



Universidad Cenfotec

**“Propuesta de guía de controles de seguridad de la
información para PYMES basado en ISO27000”**

Proyecto de graduación para optar por el grado de Maestría en
Ciberseguridad

Ronid Figueroa Rodríguez

Marzo, 2020



Universidad Cenfotec

**“Propuesta de guía de controles de seguridad de la
información para PYMES basado en ISO27000”**

Proyecto de graduación para optar por el grado de Maestría en
Ciberseguridad

Ronid Figueroa Rodríguez

Marzo, 2020

DECLARACIÓN JURADA

Yo, Ronid Figueroa Rodríguez, estudiante de la Universidad Cenfotec, declaro bajo fe de juramento y consciente de las responsabilidades penales de este acto, que soy autora intelectual de la Tesis o Proyecto de investigación titulado: "Propuesta de guía de controles de seguridad de la información para PYMES basado en ISO27000", por lo que libero a la Universidad Cenfotec de cualquier responsabilidad en caso de que nuestra declaración sea falsa.

Brindada en San Pedro, Montes de Oca, San José Costa Rica en el día 02 de marzo del año 2020.

Ronid Figueroa Rodríguez
Cédula 1-1573-0156

Agradecimientos

A la Universidad Cenfotec, que me brindo las herramientas necesarias para adquirir nuevos conocimientos y me hizo crecer profesionalmente.

A mis papás, ya que son la razón de que hoy esté donde estoy, han contribuido con su ejemplo y me han guiado siempre en la labor de crecer en valores y ética.

A mi hermana, que ha sido un apoyo incondicional en mi vida.

A mi novio, que siempre me ha apoyado y me incita a crecer cada vez más, tanto a nivel personal como profesional.

Y a todas las personas que de una u otra forma me acompañaron durante todo este proceso y me brindaron su apoyo.

ÍNDICE DE TABLAS

Tabla 1: Tabla De Activos	61
Tabla 2: Tabla De Riesgos.....	64
Tabla 3: Tabla Para Estimar La Probabilidad	67
Tabla 4: Tabla Para Estimar El Impacto.....	67
Tabla 5: Criterios De Aceptación Del Riesgo	67
Tabla 6: Matriz De Riesgo Y Escala De Criticidad Utilizada En El Análisis	68
Tabla 7: Tabla Estimación De Riesgos	68
Tabla 8: Tabla Estrategia De Tratamiento.....	75
Tabla 9: Tabla Controles.....	140

ÍNDICE DE FIGURAS

Figura 1. Clasificación Pymes.....	15
Figura 2. Cantidad De Empleados	16
Figura 3. Pymes Por Sector	16
Figura 4. Perfil De Emprendedores.....	17
Figura 5. Empresas Inscritas.....	19
Figura 6. Empresas Por Act Económica.....	20
Figura 7. Empresas Por Provincia.....	21
Figura 8. Computadoras Con Internet	24
Figura 9. Ancho De Banda	25
Figura 10. Edad Del Equipo	25
Figura 11. Software/Licenciamiento	26
Figura 12. Uso De Redes Sociales	27
Figura 13. Ventas Por Whatsapp/Sms	27
Figura 14. Número De Ventas	28
Figura 15. Ventas Por Redes Sociales.....	29
Figura 16. Número De Ventas Por Redes	29
Figura 17. Servicio De Banca Electrónica.....	29
Figura 18. Entidades.....	35
Figura 19. Uso De Teléfonos Para Pagos	30
Figura 20. Soporte Externo.....	31
Figura 21: Elementos Del Análisis De Riesgos Potenciales	37
Figura 22: Funciones	40
Figura 23. Uso De Herramientas Tecnológicas	51
Figura 24. Frecuencia Uso De Herramientas	52
Figura 25. Prácticas	52
Figura 26. Importancia De La Ciberseguridad.....	53
Figura 27. Uso De Antivirus.....	54
Figura 28. Herramientas Para Asegurar Información.....	54
Figura 29. Identificación De Activos Críticos	55

Figura 30. Análisis De Riesgos	55
Figura 31. Presupuesto A Ciberseguridad	56
Figura 32. Capacitación	56
Figura 33. Cargo Con Funciones De Ciberseguridad	57
Figura 34. Plan De Contingencia.....	58
Figura 35. Acción Ante Un Evento	58
Figura 36. Riesgos.....	59

TABLA DE CONTENIDO

<i>Introducción</i>	10
<i>Capítulo I: Aspectos Generales</i>	12
Generalidades	12
Antecedentes del Problema	12
Definición y Descripción del Problema	12
Justificación	13
Objetivos	14
Alcance y Limitaciones	14
Estado de la cuestión	15
<i>Capítulo II: Marco Teórico</i>	17
¿Qué es una Pyme?	17
Pymes en Centroamérica	19
Pymes en Costa Rica	23
Importancia de las tecnologías de la información en las Pymes	27
Tecnologías de la Información en las Pymes de Costa Rica	29
Redes Sociales y Modelos de Negocio en Internet	32
Ciberseguridad	36
Ciberseguridad de las Pymes	37
Ciberseguridad de las Pymes en América Latina	38
Sistema de Gestión de la Seguridad	40
Gestión del Riesgo	41
Magerit	41
Estándares	44
Barreras Organizacionales	50
<i>Capítulo III: Marco Metodológico</i>	54
Enfoque de Investigación	54
Tipo de Investigación	54
Población y Muestreo	55
Instrumentos de Recolección de Datos	55
Técnicas de Análisis de la Información	55
<i>Capítulo IV: Análisis de Resultados</i>	56
<i>Capítulo V: Propuesta de Estrategia de la gestión de la ciberseguridad</i>	64
<i>Capítulo VI: Conclusiones</i>	158

INTRODUCCIÓN

Los avances tecnológicos, en los últimos años, han avanzado y revolucionado por completo el mundo, en todos los aspectos, incluidos, el manejo de la información y los procesos de negocio. La mayoría de las empresas han incluido, poco a poco, el uso de la tecnología como un instrumento de ayuda y como un aliado de su negocio; a tal grado, que se ha convertido en un factor sumamente importante para la supervivencia de estas, independientemente de su tamaño. Esto ha generado gran cantidad de oportunidades y ha representado un avance con respecto a la manera antigua y tradicional de manejar la información y los procesos; sin embargo, también ha abierto las puertas a muchos riesgos, por ejemplo, los ciberataques, que han ido evolucionando de la mano con la tecnología, provocando gran cantidad de amenazas, ejecutadas cada vez con mejores técnicas y con nuevos objetivos de ataque.

Las pequeñas y medianas empresas, al igual que las grandes corporaciones, se encuentran expuestas a este tipo de riesgos. Muchas PYMES son víctimas de ciberataques, desde infecciones por *malware*, *phishing*, fuga de información hasta ataques de denegación de servicio, en muchos casos, son utilizadas para, a través de ellas, hacer daño a terceros. Sin embargo, a diferencia de las grandes empresas, las PYMES en la mayoría de los casos, no cuentan con los recursos necesarios para protegerse de manera adecuada; un estudio de la firma de seguridad informática ESET demostró que, por dos años, las PYMES son las primeras víctimas de ataques cibernéticos.

Es por esto que es necesario aumentar los esfuerzos por fortalecer la seguridad de las pequeñas y medianas empresas de una forma integral, efectiva y práctica; este trabajo pretende plantear una estrategia sencilla y fácil de implementar de gestión de ciberseguridad que permita a las empresas tener una guía, no solo basada en las buenas prácticas y normas vigentes, sino teniendo también en cuenta la realidad de estas empresas, en cuanto a los riesgos más críticos y los controles más efectivos para sus riesgos, de acuerdo a los recursos de tiempo, dinero y conocimiento que una PYME puede realmente destinar para alcanzar un nivel de protección aceptable, teniendo en cuenta que este tipo de organizaciones dependen cada día más del uso del de las TIC

para el desarrollo de las diferentes actividades que les permiten cumplir con sus objetivos estratégicos.

Para la elaboración de este trabajo se utilizarán una combinación de diversas metodologías; para la primera fase, se llevará a cabo un estudio exploratorio para conocer el panorama general promedio de las PYMES en Costa Rica, esto con el fin de identificar los riesgos más críticos, tomando en cuenta probabilidad e impacto, así como también, identificar las dificultades que se presentan en dichas empresas para la implementación de controles de seguridad y cuantificar los recursos que puede destinar una PYME para la protección ante estos; para dicha fase se va a emplear la recopilación de información relevante de estudios regionales y/o internacionales previos y encuestas a través de mecanismos no presenciales a una muestra representativa y significativa.

A partir de los resultados del estudio anterior, se elaborará una guía de buenas prácticas y posibles controles que ayuden a mitigar los riesgos identificados, realizando un análisis de factibilidad de estos, teniendo en cuenta su efectividad y los recursos necesarios para su implementación (tiempo, costo, cantidad de recursos humanos, etc.). De esta manera, seleccionar un conjunto de controles, de manera que se encuentren dentro del margen de recursos que el estudio reveló que una PYMES podría dedicarle.

La importancia de esta investigación radica, entonces, en el impacto social que pudiera tener en un futuro ya que la estrategia a desarrollar podrá ser usada por las diferentes PYMES como una base y un indicador de los aspectos mínimos de seguridad con los que deben contar para proteger sus diferentes activos y procesos.

CAPÍTULO I: ASPECTOS GENERALES

GENERALIDADES

El momento que vive el país, en que la tecnología de la computación ha penetrado todos los ámbitos de la Sociedad de la Información o Cibersociedad, que, entendida como un desarrollo social caracterizado por la capacidad de sus miembros para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma que se prefiera, es sumamente importante, ya que de la mano de este gran avance que brinda múltiples ventajas tiene que ir la seguridad que le brindamos a la misma, ya que también trae consigo riesgos, sin embargo, muchas veces olvidamos esto último y ahí es donde pueden surgir grandes problemas para nuestras organizaciones.

ANTECEDENTES DEL PROBLEMA

En esta nueva realidad surgen interrogantes acerca de la seguridad de la información, de los equipos tecnológicos de nuestras empresas, de la información que poseemos, etc. Aspectos como estos hacen que se torne fundamental conocer el estado de la ciberseguridad en nuestras organizaciones y tomar acciones al respecto.

DEFINICIÓN Y DESCRIPCIÓN DEL PROBLEMA

El desarrollo explosivo de las tecnologías de la información y la comunicación (TIC), referidas fundamentalmente a la informática y las telecomunicaciones ha modificado radicalmente las labores diarias humanas y ha transformado los patrones de comportamiento y las relaciones sociales. Los beneficios que las TIC aportan a la sociedad actual son diversos y evidentes, sin embargo, el amplio desarrollo de estas tecnologías ofrece también un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Han surgido nuevas maneras de atentar contra la privacidad y el patrimonio de las personas y las empresas, y para cometer delitos de tipo tradicional en formas no tradicionales. Los llamados delitos informáticos, que constituyen actos delictivos que se

cometen con la ayuda de las TIC y que aumentan los riesgos en el ciberespacio y ponen en entredicho la seguridad informática, se han ido multiplicando en los últimos años de manera exponencial.

En Costa Rica la seguridad informática, aunque en los últimos años aparece con mayor frecuencia en la cotidianidad de las personas y las organizaciones que enfrentan situaciones concretas de ataques informáticos, no ha sido abordada de manera integral ni ha constituido materia de atención explícita por parte de una población y de una institucionalidad que cada vez con mayor frecuencia e intensidad emplea las tecnologías de la información y la comunicación. En general, la ciberseguridad se circunscribe a la esfera de los expertos y no se ha avanzado lo suficiente en el desarrollo de una cultura colectiva en este campo.

Dada la necesidad y la importancia que presentan las empresas en la actualidad de contar con medidas preventivas y correctivas ante las amenazas de ciberseguridad que surgen conforme la tecnología evoluciona, nos surge la siguiente interrogante:

¿Cómo diseñar una estrategia de la gestión de la ciberseguridad para disminuir los impactos cibernéticos de las PYMES de Costa Rica, según el “Código de mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones”?

JUSTIFICACIÓN

Esta investigación pretende determinar la situación real de la micro, pequeña y mediana empresa de Costa Rica, con respecto a la madurez en el ámbito de la ciberseguridad. Esto aporta un valor agregado bastante alto, ya que puede ser de utilidad para que usuarios y entidades tomen un mayor grado de conciencia acerca de la importancia e impacto que este tema genera en la actualidad, y como este va aumentando conforme adoptamos las nuevas tecnologías en nuestras actividades diarias, además, contribuye a la búsqueda de mejoras en cuanto a las medidas ya establecidas que se toman en ambos casos, si es el caso que existan, caso contrario, contribuye a la generación y aplicación de estas.

La importancia de esta investigación radica, entonces, en el impacto social que pudiera tener en un futuro ya que la información obtenida puede ser utilizada como referencia para las PYMES.

OBJETIVOS

OBJETIVO GENERAL

Proponer una guía de controles en seguridad de la información que sirva de base para las PYMES de Costa Rica.

OBJETIVOS ESPECÍFICOS

- Detallar los elementos que componen el concepto de seguridad de la información en las organizaciones.
- Analizar los riesgos de seguridad de la información que presentan las PYMES.
- Identificar las barreras organizacionales para la gestión de la seguridad de la información.
- Diseñar una guía de controles para la gestión de la seguridad de la información.

ALCANCE Y LIMITACIONES

ALCANCE

El alcance del proyecto establece la identificación de los riesgos de seguridad de las PYMES, diseñando una guía base de tratamiento de riesgos que le permitan a la organización controlar y disminuir los riesgos de seguridad analizados, dicho análisis se realizó tomando como base una sola empresa.

LIMITACIONES

- La muestra en la que se basarán los resultados de la encuesta es de 10 empresas, ya que solo esta cantidad se encontró disponible para responder la encuesta.

ESTADO DE LA CUESTIÓN

Cervantes, Ballesteros y Hernández (2012) en su investigación, “Mercado de trabajo para los profesionistas de la Contaduría y la administración: una visión global”, tienen como objetivo el definir el concepto de PYME y presentar las principales características de estas en un ámbito general, lo cual es indispensable de saber, ya que toda la presente investigación utiliza dichas empresas como base; unido a esta investigación, Laura Patiño Steffani, en su estudio sobre “Ventajas y desventajas de las PyMes” menciona una serie de aspectos importantes tanto a favor, como en contra, que presentan las PYMES, lo cual contribuye a tener un mejor entendimiento de estas empresas, conociendo así, sus fortalezas, así como sus debilidades.

