clientes en la modalidad de outsourcing y sus funciones las realizan directamente en los clientes.

- ¿Cuáles son las políticas y procedimientos de seguridad de la información que suorganización tiene en su lugar para apoyar el teletrabajo?

Formalmente no se tiene, pero está en proceso de construcción y deimplementación.

- ¿Qué medidas de seguridad se han implementado para garantizar la

protección de losdatos mientras los empleados trabajan de forma remota?

Acceso remoto, VPN.

- ¿Ha proporcionado su organización una formación específica en seguridad de la información para los empleados que trabajan de forma remota?

Formalmente no, sin embargo, se les brinda capacitación y comunicados parareforzar los aspectos de seguridad de la información en el teletrabajo.

- ¿Cuáles son los principales desafíos que su organización enfrenta en términos deseguridad de la información para el teletrabajo?

Desde recursos humanos hemos tratado de que nuestros empleados se sientan cómodos, tengan un buen ambiente laboral, hagan un buen uso de los recursos que se leasigna y cumplan con los objetivos de la empresa.

- ¿Cuáles son los planes de su organización para abordar estos desafíos y mejorar laseguridad de la información para el teletrabajo?

Nos preocupamos por el bienestar de nuestros empleados y les brindamos las herramientas necesarias y los recursos para que puedan realizar sus labores dentro delmarco de seguridad de la información.

- ¿Cómo se está monitoreando el cumplimiento de las políticas y procedimientos deseguridad de la información para el teletrabajo?

Se mantiene una comunicación muy cercana entre los empleados y las directivas con el fin de hacer seguimiento a sus responsabilidades y al cumplimiento de las políticasde la empresa.

- ¿Qué otras iniciativas de seguridad de la información están planificadas para el futurocercano en su organización?

Estamos en proceso de certificación de la norma ISO 27001 y por consiguiente estamos en la construcción de las políticas de seguridad de la información con énfasis enteletrabajo.

- ¿Tiene alguna otra observación o comentario sobre la seguridad de la informaciónpara el teletrabajo en su organización?

Como responsable de recursos humanos estamos apoyando todas las iniciativas enla construcción de políticas y procedimientos en seguridad de la información y también en brindarle a nuestros empleados un buen sitio para que pueda trabajar de manera cómoda, segura y puedan desarrollarse profesionalmente.

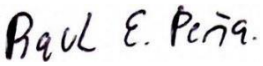
Por intermedio del presente documento en mi calidad de autor o titular de los derechos de propiedad intelectual de la obra que adjunto, titulada: *"Análisis de seguridad de la soluciónde Teletrabajo de la empresa CREASISTEMAS S.A.S."*, autorizo a la Corporación universitaria UNITEC para que utilice en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador o titular de la obra objeto del presente documento.

La presente autorización se da sin restricción de tiempo, ni territorio y de manera gratuita. Entiendo que puedo solicitar a la Corporación universitaria UNITEC retirar mi obra en cualquier momento tanto de los repositorios como del catálogo si así lo decido.

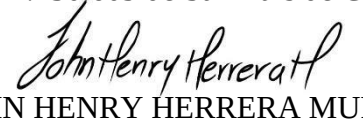
La presente autorización se otorga de manera no exclusiva, y la misma no implica transferencia de mis derechos patrimoniales en favor de la Corporación universitaria UNITEC, por lo que podré utilizar y explotar la obra de la manera que mejor considere. La presente autorización no implica la cesión de los derechos morales y la Corporaciónuniversitaria UNITEC los reconocerá y velará por el respeto a los mismos.
La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato electrónico, y en general para cualquier formato conocido o por conocer. Manifiesto que la obra objeto de la presenteautorización es original y la realicé sin violar o usurpar derechos de autor de terceros, por lotanto, la obra es de mi exclusiva autoría o tengo la titularidad sobre la misma. En caso de presentarse cualquier reclamación o por acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión asumiré toda la responsabilidad, y saldré en defensa de los derechos aquí autorizados para todos los efectos la Corporación universitariaUNITEC actúa como un tercero de buena fe. La sesión otorgada se ajusta a lo que establecela ley 23 de 1982.
Para constancia de lo expresado anteriormente firmo, como aparece a continuación.

Firma

AUGUSTO ORTEGA MOLINA
C.C. 4.150,609 de San Luis de Gaceno



RAUL ESTEBAN LEON
CC 94.522.931 Santiago de Cali



JOHN HENRY HERRERA MURCIA

CC 80232949 DE Bogotá D.C.

Señores (as)
Corporación Universitaria

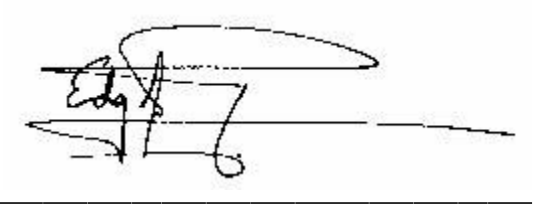
UNITEC.Programa

Posgrados Tecnología

Yo, Edgar Aguirre Cruz, identificado con cédula de ciudadanía 6.760.121 de la ciudad de Tunja y como representante legal de la empresa Crea sistemas S.A.S., autorizo a Augusto Ortega Molina, identificado con cédula de ciudadanía 4.150.609 de San Luis de Gaceno, John Henry Herrera Murcia, identificado con cédula de ciudadanía 80.232.949 de Bogotá D.C., y Raúl Esteban Peña León, identificado con cedula de ciudadanía 94.522.931 de Santiago de Cali, para desarrollar su proyectode investigación “Análisis de seguridad de la solución de Teletrabajo de la empresa Crea Sistemas S.A.S.”

Facilitaré el tiempo e información necesarias para el desarrollo de este proyecto de investigación. Laempresa y sus colaboradores apoyarán el proceso de investigación y el resultado de la misma, conuna postura abierta a las innovaciones, implementaciones, estrategias y en general a los cambios que la investigación aporte a la organización.

Atentamente,



EDGAR AGUIRRE

CC 6 .760.121 de Tunja

Representante Legal – Crea Sistemas S.A.S.