Por otra parte, M. Dini y G. Stumpo (2018), proveen información relevante del Sistema de la Integración Centroamericana (SICA) y todos los países que esta incluye (Belice, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, y la República Dominicana), brinda diferentes estadísticas en cuanto al desarrollo de las PYMES en el sector centroamericano y sus diferentes sectores, por ejemplo, productivo, etc.

Del Ministerio de Economía, Industria y Comercio (MEIC), se tomó la conceptualización y definición específica de PYMES en Costa Rica, ya que como se ha mencionado anteriormente, esta varía de país en país; a su vez, este tema se ve reforzado por el Decreto Ejecutivo No 37721, el cual tiene como objetivo, establecer los criterios cuantitativos para definir a las PYMES con base a sus ventas, activos y empleo.

Para un mayor y profundo análisis de las PYMES en Costa Rica, se obtuvo información del Directorio de Empresas y Establecimiento (DEE) del INEC, donde se contabiliza el número de empresas registradas en el país y junto a esto, se utilizó el Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica 2018 (UCR, 2018), para obtener una serie de estadísticas nacionales con respecto a diferentes aspectos de suma importancia, entre estos: actividad económica, ubicación geográfica, también se obtuvieron datos del módulo de tecnologías de información, con el fin de evaluar el nivel de madurez con el que se cuenta actualmente en el país en estos temas.

M. Kuwayama, Y. Ueki y M. Tsuji (eds.) (2005), en su informe “Information Technology for Development of Small and Medium-sized Exporters in Latin America and East Asia” para la Comisión Económica para América Latina y el Caribe (CEPAL, mencionan una serie de aspectos por los cuales las compañías adoptan las tecnologías de información, así como, aspectos por los cuales los gobiernos y las instituciones públicas deben proporcionar acceso a las tecnologías de la información.

Se consultó ISACA y el International Telecommunication Union (2010), con el fin de obtener definiciones de la ciberseguridad en general y obtener información importante como los pilares de la seguridad, definición de seguridad de la información y la diferencia entre esta última y la ciberseguridad.

Del Cisco, SMB Security Service, 2018, se obtuvieron datos acerca de los ataques que las pequeñas y medianas empresas han sufrido.

Y, por último, se obtuvo del estudio “América Latina y la protección de datos personales: hechos y cifras (1985-2014)” (Remolina, 2014), el nivel de madurez con el que cuentan los países de América Latina respecto al tema de ciberseguridad, si tienen algún tipo de protección de datos en sus constituciones, algunos casos específicos que se presentan también.

CAPÍTULO II: MARCO TEÓRICO

A continuación, se presentan las bases teóricas sobre las cuales se va a fundamentar el trabajo investigativo.

¿QUÉ ES UNA PYME?

PYME es el acrónimo empleado para agrupar al parque empresarial compuesto por micro, pequeñas y medianas empresas. Estas siglas son de fácil reconocimiento a nivel internacional, sin embargo, aun no existe una definición homogénea entre países o entre organismos internacionales como el Banco Mundial (BM), el Banco Interamericano de Desarrollo (BID), la Organización Internacional del Trabajo (OIT), CEPAL.

En su concepción más amplia una PYME, es una unidad económica productora de bienes y servicios, dirigida por su propietario, de una forma personalizada y autónoma, de pequeña dimensión en cuanto a número de trabajadores y cobertura de mercado.

Las empresas se agrupan basado en diferentes criterios, los cuales pueden diferir de país a país o incluso, del sector económico donde se localizan estas empresas. No obstante, existen tres variables que permiten clasificar a las empresas de una manera mas sencilla. Estas son:

1. Número de empleos
2. Ventas brutas anuales
3. Valor de los Activos

Basado en las variables mencionadas anteriormente, cada país define sus PYMES otorgándole sus propios pesos relativos a los criterios.

De manera general, todas las PYMES comparten en su mayoría las mismas características, según Cervantes, Ballesteros y Hernández (2012), entre estas se pueden mencionar:

- El capital es proporcionado por una o dos personas que establecen una sociedad y por lo general son de carácter familiar.

- Los propios dueños dirigen la marcha de la empresa; su administración es empírica.
- Dominan y abastecen un mercado más amplio, aunque no necesariamente tiene que ser local o regional, ya que muchas veces llegan a producir para el mercado nacional e incluso para el mercado internacional.
- Obtienen algunas ventajas fiscales por parte del Estado que algunas veces las considera causantes menores dependiendo de sus ventas y utilidades.
- Su tamaño es pequeño o mediano en relación con las otras empresas que operan en el ramo.
- Personal poco calificado o no profesional.
- Poca visión estratégica y capacidad para planear a largo plazo.
- Falta de información acerca del entorno y el mercado.
- Falta de innovación tecnológica, puede deberse a falta de recursos, o por no contar con el espíritu innovador necesario.
- Falta de políticas de capacitación, se considera un gasto, no una inversión, al no poder divisar las ventajas a largo plazo que puede generar.
- Tienden a realizar sus procesos de la misma forma con la idea de que cuando un método no funciona mal, se mantiene sin analizar si existen otros mejores.
- Falta de liquidez

Laura Patiño Steffani, en su estudio sobre “Ventajas y desventajas de las PyMes” (s.f.) menciona algunos puntos a favor que presentan las PYMES, estos son:

- Capacidad de generación de empleos.
- Asimilación y adaptación de tecnología.
- Contribuyen al desarrollo regional por su establecimiento en diversas regiones.
- Fácil conocimiento de empleados y trabajadores, facilitando resolver los problemas que se presentan por la baja ocupación de personal.
- Mantiene una unidad de mando permitiendo una adecuada vinculación entre las funciones administrativas y operativas.

- Producen y venden artículos a precios competitivos, ya que sus gastos no son muy grandes y sus ganancias no son excesivas

Y algunas desventajas son:

- Les afecta con mayor facilidad los problemas que se suscitan en el entorno económico como la inflación y la devaluación.
- Viven al día y no pueden soportar periodos largos de crisis en los cuales disminuyen las ventas.
- Son mas vulnerables a la fiscalización y control gubernamental, siempre se encuentran temerosas de las visitas de los inspectores.
- La falta de recursos financieros las limita, ya que no tienen fácil acceso a las fuentes de financiamiento.
- Tienen pocas o nulas posibilidades de fusionarse o absorber a otras empresas, es muy difícil que pasen al rango de medianas empresas.

PYMES EN CENTROAMÉRICA

En general, los países del Sistema de la Integración Centroamericana (SICA) — Belice, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, y la República Dominicana “son economías pequeñas, con tasas de crecimiento del PIB moderadas, fuertes tensiones en las cuentas fiscales y persistentes niveles de pobreza y desigualdad” (Dini y Stumpo, 2018, p. 441).

Según estudios del Sistema Regional de Información MIPYME de Centroamérica y la República Dominicana (SIRMIPYME), quien es la principal fuente de información para la caracterización de las MYPYME de Centroamérica, la clasificación de las empresas del SICA se realiza de la siguiente manera:

**Países del Sistema de la Integración Centroamericana (SICA):
clasificación de las micro, pequeñas y medianas empresas**

País	Variables	Microempresa	Pequeña	Mediana
	Empleados	Propietario menos de 5	5 - 19	20 - 50
Belice	Ventas en dólares de Belice	100 000<	100 000 - 500 000	500 000 - 1 500 000
	En dólares	50 000	250 000	750 000
	Inversión	50 000	150 000	500 000
Costa Rica	Empleo, ventas y activos	P <= 10	10 < P <= 35	35 < P <= 100
	Empleo	10	50	100
El Salvador	Ventas salarios Mínimos	482	4 817	No existe
	Anual	106 000	1 060 000	
Guatemala	Empleo	1 - 10	11 - 25	26 - 60
Honduras	Empleo	1 - 10	11 - 50	51 - 150
	Empleo	1 - 5	6 - 30	31 - 100
Nicaragua	Activos en córdobas	200 000	1 500 000	6 000 000
	En dólares	8 356	62 670	250 681
	Ventas (al año) en córdobas	1 000 000	9 000 000	40 000 000
	En dólares	41 780	376 000	1 671 000
Panamá	Empleo	1 - 5	6 - 20	21 - 100
	Ventas al año	150 000	150 000 - 1 000 000	1 000 000 - 2 000 000
República Dominicana	Empleo (estudios /normativa)	1 - 10	11 - 50	51 - 100
	Ventas en dólares	1 - 15	16 - 60	61 - 200
	Ventas en dólares	60 000	1 200 000	5 000 000

FIGURA 1. CLASIFICACIÓN PYMES

Fuente: MIPYMES en América Latina. Un frágil desempeño y nuevos desafíos para las políticas de fomento.

Es importante mencionar que, aunque los países pueden tener diferentes criterios para la clasificación de las empresas, todos se basan principalmente en el número de empleos para diferenciar entre micro, pequeñas y medianas empresas (Dini y Stumpo, 2018).

En todos los países más del 70% del total de las MIPYMES son empresas con menos de 10 trabajadores, siendo El Salvador quien mayor porcentaje tiene con un 97%, seguido por Honduras (96%), Panamá (90%), Belice (82%), Costa Rica (79%), Guatemala (79%) y República Dominicana (73%). El siguiente grupo predominante son las empresas entre 11 y 50 empleados siendo República Dominicana el país con mayor proporción de empresas en este segmento, con un 21%; seguido por Guatemala (16%), Costa Rica (16%), Belice (15%), Panamá (8%), Honduras (3%) y El Salvador (2%) (Dini y Stumpo, 2018).

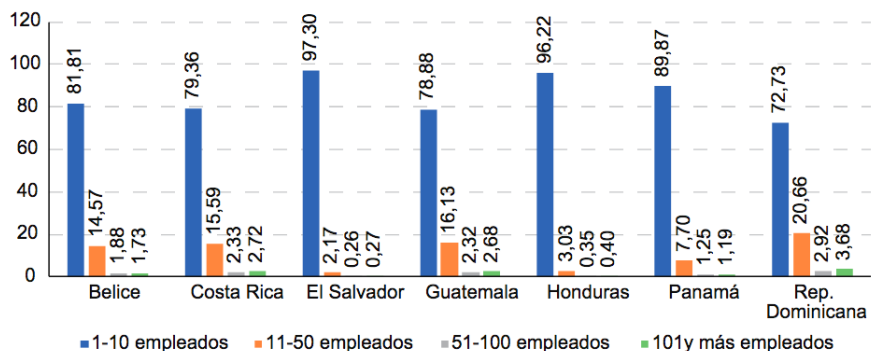


FIGURA 2. CANTIDAD DE EMPLEADOS

Fuente: MIPYMES en América Latina. Un frágil desempeño y nuevos desafíos para las políticas de fomento.

Los grupos de empresas entre 51 a 100 empleados y las mayores a 100, son mucho más escasas en la estructura empresarial en cada uno de los países, ya que en ningún caso superan el 3% del total de empresas y las que poseen más de 100 empleados llegan al 4%, siendo República Dominicana quien posee ambas cifras (Dini y Stumpo, 2018).

En cuanto al sector productivo donde operan, el mayor porcentaje le pertenece al sector de comercio con un 43% de las microempresas a nivel regional, en el caso de las pequeñas y medianas empresas, la participación es del 31% y el 25%, respectivamente (Dini y Stumpo, 2018).

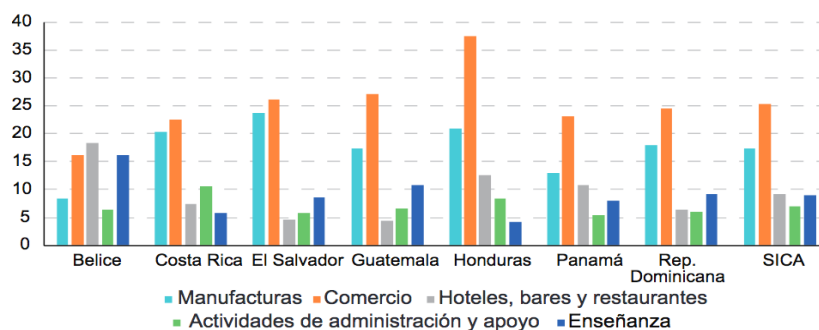


FIGURA 3. PYMES POR SECTOR

Fuente: MIPYMES en América Latina. Un frágil desempeño y nuevos desafíos para las políticas de fomento.

El SIRMIPYME ofrece información que ayuda a definir el perfil de los emprendedores y empresarios y han estimado que aproximadamente el 30% de las

personas ocupadas son trabajadores por cuenta propia, por ejemplo, Belice, Costa Rica y Panamá presentan porcentajes superiores al 20% mientras que en Honduras y República Dominicana representan más del 40% de la fuerza de trabajo del país. El sector con mayor nivel de autoempleo es el de la construcción (80%), seguido por el sector agropecuario (78%) y, en menor medida, el sector del transporte y el almacenamiento (71%) (Dini y Stumpo, 2018).

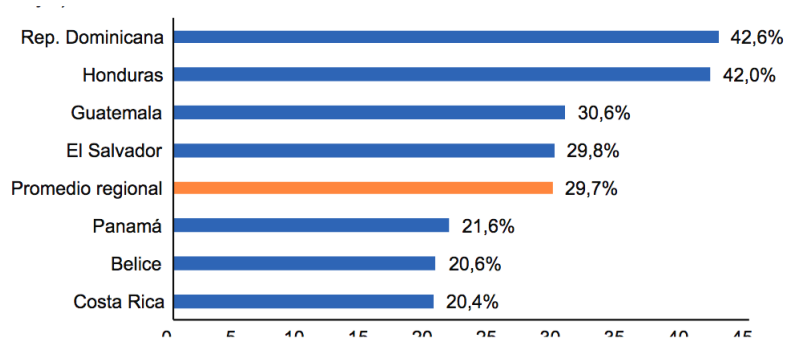


FIGURA 4. PERFIL DE EMPRENDEDORES

Fuente: MIPYMES en América Latina. Un frágil desempeño y nuevos desafíos para las políticas de fomento.

En resumen, podemos mencionar que PYMES son muy relevantes en términos de empleo y de número de empresas, con porcentajes sobre el total que superan en todos los casos el 70% del total de las empresas del país, gracias especialmente a las microempresas que caracterizan el tejido productivo de los países centroamericanos. Sin embargo, su relevancia es mucho menor en términos de producción o exportación. Su peso en los principales sectores económicos del país es grande, excepto en el sector industrial. Así, dado su volumen e importancia laboral asegura su relevancia económica, por lo que deben ser objeto prioritario de las políticas de desarrollo económico de los países de la región (Dini y Stumpo, 2018).

PYMES EN COSTA RICA

El Ministerio de Economía, Industria y Comercio (MEIC) basado en el artículo 3 de la Ley No 8262 de Fortalecimiento de las Pequeñas y Medianas Empresas y sus Reformas (2002), define una PYME como:

... toda unidad productiva de carácter permanente que disponga de los recursos humanos los maneje y opere, bajo las figuras de persona física o de persona jurídica, en actividades industriales, comerciales, de servicios o agropecuarias que desarrollen actividades de agricultura orgánica.

Las empresas se clasifican según actividad empresarial como industriales, comerciales y de servicios, utilizando la Clasificación Industrial Internacional Uniforme de todas las Actividades Económicas (CIIU).

En Costa Rica, el reglamento a la ley citada anteriormente (Decreto Ejecutivo No 37721), establece los criterios cuantitativos para definir a las Pymes con base a sus ventas, activos y empleo; esta definición propone un ponderador del tamaño “p”, a partir de la variable empleo. Basado en esto, se define el tamaño de la PYME de la siguiente manera:

- Microempresa si el resultado es igual o menor a 10.
- Pequeña empresa si el resultado es mayor que 10 pero menor o igual a 35.
- Mediana empresa si el resultado es mayor que 35 pero menor o igual a 100.

En Costa Rica, las pequeñas y medianas empresas, PYMES, ocupan un papel muy importante en la economía, debido a que son fuentes de empleo e ingresos, estas conforman el 94% de las empresas formales que hay en Costa Rica.

Durante el 2018, de acuerdo con la información del Directorio de Empresas y Establecimiento (DEE) del INEC, el total de registros de empresas de Costa Rica estuvo conformado por 35.429 empresas, de las cuales un 78,4% corresponde a empresas

clasificadas como micro, un 17,1% corresponde a empresas pequeñas y un 4,5% a empresas medianas.

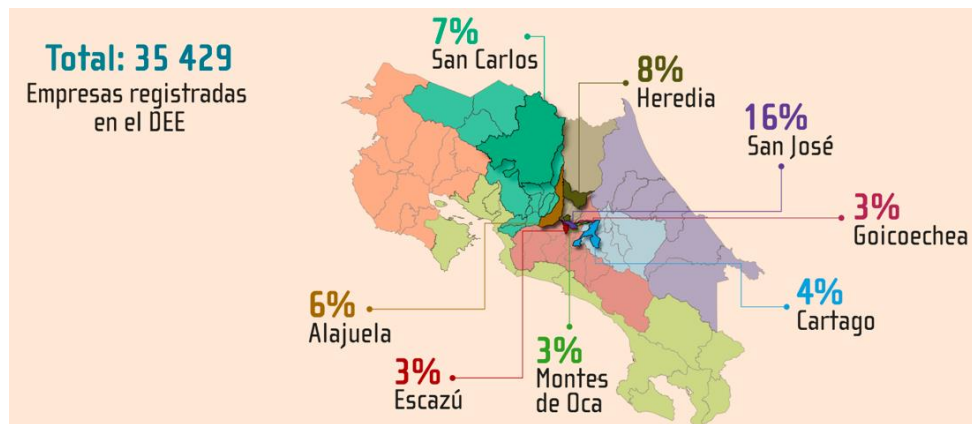


FIGURA 5. EMPRESAS INSCRITAS

Fuente: INEC-Costa Rica. Directorio de Empresas y Establecimientos, 2018.

ACTIVIDAD ECONÓMICA

Según el Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica 2018 (UCR, 2018), en cuanto al sector productivo, las empresas realizan, principalmente, actividades relacionadas con comercio y, las menos comunes son minas y canteras, más detalladamente, un 47,9% de las empresas se dedican a prestar servicios, un 27,3% a comercio y reparación de vehículos, un 0,4% a suministros de electricidad, agua y gestión de desechos, un 8,0% a agricultura, silvicultura y pesca, un 9,4% construcción, un 6,8% manufactura y un 0,2% a minas y canteras.

Costa Rica: total de empresas^{1/}, según actividad económica, por intervalo de personas trabajadoras, 2018

Descripción ^{2/}	Empresas	Intervalo de trabajadores				
		1 a 5	6 a 30	31 a 100	Más de 100	Ignorado ^{3/}
Total general	35 429	22 722	8 647	2 238	1 115	707
Actividades agropecuarias	2 534	1 749	549	114	114	8
Manufactura	3 447	1 738	1 088	359	230	32
Construcción	966	395	386	124	53	8
Comercio	12 281	8 579	2 788	573	192	149
Transporte y almacenamiento	1 049	445	362	165	72	5
Alojamiento y de servicios de comidas	4 189	2 803	1 069	175	62	80
Información y comunicaciones	546	206	214	77	39	10
Actividades financieras	508	220	185	65	36	2
Actividades inmobiliarias	596	421	133	26	11	5
Actividades profesionales	2 175	1 595	406	104	59	11
Servicios administrativos	1 271	529	391	182	153	16
Enseñanza	770	270	309	138	42	11
Salud y asistencia social	1 809	1 538	214	22	19	16
Actividades artísticas y recreativas	429	276	111	31	10	1
Otros servicios	1 813	1 526	212	35	9	31
Otros ^{4/}	329	187	114	22	6	0
Ignorado ^{5/}	717	245	116	26	8	322

FIGURA 6. EMPRESAS POR ACT ECONÓMICA

Fuente: INEC- Costa Rica. Directorio de Empresas y Establecimientos, 2018.

UBICACIÓN GEOGRÁFICA

En cuanto a la distribución geográfica de las empresas, la provincia con mayor cantidad de empresas es San José con un 41,3% y la que tiene menor cantidad es Limón, con un 4,4%; el resto de las provincias tienen los siguientes números: 20,9% en Alajuela, 7,9% en Cartago, 10,8% en Heredia, 6,9% en Guanacaste, 7,5% en Puntarenas, y 0.3% no quiso indicar el lugar de ubicación de la empresa (UCR, 2018).

Gráfico N° 2 Ubicación de las empresas por provincia

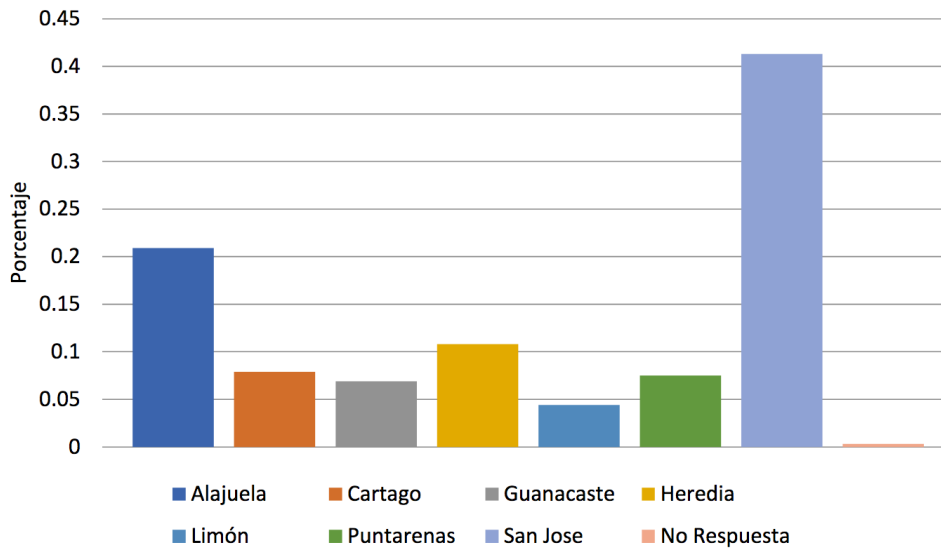


FIGURA 7. EMPRESAS POR PROVINCIA

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

REGISTRO DE PYMES Y PYMPAS

Al determinar la cantidad de empresas registradas en el Sistema de Información Empresarial Costarricense (SIEC) del Ministerio de Economía, Industria y Comercio (MEIC) con la condición PYME fue posible apreciar que el 38,0% de las microempresas se encontraban registradas ante el MEIC como PYME, en el caso de las pequeñas un 49,1% y las medianas un 34,2%. En cuanto las empresas registradas ante el Ministerio de Agricultura y Ganadería (MAG), los porcentajes de inscripción son considerablemente más bajos, en el caso de las Micro es un 7,1% para las pequeñas un 10,6% y para las medianas un 14,9% (UCR, 2018).

TECNOLOGÍAS DE LA INFORMACIÓN

Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesarla para poder calcular resultados y elaborar informes. Algunos de los elementos más utilizados dentro del

ámbito de las TIC son las computadoras, el teléfono fijo, los teléfonos móviles, y con mayor incidencia los teléfonos inteligentes y por supuesto el internet.

Las TIC han transformado la forma en que las personas se relacionan con el entorno, así como la forma de trabajar y de gestionar recursos. Las TIC son un elemento clave para hacer que el trabajo sea más productivo: agilizando las comunicaciones, sustentando el trabajo en equipo, gestionando las existencias, realizando análisis financieros, y promocionando los productos y servicios en el mercado.

Bien utilizadas, las TIC permiten a las empresas producir más cantidad, mayor calidad, y en menos tiempo. Permite a las PYMES ser más competitivas en el mercado, y además tienen el potencial de impactar positivamente en el crecimiento económico y el empleo a través del aumento de la eficiencia y la productividad, dándole mayor oportunidad a sus propietarios/as de disponer de tiempo libre para otras actividades.

IMPORTANCIA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LAS PYMES

A nivel general, se reconoce que las pequeñas y medianas empresas representan uno de los sectores clave para mejorar los niveles de empleo en la mayor parte de las economías. Además, estas compañías también pueden tener un espacio protagónico en la creación de fuentes de innovación y de ventajas competitivas en nuevas actividades de producción o áreas de servicio; sólo mediante el fortalecimiento de las PYMES se puede llegar a tener un sector productivo más equilibrado.

Una de las maneras de promover el desarrollo y fortalecimiento de estas empresas es mediante la creación de condiciones que les permitan forma parte del intercambio de bienes servicios a nivel internacional. Sin embargo, para crear las condiciones de participación adecuadas en el contexto actual de una economía mundial globalizada y automatizada, es fundamental que las PYMES estén preparadas para aceptar nuevos niveles tecnológicos y adoptar nuevos estándares en cuanto a estructura organizativa, intercambio de información y comunicaciones. Es por esto, que las PYMES necesitan incorporar tecnología a sus estrategias de negocio, para poder ser más productivas y aumentar su grado de eficiencia.

Las empresas empiezan a darse cuenta de que, ante la globalización, puede decirse que el uso de tecnología ya no es un lujo, y pasa a formar parte integral del modelo de negocio de las empresas y en particular del segmento PYME. Ante ello surgen necesidades que para satisfacerlas necesitan el desarrollo e implantación de proyectos que involucren a las tecnologías de información. Entre estas necesidades se puede citar:

- Mejorar producción y administración productiva
- Mejorar administración de la empresa
- Mejorar integración funcional de la empresa
- Mejorar relación con clientes

Como se puede notar, el común denominador de estas necesidades es la mejora, lo que implica automatización y eficiencia en los procesos tanto internos como externos, lo cual se logra con la implementación de herramientas tecnológicas.

En el informe de un proyecto de la CEPAL se evaluaron varios estudios de casos sobre la incorporación de tecnologías de la información por parte de las PYMES en Asia y América Latina; y se concluyó que las principales razones estaban vinculadas a la efectividad de las TIC para facilitar la internacionalización de estas. En el documento se establece que las compañías privadas adoptan estas tecnologías para:

- Lograr un mayor acceso a la información.
- Mejorar la administración a nivel interno.
- Mejorar la gestión de los productos y el control de calidad.
- Aumentar la productividad mediante una mejora en la administración interna.
- Facilitar la cooperación con otras empresas y alcanzar economías de escala.
- Descubrir nuevas oportunidades de negocios.

Además, del estudio se concluye que los gobiernos y las instituciones públicas deben proporcionar acceso a las tecnologías de la información para:

- Mejorar la competitividad de las pymes y desarrollar conglomerados empresariales.
- Promover la cooperación entre las grandes empresas y las PYMES, y entre PYMES.
- Reducir los costos de los procedimientos comerciales para los sectores público y privado.
- Mejorar la productividad y la transparencia del sector público.
- Facilitar la implementación de políticas de fomento y acuerdos comerciales.

Según los estudios, en el sector público existen dos metas en el uso de estas tecnologías: una es la implementación de políticas económicas y sociales más efectivas, mientras que la otra es la necesidad de mejorar la gestión a nivel interno (Kuwayama, Ueki, Tsuji, 2005).

TECNOLOGÍAS DE LA INFORMACIÓN EN LAS PYMES DE COSTA RICA

CONECTIVIDAD A INTERNET

De acuerdo con el Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica 2018 (UCR, 2018), el 82,0% de las empresas cuenta con computadoras conectadas a internet. Analizando estos resultados más específicamente por tamaño de empresa, las micros indicaron en un 79,5% tener computadoras conectadas a internet, las pequeñas lo afirman en un 90,2% y las medianas en un 93,3% (UCR, 2018).

Cuadro N° 35 Se cuenta con computadoras conectadas a internet

Respuesta	Porcentaje
Sí	82
No	17.7
No responde	0.4
Total	100

FIGURA 8. COMPUTADORAS CON INTERNET

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

En cuanto al ancho de banda, un 67% de las empresas cuenta con menos de 10 GB de conexión, mientras que sólo un 10% tiene conexiones superiores a los 10 GB. Analizando estos datos de acuerdo con el tamaño de la empresa, en promedio las micros indican tener en un 69,3% un ancho de banda de 10 GB, las pequeñas un 58,3% tienen el mismo ancho de banda y las medianas un 63,5% (UCR, 2018).

Gráfico N° 13 ¿Cuál es el ancho de banda que tiene su empresa?

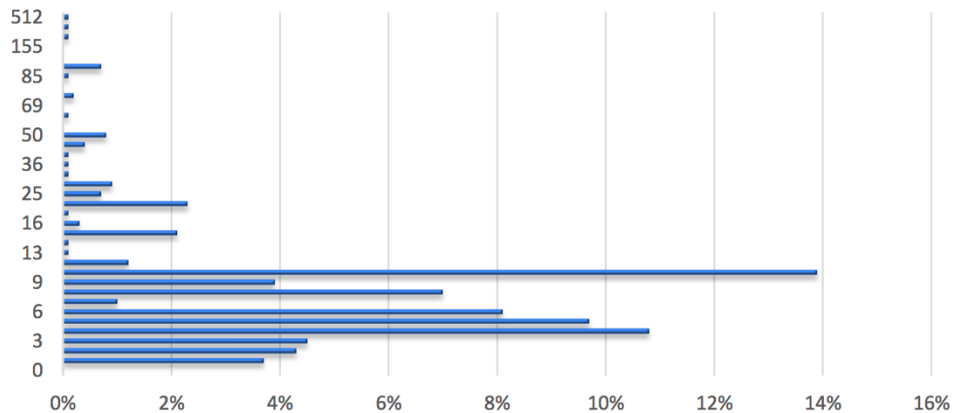


FIGURA 9. ANCHO DE BANDA

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

EQUIPAMIENTO

En cuanto a la antigüedad del equipo informático en las empresas, el estudio indica que un 14,7% no cuenta con equipo informático, el 11,9% cuenta con menos de 1 año de antigüedad, el 23,8% entre 1 y 2 años, el 19,8% entre 2 y 3 años, y el 28,1% más de 3 años (UCR, 2018).

Cuadro N° 36 Con respecto al equipo de informática que posee la empresa los mismos tienen

Respuesta	Porcentaje
No posee	14.7
Menos de un año	11.9
De 1 a menos de 2 años	23.8
De 2 a menos de 3 años	19.8
Tres o más años	28.1
No responde	1.7
Total	100

FIGURA 10. EDAD DEL EQUIPO

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

El comportamiento por tamaño de empresa indica que, del equipo de informática de las microempresas, un 12,1% tiene menos de un año, un 21,8% de 1 a 2 años, un 19,0% entre 2 y 3 años y un 28,8% más de tres años. En el caso de las empresas pequeñas indica que 9,8% tiene menos de 1 año, 28,9% entre 1 y 2 años, un 22,2% entre 2 y 3 años y un 28,6% más de tres años. Y para el caso de las empresas medianas un 15,5% menos de 1 año, un 40,8% entre 1 y 2 años, un 24,0% entre 2 y 3 años y un 15,2% más de tres años (UCR, 2018).

SOFTWARE Y LICENCIAMIENTO

En cuanto al tipo de software, un 77,5% cuenta con algún tipo de software libre dentro de la empresa, cerca de un 40,7% cuenta con firma digital, un 46,8% cuenta con página web (UCR, 2018).

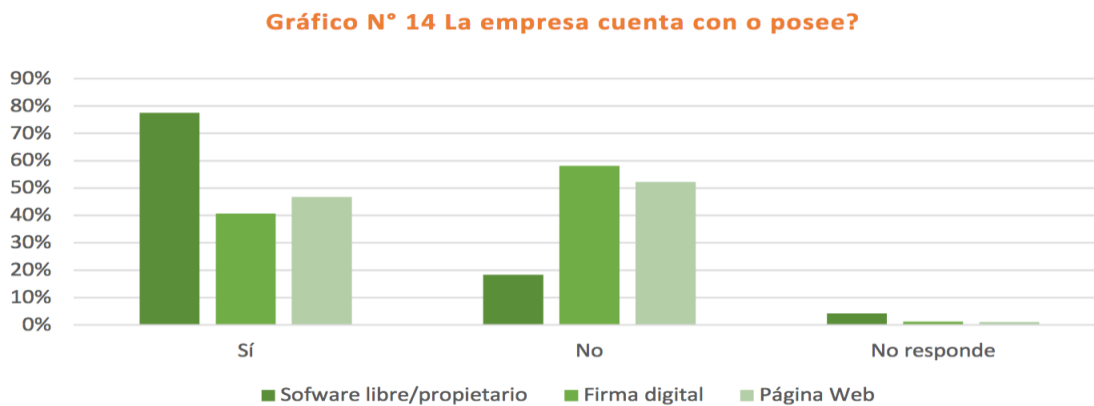


FIGURA 11. SOFTWARE/LICENCIAMIENTO

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

En cuanto al uso de redes sociales, los resultados indican que el 59,6% posee Facebook, un 12,5% Instagram y un 7,0% tiene Twitter (UCR, 2018).

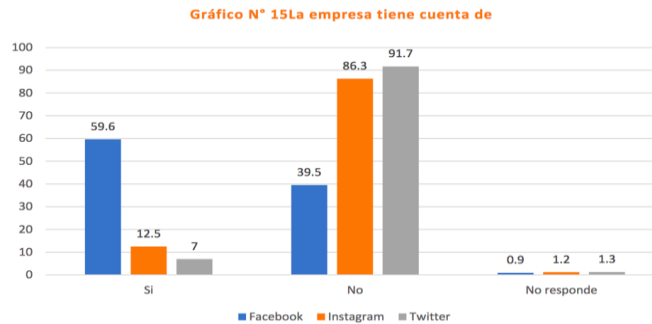


FIGURA 12. USO DE REDES SOCIALES

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

Además, un 20,5% vende productos o servicios a través de la página Web, un 41,5% paga o compra a los proveedores por internet, un 21,3% ha recibido cursos en línea, un 14,6% tiene un sistema de puntos de venta, un 53% utiliza las redes sociales para publicitar información de la empresa, un 39,9% ofrece internet gratis para los clientes, y un 36% realiza ventas o negocios por medio de la plataforma de WhatsApp (UCR, 2018).

Sobre la consulta de cuanto es el porcentaje de ventas que se realizan por este medio, el 48% destina un 20% de las ventas, un 24,7% destina entre un 25 y 50% y un 16,5% destina entre un 50 y 90% de sus ventas (UCR, 2018).

REDES SOCIALES Y MODELOS DE NEGOCIO EN INTERNET

Analizando el uso de la herramienta de WhatsApp como medio para ventas, es interesante observar que tanto las empresas micros como medianas indican en un 37% que lo emplean, a nivel general un 36,0% afirmó que realiza ventas por medios WhatsApp (UCR, 2018).

Cuadro N° 38 En la empresa se realizan ventas por WhatsApp o mensaje de texto

Respuesta	Porcentaje
Sí	36
No	62.7
No responde	1.3
Total	100

FIGURA 13. VENTAS POR WHATSAPP/SMS

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

De las empresas que afirmaron que si realizan ventas por este medio (WhatsApp), un 42,5% indica que el porcentaje de ventas es cercano al 10%, un 33,1% indica que es entre 10 y 50% de las ventas, y un 16,6% indica que entre un 50 y 95% de sus ventas corresponde a este medio (UCR, 2018).

Gráfico N° 16¿Cuál es el porcentaje de ventas que realiza por este medio?

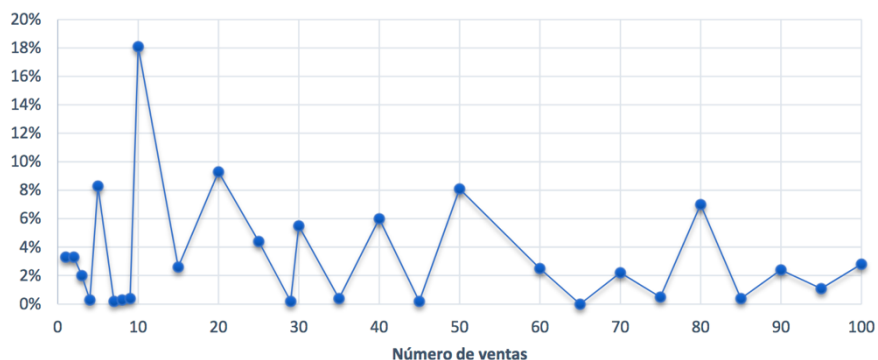


FIGURA 14. NÚMERO DE VENTAS

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

Analizando estos resultados de acuerdo con el tamaño de la empresa se puede apreciar que, para el caso de las micros un 35,3% vende cerca de un 10% por este medio, un 35,8% de las empresas vende entre 10% y el 50% y un 17,9% entre 50 y 98%. Para el caso de las empresas pequeñas se observa que destinan un 10% el 39,7% de las empresas, entre 10 y 50% un 29,0% y un 16,5 entre 50 y 85%. Para el caso de las empresas medianas se tiene que un 38,2% de las mismas indicó vender cerca de un 10% por este medio, entre un 10 y 50% un 49.1% y entre 50 y 96% un 9,4%. De igual manera se les consultó a las empresas si realizan ventas en redes sociales y un 17,0% de las mismas indicó que si (UCR, 2018).

Cuadro N° 39 En la empresa realizan ventas por medio de redes sociales

Respuesta	Porcentaje
Sí	17
No	80.9
No responde	2.1
Total	100

FIGURA 15. VENTAS POR REDES SOCIALES

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

En cuanto al comportamiento por tamaño las micros indicaron en un 17% que realizan ventas por redes sociales, un 14,7% las empresas pequeñas y un 25,4% las empresas medianas (UCR, 2018).

Gráfico N° 17: ¿Cuál es el porcentaje de ventas que realiza por este medio?

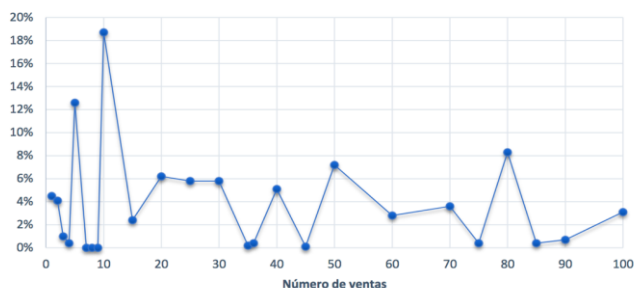


FIGURA 16. NÚMERO DE VENTAS POR REDES

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

Un 70,4% de las empresas indicaron contar con un servicio de Banca Electrónica (UCR, 2018).

Cuadro N° 40 Actualmente la empresa tiene servicio de Banca Electrónica con algún Banco

Respuesta	Porcentaje
Sí	70.4
No	27.9
No responde	1.7
Total	100

FIGURA 17. SERVICIO DE BANCA ELECTRÓNICA

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

De estas empresas, un 51,6% indicó tener servicios con el Banco Nacional, un 19,3% con Banco de Costa Rica, 18,9% con el BAC San José, un 1,2% con el Banco Popular, un 1,9% con Davivienda, y un 1,1% con Scotiabank. A la consulta de si las

empresas utilizan teléfonos inteligentes para gestionar pagos a entidades financieras un 21,4% lo afirmó de manera positiva (UCR, 2018).

Cuadro N° 41 Con cual entidad usa estos servicios

Bancos	Porcentaje
Banco Nacional	51.6
Banco Popular	1.2
Banco de Costa Rica	19.3
BAC /Credomatic/ BAC San José	18.9
Scotiabank	1.1
Davivienda	1.9
Banco Promerica	0.5
Mutual Alajuela	0.1
Lafisse	0.3
Bancos públicos	0.9
Bancos privados	0.2
Todos los bancos	0.7
BCT	0.3
Banco Mundial	0.1
Bancos extranjeros	0
No responde	2.8
Total	100

FIGURA 18. ENTIDADES

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

Analizando de acuerdo con el tamaño de la empresa un 70,2% de las micros indicaron contar con un servicio de banca electrónica un 70% de las pequeñas y un 75,9% de las medianas. En cuanto a la principal entidad con la cual poseen el servicio para el caso de las micros se encuentra, Banco Nacional (52,0%), Banco de Costa Rica (19,8%), BAC San José (19,4%). Para el caso de las empresas pequeñas los porcentajes son, Banco Nacional (51,6%), Banco de Costa Rica (17%), BAC San José (17,7%) y para el caso de las empresas medianas el porcentaje fue: Banco Nacional (45,8%), Banco de Costa Rica (20%), BAC San José (17,3%). Se consultó si las empresas utilizan aplicaciones para teléfonos inteligentes para gestionar los pagos a entidades financieras, el 22,6% de las empresas micros indicó usar este tipo de aplicaciones, un 16,0% de las empresas pequeñas y un 24,0% de las empresas medianas (UCR, 2018).

Cuadro N° 42 Utilizan aplicaciones para teléfonos inteligentes para gestionar pagos a entidades financieras

Respuesta	Porcentaje
Sí	21.4
No	76.5
No responde	2.1
Total	100

FIGURA 19. USO DE TELÉFONOS PARA PAGOS

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

Por último, se consultó si la empresa contrataba algún tipo de soporte externo u *outsourcing* para la gestión y administración del negocio a lo cual un 19,8% indicó que si lo hacen. Analizando los resultados de acuerdo con el tamaño de la empresa, un 20,2% de las micros indicó usar este tipo de soporte, un 16,7% de las pequeñas y un 24,5% de las empresas medianas (UCR, 2018).

Cuadro N° 43 La empresa contrata algún soporte externo para la gestión del negocio

Respuesta	Porcentaje
Sí	19.8
No	79.1
No responde	1.1
Total	100

FIGURA 20. SOPORTE EXTERNO

Fuente: Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica, 2018.

CIBERSEGURIDAD

Según la asociación de profesionales de seguridad ISACA la ciberseguridad se entiende como: “Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena y se transporta mediante los sistemas de información que se encuentran interconectados”. Asimismo, la International Telecommunication Union (ITU) establece que la ciberseguridad es:

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguarda de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y herramientas tecnológicas que pueden utilizarse para proteger los activos de la organización y los usuarios en el entorno de ciberespacio (2010, p.5).

La ciberseguridad garantiza que se alcancen y mantengan los pilares de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno (UIT, 2010). Los pilares de seguridad son:

- Disponibilidad
- Integridad
- Confidencialidad

La ciberseguridad ofrece un foco de protección para la información digital que se encuentra entre sistemas interconectados. Como consecuencia, se encuentra en la seguridad de la información.

Para poder establecer la diferencia con la seguridad de la información, es necesario revisar varios conceptos más que permiten tener el contexto general. Según la Real Academia Española (RAE), la seguridad se puede definir como: “Libre o exento de todo peligro, daño o riesgos”. Sin embargo, es una condición ideal, ya que en la realidad no es posible tener la certeza de que se puedan evitar todos los peligros.

El principal propósito de seguridad en todos los ámbitos de aplicación es el de reducir riesgos hasta un nivel que se pueda aceptar y que los interesados puedan mitigar las amenazas latentes. Es decir, la seguridad también entiende que las actividades se encuentran destinadas a proteger del peligro a los activos sensibles de la organización.

La información se puede encontrar en diferentes formatos, por ejemplo, en formato digital, físico, etc. No importa la forma o el estado, la información requiere que se cumpla una serie de medidas de protección que sean adecuadas según la importancia y la criticidad de esta, esto es especialmente importante en el ámbito de la seguridad de la información.

CIBERSEGURIDAD DE LAS PYMES

Hace varios años que se ha identificado la necesidad de aumentar los esfuerzos orientados a la protección a pequeñas y medianas empresas frente a ciberataques, siendo éstas un blanco importante para cibercriminales. Esto ocurre, en gran medida, debido a que, por lo general, las PYMES no cuentan con los mismos niveles de protección de empresas grandes. Existen diversas razones para este fenómeno, entre las cuales podemos citar:

- Las PYMES suele creer que no son de interés para los criminales, y que por tanto no serán blancos de un ciberataque.
- Cuentan con recursos limitados (recursos financieros, humanos, de tiempo y de conocimiento).
- La gestión de la seguridad de la información, como un proceso continuo y sistemático, no está incorporado en sus procesos de negocio.
- No conocen mecanismos simples y prácticos para la protección de sus activos, que estén adaptados a su realidad.
- La mayoría de las normas, estándares, y guías de seguridad no están pensados para PYMES y son difíciles de ejecutar.

Cuando las noticias reportan ataques de ciberseguridad, generalmente se enfocan en las pérdidas que sufren las grandes organizaciones. Y se pone poca atención en el impacto a las pequeñas y medianas empresas. Esto crea la falsa idea de que estas empresas no son blancos atractivos de los hackers, cuando en realidad también generan ganancias.

De acuerdo con Cisco, en los últimos 12 meses, 61% de los pequeños negocios ha experimentado un ciberataque y un 52% ha sufrido ataques de ransomware. Al igual que existen grandes organizaciones profesionales de cibercriminales, también existen pequeños grupos de hackers, cuyo objetivo son las empresas u organizaciones que no poseen infraestructura de ciberseguridad.

Actualmente, las PYMES se enfrentan a los mismos retos en seguridad que las organizaciones más grandes, (ransomware, prevención de intrusos, spam, phishing, malvertising, etc.); sin embargo, no cuentan con los recursos para invertir en una infraestructura robusta.

CIBERSEGURIDAD DE LAS PYMES EN AMÉRICA LATINA

La conciencia de la importancia de desarrollar estrategias de seguridad cibernética está aumentando entre los países de la región de América Latina y del Caribe (ALC). Algunos de ellos ya tienen una estrategia en operación, como Colombia, Jamaica, Panamá y Trinidad y Tobago; otros países están en proceso de su desarrollo, como

Costa Rica, Dominica, Perú, Paraguay y Suriname. El nivel de madurez de estas estrategias varía, incluso en términos de proporcionar un marco para la cooperación entre los organismos gubernamentales y con actores externos.

Una de las principales preocupaciones planteadas en los países de ALC ha sido la definición y penalización de los delitos cibernéticos, ya sea por la creación de nuevas leyes o actualización de las ya existentes. Otra tendencia regulatoria en la región de ALC es una creciente preocupación por la protección de la privacidad en línea y los datos personales. A medida que Internet se ha vuelto esencial para el desarrollo socioeconómico de América Latina, las consecuencias de no protegerla pueden afectar la confianza de las actividades en línea, que tiene consecuencias potencialmente negativas para la economía de Internet y en la sociedad en su conjunto.

Según el estudio América Latina y la protección de datos personales: hechos y cifras (1985-2014) (Remolina, 2014), el 70% de los países de América Latina tienen algún tipo de protección de datos en sus constituciones. Por otra parte, distintos países, por ejemplo, Antigua y Barbuda, Argentina, Colombia, Costa Rica, México, Perú y Uruguay, ya han promulgado leyes de protección de datos y otros, como Brasil, están en proceso de redacción de estas. A pesar de esto, la retención de los datos obligatorios es una práctica cada vez más utilizada en la región y, en muchos casos, se pueden obtener datos almacenados sin una orden judicial.

En Argentina, una ley fue impugnada ante la Corte Suprema, debido a que autorizó la interceptación de teléfonos y comunicaciones electrónicas sin contar con directrices para la aplicación de las disposiciones. Además, se requiere que los datos se almacenen durante 10 años. La ley fue declarada inconstitucional por la Corte Suprema en 2009.

En Brasil, el Marco Civil de Internet, promulgado en 2014, ha sido considerado como un documento de avanzada que protege los intereses de los ciudadanos. No obstante, sus disposiciones relativas a la retención obligatoria de datos posiblemente podrían inclinar la balanza hacia las preocupaciones de seguridad sobre la privacidad y las libertades civiles. Según el Marco Civil, los registros de servicios y aplicaciones deben ser almacenados durante seis meses, mientras que los registros de conexión deben almacenarse durante un año.

En México, se promulgó en 2014 una ley de telecomunicaciones con diferentes disposiciones de retención de datos. Las autoridades pueden acceder a datos retenidos sin una orden judicial. Por otra parte, algunos datos deben almacenarse 24 meses. Esto corresponde a un aumento de 12 meses en comparación con la norma que ya operaba.

En Paraguay, un proyecto de ley conocido como “pyraweb” requiere proveedores de servicios de Internet para almacenar los metadatos de un año. Por otra parte, las autoridades no necesitaban una orden judicial para solicitar los datos. Después de enfrentarse a la presión política de los grupos de la sociedad civil, el proyecto de ley fue rechazado por el Senado.

SISTEMA DE GESTIÓN DE LA SEGURIDAD

Un Sistema de Gestión de Seguridad de la Información (SGSI) es el conjunto de políticas y procesos que permiten gestionar eficazmente todas las mejoras que se emprendan en la organización en materia de seguridad de la información y consta de todos los elementos necesarios para planificar, definir, implantar, verificar y supervisar las medidas de seguridad necesarias para cumplir los requisitos de seguridad de la organización.

Por lo tanto, un Sistema de Gestión de Seguridad de la Información comprende el diseño, implantación y mantenimiento de un conjunto de procesos que permitan gestionar eficientemente la accesibilidad de la información, buscando asegurar y mantener los niveles de confidencialidad, integridad y disponibilidad de los activos de información y minimizando a la vez los riesgos de seguridad de la información. Entre sus ventajas se encuentran:

- Menor riesgo de pérdida de información.
- Revisión continua de los riesgos de forma periódica.
- Uso de una metodología para la gestión de la seguridad informática.
- Se definen medidas de seguridad para el acceso a la información.
- Integración con otros sistemas de gestión ya normalizados.
- Cumplimiento con la ley vigente.
- Proporcionar confianza interna a la organización.

- Simplificar las evaluaciones sobre los productos o servicios de la entidad.
- Factor diferenciador frente a la competencia.
- Reducción de auditorías de segundas partes.
- Cumplimiento de requerimientos del mercado.
- Abaratamiento de las primas de riesgo de seguros.
- Fomento de las medidas de seguridad.

GESTIÓN DEL RIESGO

Implica clasificar los riesgos obtenidos mediante el Análisis de Riesgos en aceptables y no aceptables, la gestión del riesgo debe enfocarse hacia los riesgos que la organización no está dispuesta a aceptar, y se debe definir el tratamiento que se va a emplear hasta alcanzar un nivel de riesgo aceptable. El tratamiento más común es tratarlo mediante la utilización de controles o salvaguardas adecuados; dichos controles serán los necesarios para prevenir, neutralizar o mitigar la probabilidad de que ocurran incidentes o bien reducir el impacto que tendría en caso de que ocurrieran.

MAGERIT

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Asimismo, MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se

persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

El análisis de riesgos según MAGERIT es una aproximación metódica para determinar el riesgo siguiendo los siguientes pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

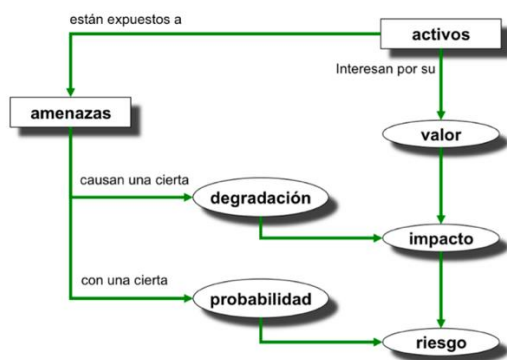


FIGURA 21: ELEMENTOS DEL ANÁLISIS DE RIESGOS POTENCIALES

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

PASO 1: ACTIVOS

Identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.

PASO 2: AMENAZAS

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos y causar un daño.

PASO 3: SALVAGUARDAS

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

PASO 4: IMPACTO RESIDUAL

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

PASO 5: RIESGO RESIDUAL

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

ESTÁNDARES

Estos son algunos estándares importantes en el ámbito de la ciberseguridad y la seguridad de la información.

NIST CYBERSECURITY FRAMEWORK

Es una metodología con un enfoque para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información, y está compuesto por tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco. Estos componentes se explican a continuación:

- Núcleo: conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. Consta de cuatro elementos: Funciones, Categorías, Subcategorías y Referencias Informativas.
 - Funciones: organizan actividades básicas de seguridad cibernética en su nivel más alto. Estas funciones son: identificar, proteger, detectar, responder y recuperar.
 - Identificar: desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.
 - Proteger: desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.
 - Detectar: desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.
 - Responder: desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.
 - Desarrollar: desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad

o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.

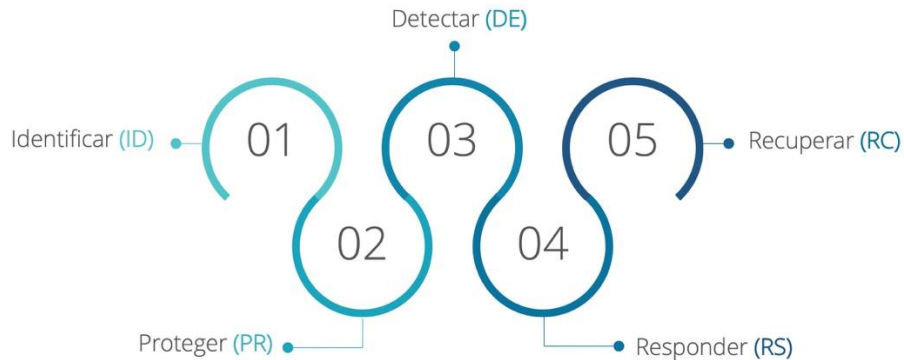


FIGURA 22: FUNCIONES

Fuente: Instituto Nacional de Estándares y Tecnología

- Categorías: subdivisiones de una función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas y actividades particulares.
- Subcategorías: dividen aún más una categoría en resultados específicos de actividades técnicas o de gestión.
- Referencias informativas: secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada subcategoría.
- Niveles de Implementación: proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo.

Los Niveles caracterizan las prácticas de una organización en un rango, desde Parcial (Nivel 1) hasta Adaptable (Nivel 4), estos niveles reflejan una progresión desde respuestas informales y reactivas a enfoques que son ágiles e informados sobre los riesgos.

- Nivel 1 (Parcial)

- Proceso de gestión de riesgos: las prácticas de gestión de riesgos de seguridad cibernética de la organización no están formalizadas, y el riesgo se gestiona de forma ad hoc y, en ocasiones, de forma reactiva.
 - Programa integrado de gestión de riesgos: existe una conciencia limitada sobre el riesgo de seguridad cibernética a nivel organizacional.
 - Participación externa: la organización no comprende su función en el ecosistema más amplio con respecto a sus dependencias o dependientes.
- Nivel 2 (Riesgo informado)
 - Proceso de gestión de riesgos: las prácticas de gestión de riesgos son aprobadas por la administración, pero posiblemente no son establecidas como políticas de toda la organización.
 - Programa integrado de gestión de riesgos: existe una conciencia del riesgo de seguridad cibernética a nivel organizacional, pero no se ha establecido un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética.
 - Participación externa: generalmente, la organización entiende su función en el ecosistema más amplio con respecto a sus propias dependencias o dependientes, pero no ambos.
- Nivel 3 (Repetible)
 - Proceso de gestión de riesgos: las prácticas para la gestión de riesgos de la organización se aprueban formalmente y se expresan como políticas.
 - Programa integrado de gestión de riesgos: existe un enfoque de toda la organización para gestionar el riesgo de seguridad cibernética.
 - Participación externa: la organización entiende su función, dependencias y dependientes en un ecosistema más amplio y

posiblemente contribuya a una más amplia comprensión de los riesgos por parte de la comunidad.

- Nivel 4 (Adaptable)
 - Proceso de gestión de riesgos: la organización adapta sus prácticas de seguridad cibernética basándose en actividades previas y actuales de ciberseguridad, el cual incluye las lecciones aprendidas y los indicadores predictivos.
 - Programa integrado de gestión de riesgos: existe un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética que utiliza las políticas, los procesos y los procedimientos informados sobre riesgos para abordar posibles eventos de seguridad cibernética.
 - Participación externa: la organización entiende su rol, sus dependencias y sus dependientes en el ecosistema más amplio y contribuye a una mayor comprensión de los riesgos por parte de la comunidad.
- Perfiles: presenta los resultados que se basan en las necesidades empresariales que una organización ha seleccionado de las categorías y subcategorías del marco.

NIST SP 800 SERIES

La serie NIST 800 es un conjunto de documentos que describen las políticas, procedimientos y pautas de seguridad informática del gobierno federal de los Estados Unidos. El NIST (Instituto Nacional de Estándares y Tecnología) es una unidad del Departamento de Comercio.

Las publicaciones cubren todos los procedimientos y criterios recomendados por el NIST para evaluar y documentar las amenazas y vulnerabilidades y para implementar medidas de seguridad para minimizar el riesgo de eventos adversos.

ENISA EU CYBERSECURITY STRATEGY

Para hacer frente a las amenazas actuales y emergentes de ciberseguridad, los Estados miembros de la UE deben desarrollar y adaptar constantemente sus estrategias de ciberseguridad. Las estrategias nacionales de seguridad cibernética (NCSS) son los principales documentos de los estados nacionales para establecer principios estratégicos, pautas y objetivos y, en algunos casos, medidas específicas para mitigar el riesgo asociado con la seguridad cibernética.

ISO 27000

ISO/IEC 27001 – describe como implantar un SGSI que servirá para gestionar los controles y riesgos de la seguridad de la información dentro de una organización. Especifica los requisitos para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI dentro del contexto de los riesgos de negocio de la organización. Los objetivos de control y la lista de controles derivan y están alineados con los que están en la lista de la ISO/IEC 27002.

ISO/IEC 27002 – es una guía de buenas prácticas que describe los objetivos de control y controles recomendables y comúnmente aceptados en la seguridad de la información.

COBIT

Es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por ISACA (Information Systems Audit and Control Association) y el IT GI (IT Governance Institute), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos; se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado, público o entidades sin fines de lucro.

Mediante sus cinco principios y siete habilitadores, COBIT 5 utiliza prácticas de gobierno y gestión para describir las acciones que son ejemplo de mejores prácticas de su aplicación.

Principios:

- Satisfacer las necesidades del accionista.
- Considerar la empresa de punta a punta.
- Aplicar un único modelo de referencia integrado.
- Posibilitar un enfoque holístico.
- Separar gobierno de la gestión.

Habilitadores:

- Principios, políticas y modelos de referencia.
- Procesos.
- Estructuras organizacionales.
- Cultura, ética y comportamiento.
- Información.
- Servicios, infraestructura y aplicaciones.
- Gente, habilidades y competencias.

CIS CONTROLS

Es un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes. Asimismo, es importante destacar que los Controles CIS son desarrollados por una comunidad de expertos en TI que aplican su experiencia de primera mano como defensores cibernéticos para crear estas mejores prácticas de seguridad aceptadas globalmente.

Cuenta con seis controles que son:

- Control 1: Inventario de Dispositivos autorizados y no autorizados.

- Control 2: Inventario de Software autorizados y no autorizados.
- Control 3: Gestión continua de vulnerabilidades.
- Control 4: Uso controlado de privilegios administrativos.
- Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores.
- Control 6: Mantenimiento, monitoreo y análisis de *logs* de auditoría.

BARRERAS ORGANIZACIONALES

A continuación, se muestran algunas de las causas por las cuales se considera que se dificulta o imposibilita la implementación del concepto de ciberseguridad organizacional en las pequeñas y medianas empresas:

- Falta de tiempo

El factor tiempo en las organizaciones es muy importante y puede llegar a ser una gran barrera debido a que se requiere tiempo para llevar a cabo todo el proceso de análisis, implementación, mantenimiento, etc., de la ciberseguridad, y muchas veces, las organizaciones no cuentan con dicho tiempo debido a la demanda de funciones que poseen o al poco personal con el que cuentan para realizar las tareas.

- Falta de compromiso

El compromiso y participación por parte de los funcionarios es una parte fundamental en cualquier proyecto que se quiera llevar a cabo en una organización y el área de seguridad de la información no es la excepción, es necesario que las partes se comprometan a la implementación de la misma y decidan tomar parte y acción en los procesos requeridos, ya que la seguridad depende de todos los que conforman la organización y no solo de unos cuantos; por esto es que la falta de compromiso y participación se considerada una barrera organizacional importante.

- Falta de presupuesto

La implementación de cualquier proyecto en una organización requiere de ciertos egresos mínimos, ya sea para capacitación, entrenamiento, consultoría, entre otros, para ello es fundamental contar con suficiente presupuesto que permita de una manera fluida hacer frente a lo mencionado anteriormente, lo cual debe ser considerado como una inversión, no como un gasto, sin embargo, para las PYMES esto se convierte en una dificultad por sus limitados recursos económicos.

- Desconocimiento de la materia

El no tener conocimientos claros del tema o no tener los suficientes, genera una barrera de dificultad bastante grande para las organizaciones, ya que da lugar a pérdida de tiempo, desperdicio de recursos, malentendidos y falta de resultados. Por razones como las mencionadas anteriormente, es de suma importancia que, si no se tienen dichos conocimientos dentro de la institución, asegurar que los consigamos de manera externa, apoyándonos en un profesional de la materia que nos pueda brindar guía y apoyo en la implementación.

- Falta de profesionales preparados

Relacionado al punto anterior, el no contar con profesionales capacitados que puedan dar apoyo en todo el proceso de asegurar la información, es una de las barreras más comunes, ya que es sumamente importante contar con las personas correctas a la hora de querer llevar a cabo nuestros proyectos, de esta manera podrán guiarnos durante todo el proceso de la mejor manera.

- Ausencia de liderazgo

Sin duda este punto es una de las barreras más significativas que existen en las empresas; es indispensable que exista liderazgo por parte del gobierno, ya que ellos deben ser quienes den el ejemplo a los demás, todo inicia por ellos, el gobierno debe

tomar *conciencia* de los cambios que genera la implementación de los SIG y la consecución en la mejora continua, conlleva a adoptar una decisión firme y prestar un apoyo incondicional que permita al personal ver la decisión que tienen los directivos, la cual disminuirá día a día los fallos, los costos, los plazos y aumentar el valor agregado a las organizaciones.

- Resistencia al cambio

Una de las barreras más significativas es la resistencia al cambio, es muy común en las organizaciones que se presente este factor, donde las personas no aceptan ni se encuentran abiertas a cambios, nuevos procesos, nuevas implementaciones, etc., creen que las cosas como están actualmente funcionan y no entienden el por qué de cambiarlas, y es realmente complicado intentar cambiar esa mentalidad en los funcionarios, lleva todo un proceso.

- Falta de entrenamiento

El entrenamiento es fundamental en cualquier implementación, es importante que se capacite al personal en todas las áreas, con mas razón aun si se introduce algo nuevo, de esta manera las personas podrán adquirir conocimientos y saber como actuar ante las diferentes situaciones. Esto se convierte en una barrera, ya que la falta de ese conocimiento desencadena en errores, perdida de tiempo, etc.

- Falta de concientización

-

Relacionado al punto anterior, es importante que existe la concientización en las empresas, hacerle saber a todos los que forman parte de ella la labor importante que realizan, hacerles saber cuales son sus responsabilidades, el aporte que realizan con su trabajo, para que de esta manera se comprometan y entiendan el por qué de realizar sus funciones de manera correcta, ya que al realizar esto se incentiva a que las personas

comprendan de una mejor manera las normas, políticas que puedan existir y por ende que las apliquen.

- Falta de cultura organizacional

La implantación de sistemas de seguridad de la información supone cambio cultural dentro de las organizaciones, lo que requiere de tiempo. Este cambio implica llevar a cabo algunas actividades nuevas al interior de las organizaciones por lo que el personal muchas veces se puede mostrar indispuesto a esto.

La cultura organizacional, es la suma de visión, misión, valores corporativos y objetivos, de modo que en la medida en que las empresas los tenga claramente definidos se logrará una evolución y permanencia en el mercado. La cultura organizacional implica la interacción de sus colaboradores y su consolidación como grupo. El comportamiento de los colaboradores tiene su origen en la misma cultura: define las actitudes de los individuos hacia la organización para que estos contribuyan a su éxito.

La barrera se presenta en la creación de dichos hábitos y cultura, ya que esta orienta el comportamiento de los colaboradores y puede ser un impulsor o puede, al contrario, restringir a la organización en el logro de sus metas.

- Barreras de poder

La existencia de diferentes áreas de responsabilidad con intereses particulares (personas que se creen dueños de los puestos de trabajo) pueden crear luchas de poder a la hora de llevar a cabo la implementación de sistemas de seguridad de la información, ya que lo que para un departamento es crítico o importante no necesariamente lo es para otro, todos creen que sus procesos son los mas críticos; esta barrera puede generar resistencias en los departamentos que se sientan amenazados a la hora de efectuar la implementación.

CAPÍTULO III: MARCO METODOLÓGICO

ENFOQUE DE INVESTIGACIÓN

Para el desarrollo de este trabajo se aplicó una metodología descriptiva, cuya metodología tiene como propósito orientar los procesos de investigación del estudio y guiar al investigador. A su vez, es una herramienta esencial para el desarrollo de cualquier trabajo académico o científico y forja el rumbo de la investigación (Cortés, M. e Iglesias, M, 2004).

Bajo el anterior criterio, la investigación procuró abordar con objetividad las ventajas de las tecnologías de la información y las comunicaciones, haciendo énfasis en las amenazas y vulnerabilidades cibernéticas que en la actualidad representan un mayor nivel de riesgo para las Pymes de Costa Rica.

TIPO DE INVESTIGACIÓN

La presente investigación es de tipo descriptiva/explicativa. Según Dankhe:

La investigación descriptiva tiene el propósito de describir situaciones y eventos. Buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis. Miden de manera independiente las variables con las que tiene que ver el problema, aunque muchas veces se integran esas mediciones, su objetivo final no es indicar como se relacionan estas (Echeverría, 2009, p. 131).

En esta misma línea, también se establece: “En la investigación descriptiva su objetivo central es la descripción de fenómenos. Se sitúa en un primer nivel del conocimiento científico. Usa la observación, estudios correlacionales y de desarrollo” (Echeverría, 2009, p. 64). Así como: “En la investigación explicativa, se explica los fenómenos y el estudio de sus relaciones para conocer su estructura y los aspectos que intervienen en su dinámica” (Echeverría, 2009, p. 64).

Asimismo, es pertinente destacar que:

La investigación explicativa va mas allá de la descripción de fenómenos o el establecimiento de la relación entre variables, buscan responder a las causas de los eventos físicos o sociales. Explica por que ocurren los fenómenos y en qué condiciones se dan estos y por qué se relacionan dos o más variables. Es más estructurada que las otras investigaciones” (Echeverría, 2009, p. 132).

POBLACIÓN Y MUESTREO

La población de la cual se extrajo la información necesaria para realizar la investigación fue de 15 empresas PYMES que se encuentran en Costa Rica, de las cuales solo 10 se encontraron disponibles para responder la encuesta.

Con respecto a la muestra, esta fue obtenida a partir de la lista de PYMES activas al 30 de abril del 2019 del MEIC y las PYMES participantes de la EXPOPYME 2019.

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El método que se utilizó para recolectar la información fue a través de la encuesta, los cuestionarios diseñados con preguntas cerradas y abiertas dirigidas a empresas registradas como PYMES en Costa Rica. Según Naresh K. Malhotra:

Las encuestas son entrevistas con un gran número de personas utilizando un cuestionario prediseñado. Según el mencionado autor, el método de encuesta incluye un cuestionario estructurado que se da a los encuestados y que está diseñado para obtener información específica (Malhotra, 2004, p. 168).

TÉCNICAS DE ANÁLISIS DE LA INFORMACIÓN

La información bibliográfica utilizada para el desarrollo de la investigación se obtuvo a partir del análisis documental. Además, se emplearon fichas de trabajo para

recolectar la información y hacer anotaciones importantes. También se tuvo en consideración el cuestionario que fue aplicado a las organizaciones.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

A continuación, se muestra el análisis de los resultados del instrumento utilizado por el investigador para el cumplimiento del segundo y tercer objetivo de la investigación; los resultados fueron obtenidos mediante una encuesta realizada a diez PYMES durante la EXPOPYME 2019 en el Centro de Convenciones de Costa Rica.

Este análisis pretende demostrar las debilidades que poseen las pequeñas y medianas empresas en cuanto al tema de seguridad de la información se refiere, esto con el fin de conocer un poco de la realidad que presentan estas empresas en ciertas áreas específicas de la seguridad.

Pregunta #1

Por medio de esta pregunta se pretende medir el nivel en que las PYMES utilizan herramientas tecnológicas.

¿Hace uso de herramientas tecnológicas (computadoras, celulares, página web, datáfono, etc)?

10 respuestas

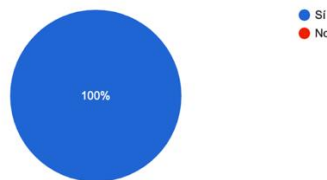


FIGURA 23. USO DE HERRAMIENTAS TECNOLÓGICAS

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 100% de las empresas hace uso de algún tipo de herramienta tecnológica dentro de sus actividades diarias; los resultados indicaron hacer uso en mayor cantidad de dispositivos como computadoras y teléfonos, sin embargo, las empresas también utilizan otros como datafonos, paginas web e impresoras.

Pregunta #2

Por medio de esta pregunta se pretende medir el nivel de frecuencia con el que las PYMES utilizan herramientas tecnológicas.

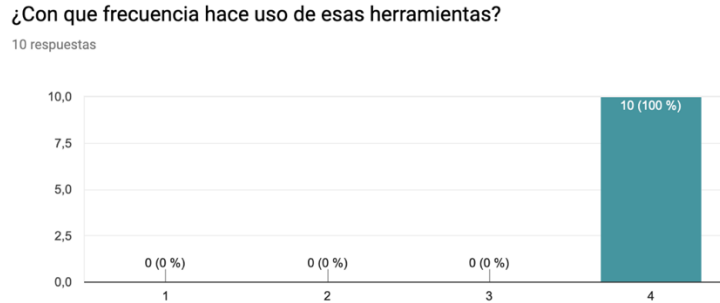


FIGURA 24. FRECUENCIA USO DE HERRAMIENTAS

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 100% de las empresas señalan hacer uso frecuente de algún tipo de herramienta tecnológica dentro de sus actividades diarias, los resultados muestran que todas las empresas sin duda alguna necesitan de las herramientas tecnológicas para llevar a cabo sus funciones básicas y poder operar de una manera correcta.

Pregunta #3

Por medio de esta pregunta se pretende saber si las empresas cuentan con normas dentro de la organización para la gestión de información.

¿Su organización cuenta con normas o prácticas que orienten la forma de gestionar los activos de información?

10 respuestas

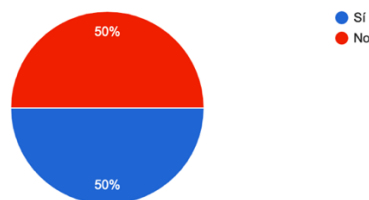


FIGURA 25. PRÁCTICAS

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 50% de las empresas indica contar con algún tipo de norma para la gestión de activos de información, mientras que el otro 50%, dice no contar con normas ni políticas; sin embargo, los resultados mostraron como muchas de estas empresas no emplean políticas de manera formal ni escrita, pero si implementan en ciertos casos de manera verbal.

Pregunta #4

Por medio de esta pregunta se pretende medir el nivel de importancia de la ciberseguridad para las PYMES.

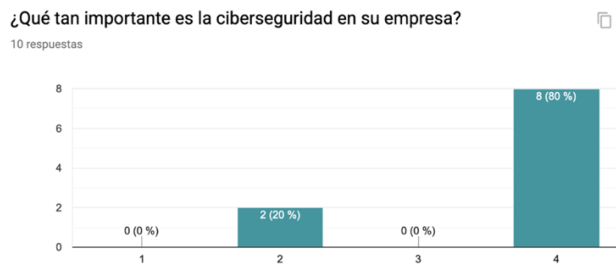


FIGURA 26. IMPORTANCIA DE LA CIBERSEGURIDAD
Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 80% de las empresas indica que la ciberseguridad es importante para la organización, mientras el 20% restante indica que es poco importante; en el caso de minoría, los resultados mostraron como esto se debe a la falta de conocimiento y concientización que posee la población con respecto a temas de esta índole.

Pregunta #5

Por medio de esta pregunta se pretende saber si las empresas emplean herramientas para proteger sus equipos, por ejemplo, antivirus.

¿Su empresa utiliza alguna herramienta de hardware o software, como un antivirus, para incrementar los niveles de seguridad de los equipos de cómputo?

10 respuestas

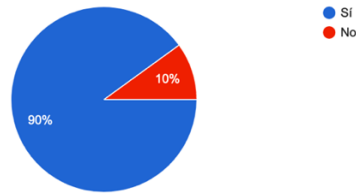


FIGURA 27. USO DE ANTIVIRUS

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 90% de las empresas indica hacer uso de algún tipo de herramienta para aumentar los niveles de seguridad en sus equipos, mientras el 10% restante no cuenta con ninguna herramienta; los resultados señalan que las herramientas utilizadas son básicas tales como software antivirus gratuito y en la mayoría de los casos configurado sin conocimiento.

Pregunta #6

Por medio de esta pregunta se pretende saber si las empresas emplean alguna otra herramienta para proteger la información de su empresa.

¿Cuentan con algún otro tipo de herramientas que permitan asegurar la información de su empresa?

10 respuestas

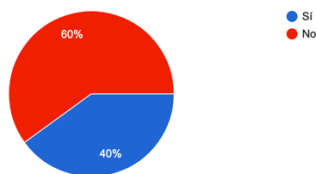


FIGURA 28. HERRAMIENTAS PARA ASEGURAR INFORMACIÓN

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 60% de las empresas indica hacer uso de algún tipo de herramienta para aumentar los niveles de seguridad en sus equipos, los resultados señalan que entre estas herramientas utilizadas por algunas empresas se encuentra el uso de firewall y copias de seguridad.

Pregunta #7

Por medio de esta pregunta se pretende saber si las empresas tienen identificados los activos críticos.



FIGURA 29. IDENTIFICACIÓN DE ACTIVOS CRÍTICOS
Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 70% de las empresas indica tener los activos críticos identificados, mientras el 30% restante de empresas no los tiene identificados; en este último caso, las empresas no tenían conocimiento de lo que era un activo para su organización.

Pregunta #8

Por medio de esta pregunta se pretende identificar si las empresas realizan análisis de riesgos enfocados en riesgos tecnológicos.

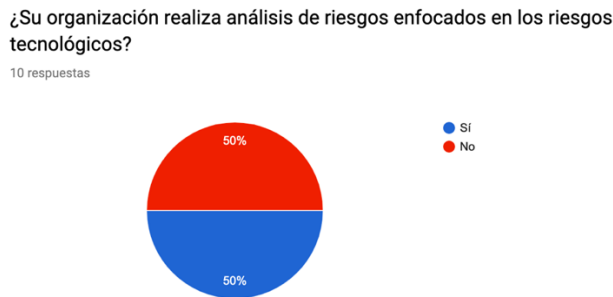


FIGURA 30. ANÁLISIS DE RIESGOS
Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 50% de las empresas indica realizar análisis de riesgos, mientras el otro 50% indica no realizar análisis de riesgos; los resultados señalan como las empresas que realizan análisis lo

llevan a cabo de una manera básica, sin considerar muchos aspectos importantes, solo identifican los posibles riesgos que podría sufrir su empresa.

Pregunta #9

Por medio de esta pregunta se pretende identificar si las empresas asignan algún tipo de presupuesto a la ciberseguridad.

¿Su organización asigna anualmente, presupuesto destinado a la ciberseguridad?
10 respuestas

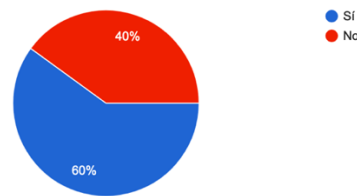


FIGURA 31. PRESUPUESTO A CIBERSEGURIDAD
Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 60% de las empresas indica asignar presupuesto anualmente destinado a la ciberseguridad, mientras el 40% restante indica no destinar ningún monto a la ciberseguridad; este último porcentaje considera que existen áreas de mayor relevancia en las cuales invertir dinero, dejando como última opción la seguridad de la información.

Pregunta #10

Por medio de esta pregunta se pretende identificar si los funcionarios de las empresas reciben capacitaciones relacionadas a la ciberseguridad.

¿Usted o los demás empleados de su empresa reciben capacitación acerca de ciberseguridad y las amenazas cibernéticas?
10 respuestas

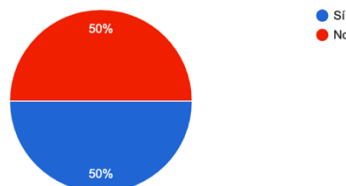


FIGURA 32. CAPACITACIÓN
Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 50% de las empresas dan algún tipo de capacitación relacionada a la ciberseguridad a sus funcionarios, mientras el otro 50% no da ningún tipo de capacitación relacionada a ciberseguridad a sus funcionarios; en el caso de las empresas que brindan capacitación, los cursos dados son realmente básicos y muchas veces incompletos.

Pregunta #11

Por medio de esta pregunta se pretende identificar si dentro de la estructura organizacional de las empresas existe algún cargo con funciones de ciberseguridad.

¿Dentro de la estructura organizacional de su empresa existe algún cargo con funciones de ciberseguridad?
10 respuestas

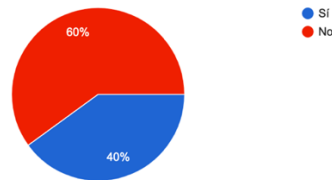


FIGURA 33. CARGO CON FUNCIONES DE CIBERSEGURIDAD

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 60% de las empresas cuentan con un funcionario dedicado al área de ciberseguridad, mientras el 40% no cuenta con nadie destinado a esta área; es importante mencionar que en los casos de las empresas que cuentan con funciones de ciberseguridad, en su mayoría no están asignados a una persona en particular que se dedique solamente a estas labores, si no que una persona con otro cargo se encarga también de desarrollar algunas tareas de esta área.

Pregunta #12

Por medio de esta pregunta se pretende identificar si las empresas cuentan con un plan de contingencia ante algún evento de ciberseguridad que se pueda presentar.

¿Su empresa cuenta con un plan de contingencia ante un evento de ciberseguridad?

10 respuestas

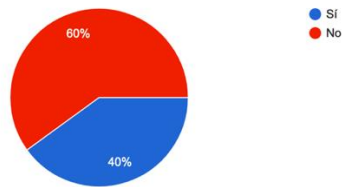


FIGURA 34. PLAN DE CONTINGENCIA

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 60% de las empresas indican contar con un plan de contingencia ante eventos de ciberseguridad, mientras el 40% indica no contar con planes de contingencia; sin embargo, cabe mencionar que los planes que indican que existen no se encuentran completos ni se encuentran de forma escrita, si no que se conoce algún tipo de procedimiento de forma verbal para mantener la operación de la empresa.

Pregunta #13

Por medio de esta pregunta se pretende identificar si los funcionarios de la organización saben como actuar ante algún evento donde se vea comprometida la información de la empresa.

¿Usted sabe qué debe hacer ante un evento donde se vea comprometida la información de su compañía?

10 respuestas

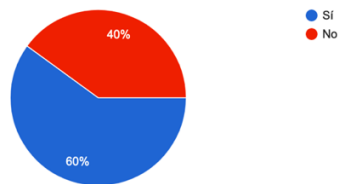


FIGURA 35. ACCIÓN ANTE UN EVENTO

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el 60% de las empresas afirman que sus funcionarios saben como proceder en caso de presentarse algún evento relacionado a ciberseguridad, mientras el 40% indica que sus funcionarios no saben como proceder en caso de presentarse algún evento; en el caso del 60%, si conocen como proceder en su mayoría es por procedimientos verbales que en algún

momento se les han comunicado, sin embargo, en su mayoría, no existen procedimientos por escrito para estos eventos.

Pregunta #14

Por medio de esta pregunta se pretende conocer cuales son los riesgos que las empresas consideran son a los que mas se podrían ver expuestos.

¿Cuáles considera son los riesgos a los que su empresa se podría ver expuesta?

10 respuestas

Robo de información de cuentas bancarias y clientes
Robo de información de clientes
Robo de información de clientes y cuentas bancarias
Hackeo de servidores (nube), interrupción del servicio
Robo de información de clientes
Pérdida de información, continuidad del negocio, robo de información bancaria, clientes
Robo de información clientes, bases de datos
Pérdida de información de clientes
Pérdida de información, disrupción del servicio
robo de informacion, interrupcion del servicio

FIGURA 36. RIESGOS

Fuente: Elaboración propia basado en respuestas de la encuesta.

Comentario: Basado en el gráfico anterior se puede determinar que el riesgo que las empresas consideran puede ser su mayor amenaza es el robo o pérdida de información y en menor medida, se consideran riesgos como interrupción del servicio, continuidad del negocio y ataque a servidores.

CAPÍTULO V: PROPUESTA DE ESTRATEGIA DE LA GESTIÓN DE LA CIBERSEGURIDAD

Según los resultados obtenidos en la encuesta realizada, se puede observar como las empresas aseguran que la seguridad de la información es importante para ellos, sin embargo, una gran cantidad de empresas no cuentan con las medidas necesarias para

evitar o minimizar situaciones de este tipo; por esta razón, se propone una estrategia de la gestión de la seguridad de la información, donde se va a definir una guía de controles de fácil implementación, considerando aspectos importantes como recursos económicos, personal, tiempo etc.

Para la elaboración de dicha guía, primeramente, se realizará un análisis de riesgos tomando como base una empresa PYMES, esto para facilitar el proceso de análisis de riesgos, ya que, en una PYME, el conjunto de activos de información es relativamente limitado y estándar.

Como parte de dicho análisis, primero, se realizará una identificación de los activos, posteriormente, para cada activo se van a identificar los posibles riesgos que podrían afectarlo y dichos riesgos serán clasificados basados en diferentes criterios con el fin de determinar la severidad; basado en los resultados de dicha clasificación, se va a decidir que riesgos son mas críticos y requieren un tratamiento inmediato y cuales pueden esperar para ser tratados.

PASO 1: IDENTIFICACIÓN DE ACTIVOS

Según la ISO 27001: “Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección”.

Para este proceso, se tomó como base la microempresa “Óptima Seguridad S.A”, la cual brinda servicios de importación y venta al por mayor y al detalle de cajas fuertes de seguridad, así como, la reparación de estas.

Mediante el análisis realizado a dicha empresa, se determinaron los activos definidos en la Tabla 1, los cuales fueron clasificados según la metodología Magerit en:

- [D] Datos / Información
- [P] Personal
- [SI] Sistema de Información
- [S] Servicios
- [HW] Hardware / Equipos informáticos
- [COM] Redes de comunicaciones
- [SW] Software / Aplicativos

TABLA 1: TABLA DE ACTIVOS

Código	Tipo de Activo	Activo	Descripción
D01	[D] Datos / Información	Datos	Información de clientes, proveedores, inventario, etc.
P01	[P] Personal	Personal	Funcionarios que laboran en la empresa
S01	[S] Servicios	Correo Electrónico	Hotmail, Gmail
S02	[S] Servicios	Servicios en la nube	Google Drive, Dropbox
COM01	[COM] Redes de comunicaciones	Recursos de conectividad	Red Wifi, telefonía fija
HW01	[HW] Hardware / Equipos informáticos	PC	Computadoras de escritorio y portátiles
HW02	[HW] Hardware / Equipos informáticos	Dispositivos móviles	Teléfonos celulares, tabletas, datafonos, etc.
HW03	[HW] Hardware / Equipos informáticos	Dispositivos periféricos	Impresora, memorias USB, etc.
SW01	[SW] Software / Aplicativos	Servicio web	Página web
SW02	[SW] Software / Aplicativos	Redes Sociales	Facebook, WhatsApp, Instagram
SW03	[SW] Software / Aplicativos	Sistemas o aplicaciones	Excel, Word, aplicaciones bancarias, portal de Hacienda, firma digital
SW04	[SW] Software / Aplicativos	Sistema Operativo	Windows, MAC

Fuente: Elaboración propia.

PASO 2: IDENTIFICACIÓN DE RIESGOS

Este paso corresponde a la determinación de las amenazas a los que están sometidos los activos definidos en el postulado anterior. Los activos pueden estar expuestos a amenazas naturales como terremotos, inundaciones, amenazas causadas por el personal de la organización, etc.

Para la identificación de riesgos de la Tabla 2, se utilizó el catálogo de amenazas que presenta la metodología Magerit, la cual fue explicada en el marco teórico y define las amenazas en 4 categorías, estas son:

- [N] Desastres Naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
 - [N.1] Fuego
 - [N.2] Daños por agua
- [I] De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
 - [I.1] Fuego
 - [I.2] Daños por agua
 - [I.3] Contaminación mecánica
 - [I.4] Contaminación electromagnética
 - [I.5] Avería de origen físico o lógico
 - [I.6] Corte del suministro eléctrico
 - [I.7] Condiciones inadecuadas de temperatura o humedad
 - [I.8] Fallo de servicios de comunicaciones
 - [I.9] Interrupción de otros servicios y suministros esenciales
 - [I.10] Degradación de los soportes de almacenamiento de la información
 - [I.11] Emanaciones electromagnéticas
- [E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas.
 - [E.1] Errores de los usuarios
 - [E.2] Errores del administrador
 - [E.3] Errores de monitorización (log)
 - [E.4] Errores de configuración
 - [E.7] Deficiencias en la organización
 - [E.8] Difusión de software dañino
 - [E.9] Errores de [re-]encaminamiento
 - [E.10] Errores de secuencia

- [E.14] Escapes de información
- [E.15] Alteración accidental de la información
- [E.18] Destrucción de información
- [E.19] Fugas de información
- [E.20] Vulnerabilidades de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal
- [A] Ataque intencionados: Fallos deliberados causados por las personas.
 - [A.3] Manipulación de los registros de actividad (log)
 - [A.4] Manipulación de la configuración
 - [A.5] Suplantación de la identidad del usuario
 - [A.6] Abuso de privilegios de acceso
 - [A.7] Uso no previsto
 - [A.8] Difusión de software dañino
 - [A.9] [Re-]encaminamiento de mensajes
 - [A.10] Alteración de secuencia
 - [A.11] Acceso no autorizado
 - [A.12] Análisis de tráfico
 - [A.13] Repudio
 - [A.14] Interceptación de información (escucha)
 - [A.15] Modificación deliberada de la información
 - [A.18] Destrucción de información
 - [A.19] Divulgación de información
 - [A.22] Manipulación de programas
 - [A.23] Manipulación de los equipos
 - [A.24] Denegación de servicio
 - [A.25] Robo
 - [A.26] Ataque destructivo

- [A.27] Ocupación enemiga
- [A.28] Indisponibilidad del personal
- [A.29] Extorsión
- [A.30] Ingeniería social (picaresca)

Para la siguiente evaluación de riesgos se tomo como principal fuente la participación del Gerente General, quien es el que se encuentra al tanto de toda la situación de la empresa; sin embargo, también se tomo en consideración el punto de vista del ejecutivo de ventas, el técnico y mensajero, esto con el fin de entender mejor los procesos de cada uno de ellos.

TABLA 2: TABLA DE RIESGOS

CÓDIGO	ACTIVO	AMENAZA
D01	Datos	[E.19] Fugas de información
		[A.18] Destrucción de información
		[A.15] Modificación deliberada de la información
		[E.15] Alteración accidental de la información
P01	Personal	[E.19] Fugas de información
		[A.19] Divulgación de información
		[A.28] Indisponibilidad del personal
		[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
S01	Correo Electrónico	[E.8] Difusión de software dañino
		[A.11] Acceso no autorizado
		[E.19] Fugas de información
S02	Servicios en la nube	[A.11] Acceso no autorizado
		[A.15] Modificación deliberada de la información
		[A.24] Denegación de servicio
		[E.18] Destrucción de información
		[E.2] Errores del administrador
COM01	Recursos de conectividad	[E.8] Difusión de software dañino
		[A.14] Interceptación de información (escucha)

		[E.4] Errores de configuración
		[A.24] Denegación de servicio
		[E.24] Caída del sistema por agotamiento de recursos
		[A.5] Suplantación de la identidad del usuario
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[A.12] Análisis de tráfico
HW01	Estaciones de trabajo	[I.6] Corte del suministro eléctrico
		[A.25] Robo
		[A.11] Acceso no autorizado
		[E.8] Difusión de software dañino
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[I.5] Avería de origen físico o lógico
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.25] Pérdida de equipos		
HW02	Teléfonos o dispositivos móviles	[A.11] Acceso no autorizado
		[E.8] Difusión de software dañino
		[E.25] Pérdida de equipos
		[I.5] Avería de origen físico o lógico
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[A.25] Robo
HW03	Dispositivos periféricos	[I.6] Corte del suministro eléctrico
		[E.8] Difusión de software dañino
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.25] Pérdida de equipos
		[I.5] Avería de origen físico o lógico
SW01	Servicio web	[A.15] Modificación deliberada de la información
		[A.24] Denegación de servicio
		[A.30] Ingeniería social (picaresca)
		[A.11] Acceso no autorizado

		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas (software)
		[A.5] Suplantación de la identidad del usuario
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.8] Difusión de software dañino
SW02	Redes Sociales	[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas (software)
		[A.5] Suplantación de la identidad del usuario
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[A.11] Acceso no autorizado
SW03	Sistemas o aplicaciones	[E.8] Difusión de software dañino
		[A.24] Denegación de servicio
		[E.20] Vulnerabilidades de los programas (software)
		[A.5] Suplantación de la identidad del usuario
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.21] Errores de mantenimiento / actualización de programas (software)
SW04	Sistema Operativo	[E.21] Errores de mantenimiento / actualización de programas (software)
		[A.5] Suplantación de la identidad del usuario
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[A.24] Denegación de servicio
		[E.8] Difusión de software dañino
SW05	Antivirus	[A.6] Abuso de privilegios de acceso
		[E.21] Errores de mantenimiento / actualización de programas (software)

Fuente: Elaboración propia.

CRITERIOS DE VALORACIÓN

Se han evaluado los riesgos obtenidos anteriormente según diferentes criterios de valoración, los cuales determinan las posibilidades que existen de que el daño se materialice y cómo afectaría a la organización si esto ocurriese, así como, cuales son los activos que deben ser protegidos con prioridad. En las tablas 2, 3 y 4 se encuentra la definición de dichos criterios:

TABLA 3: TABLA PARA ESTIMAR LA PROBABILIDAD

VALOR	DESCRIPCIÓN
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año o más.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

Fuente: Elaboración propia.

TABLA 4: TABLA PARA ESTIMAR EL IMPACTO

VALOR	DESCRIPCIÓN
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias importantes para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.

Fuente: Elaboración propia.

TABLA 5: CRITERIOS DE ACEPTACIÓN DEL RIESGO

RANGO	DESCRIPCIÓN
Riesgo \leq 3	La organización considera el riesgo aceptable.
Riesgo $>$ 3	La organización considera el riesgo no aceptable y debe proceder a su tratamiento.

Fuente: Elaboración propia.

TABLA 6: MATRIZ DE RIESGO Y ESCALA DE CRITICIDAD UTILIZADA EN EL ANÁLISIS

		Probabilidad			Criticidad
		Baja	Media	Alta	
Impacto	Alto	3	6	9	Baja
	Medio	2	4	6	Media
	Bajo	1	2	3	Alta

Fuente: Elaboración propia.

PASO 3: ESTIMACIÓN DEL RIESGO

Basado en los criterios anteriores, se ha realizado la estimación de la vulnerabilidad de las amenazas sobre cada activo, la Tabla 7 muestra los riesgos analizados.

TABLA 7: TABLA ESTIMACIÓN DE RIESGOS

ANÁLISIS DE RIESGOS						
CÓDIGO	ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO	TOTAL CUALITATIVO
D01	Datos	[E.19] Fugas de información	1	3	3	Medio
		[A.18] Destrucción de información	1	3	3	Medio
		[A.15] Modificación deliberada de la información	1	3	3	Medio
		[E.15] Alteración accidental de la información	2	3	6	Alto

		[E.1] Errores de los usuarios	3	2	6	Alto
P01	Personal	[A.28] Disponibilidad del personal	2	2	4	Medio
		[A.30] Ingeniería social (picaresca)	2	2	4	Medio
		[E.7] Deficiencias en la organización	3	2	6	Alto
		[E.28] Disponibilidad del personal	2	2	4	Medio
S01	Correo Electrónico	[A.11] Acceso no autorizado	2	2	4	Medio
		[E.1] Errores de los usuarios	2	2	4	Medio
		[E.19] Fugas de información	2	3	6	Alto
S02	Servicios en la nube	[A.11] Acceso no autorizado	2	2	4	Medio
		[A.15] Modificación deliberada de la información	1	2	2	Bajo
		[A.24] Denegación de servicio	2	2	4	Medio
		[E.18] Destrucción de información	2	3	6	Alto
		[E.1] Errores de los usuarios	3	2	6	Alto
COM01	Recursos de conectividad	[A.14] Interceptación de información (escucha)	2	2	4	Medio

		[A.24] Denegación de servicio	1	3	3	Medio
		[E.24] Caída del sistema por agotamiento de recursos	2	3	6	Alto
		[A.5] Suplantación de la identidad del usuario	1	3	3	Medio
		[A.6] Abuso de privilegios de acceso	1	3	3	Medio
		[A.7] Uso no previsto	3	1	3	Medio
		[I.8] Fallo de servicios de comunicaciones	2	2	4	Medio
		[A.12] Análisis de tráfico	1	3	3	Medio
HW01	Estaciones de trabajo	[I.6] Corte del suministro eléctrico	3	2	6	Alto
		[A.25] Robo	1	2	2	Bajo
		[A.11] Acceso no autorizado	2	2	4	Medio
		[I.7] Condiciones inadecuadas de temperatura o humedad	1	2	2	Bajo
		[I.5] Avería de origen físico o lógico	2	2	4	Medio
		[E.23] Errores de mantenimiento / actualización	2	2	4	Medio

		de equipos (hardware)				
		[E.25] Pérdida de equipos	1	2	2	Bajo
HW02	Teléfonos o dispositivos móviles	[A.11] Acceso no autorizado	2	2	4	Medio
		[E.25] Pérdida de equipos	1	2	2	Bajo
		[I.5] Avería de origen físico o lógico	3	2	6	Alto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	2	4	Medio
		[A.25] Robo	1	2	2	Bajo
HW03	Dispositivos periféricos	[I.6] Corte del suministro eléctrico	3	1	3	Medio
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	2	4	Medio
		[E.25] Pérdida de equipos	2	2	4	Medio
		[A.25] Robo	1	3	3	Medio
		[I.5] Avería de origen físico o lógico	2	2	4	Medio
SW01	Servicio web	[A.15] Modificación deliberada de la información	2	2	4	Medio
		[A.11] Acceso no autorizado	2	3	6	Alto
		[E.20] Vulnerabilidades de los	3	3	9	Alto

		programas (software)				
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	4	Medio
		[A.5] Suplantación de la identidad del usuario	2	2	4	Medio
		[A.6] Abuso de privilegios de acceso	2	3	6	Alto
		[A.7] Uso no previsto	2	2	4	Medio
		[E.1] Errores de los usuarios	3	2	6	Alto
		[E.8] Difusión de software dañino	3	3	9	Alto
SW02	Redes Sociales	[E.20] Vulnerabilidades de los programas (software)	3	1	3	Medio
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	1	2	Bajo
		[A.5] Suplantación de la identidad del usuario	2	2	4	Medio
		[A.6] Abuso de privilegios de acceso	2	2	4	Medio
		[A.7] Uso no previsto	3	1	3	Medio

		[E.1] Errores de los usuarios	3	2	6	Alto
		[E.8] Difusión de software dañino	2	2	4	Medio
		[A.11] Acceso no autorizado	2	2	4	Medio
SW03	Sistemas o aplicaciones	[E.8] Difusión de software dañino	2	3	6	Alto
		[E.1] Errores de los usuarios	3	2	6	Alto
		[E.20] Vulnerabilidades de los programas (software)	2	2	4	Medio
		[A.5] Suplantación de la identidad del usuario	2	3	6	Alto
		[A.6] Abuso de privilegios de acceso	2	3	6	Alto
		[A.7] Uso no previsto	2	1	2	Bajo
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	4	Medio
SW04	Sistema Operativo	[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	4	Medio
		[A.5] Suplantación de la identidad del usuario	1	2	2	Bajo

		[A.6] Abuso de privilegios de acceso	2	3	6	Alto
		[A.7] Uso no previsto	2	1	2	Bajo
		[E.1] Errores de los usuarios	3	2	6	Alto
		[E.8] Difusión de software dañino	2	3	6	Alto

Fuente: Elaboración propia.

PASO 4: IDENTIFICACIÓN DE CONTROLES

Una vez identificados los activos de información y las amenazas de estos, así como, evaluado el nivel del riesgo, se propone como estrategia para el tratamiento de dichos riesgos, una lista de controles basados en el “Código de mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones” (ISO 27002).

El objetivo de la lista de controles es definir una serie de acciones que orienten y sirvan de guía base para la pequeña o mediana empresa de cualquier sector, con el fin de controlar los riesgos relacionados a tecnologías de la información que se puedan presentar; esto para minimizar su impacto en la medida de lo posible.

Las salvaguardas, son medidas de protección frente a las amenazas y pueden convertirse en procedimientos para ayudar a prevenir riesgos e impactos. La implantación de salvaguardas en la organización va a ayudar a prevenir, impedir, reducir o controlar los riesgos identificados.

Existen varias estrategias de respuesta a los riesgos:

- **Aceptar:** la organización asume que se encuentra bajo riesgo y aun así no ejecuta ninguna acción. Suele utilizarse en aquellas amenazas menos importantes ya que el costo que acarrearía su materialización es aceptable. No obstante, sería recomendable definir una serie de procedimientos a seguir en la organización en caso de que el evento ocurra.

- Transferir: el riesgo se transfiere a un tercero, por ejemplo, a un seguro, que asumirá la responsabilidad de la gestión. Sin embargo, la organización no debería dejar de prestarle atención ya que sigue existiendo. Se recomendaría realizar un seguimiento al igual que con el resto que no han sido transferidos.
- Mitigar: la organización aplica los controles que considere oportunos para reducir el impacto del riesgo si llegara a materializarse. No se habría eliminado del todo, pero podría ser asumido por la organización.
- Evitar: la organización intenta eliminar el riesgo completamente y para ello implanta todos los controles necesarios. Esta sería la solución idónea, aunque la más costosa en recursos.

Con base en lo anterior, se han clasificado los activos y sus riesgos según la estrategia de tratamiento que se vaya a dar para posteriormente plantear los controles necesarios para cumplir con el tratamiento propuesto. La Tabla 8 muestra los resultados de dicha clasificación.

TABLA 8: TABLA ESTRATEGIA DE TRATAMIENTO

CÓDIGO	ACTIVO	AMENAZA	TOTAL CUALITATIVO	ESTRATEGIA DE TRATAMIENTO DEL RIESGO
D01	Datos	[E.19] Fugas de información	Medio	Mitigar el riesgo
		[A.18] Destrucción de información	Medio	Mitigar el riesgo
		[A.15] Modificación deliberada de la información	Medio	Mitigar el riesgo
		[E.15] Alteración accidental de la información	Alto	Mitigar el riesgo
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo
P01	Personal	[A.28] Indisponibilidad del personal	Medio	Mitigar el riesgo
		[A.30] Ingeniería social (picaresca)	Medio	Mitigar el riesgo
		[E.7] Deficiencias en la organización	Alto	Mitigar el riesgo
		[E.28] Indisponibilidad del personal	Medio	Mitigar el riesgo

S01	Correo Electrónico	[A.11] Acceso no autorizado	Medio	Mitigar el riesgo
		[E.1] Errores de los usuarios	Medio	Mitigar el riesgo
		[E.19] Fugas de información	Alto	Mitigar el riesgo
S02	Servicios en la nube	[A.11] Acceso no autorizado	Medio	Mitigar el riesgo
		[A.15] Modificación deliberada de la información	Bajo	Aceptar el riesgo
		[A.24] Denegación de servicio	Medio	Mitigar el riesgo
		[E.18] Destrucción de información	Alto	Mitigar el riesgo
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo
COM01	Recursos de conectividad	[A.14] Interceptación de información (escucha)	Medio	Mitigar el riesgo
		[A.24] Denegación de servicio	Medio	Mitigar el riesgo
		[E.24] Caída del sistema por agotamiento de recursos	Alto	Mitigar el riesgo
		[A.5] Suplantación de la identidad del usuario	Medio	Mitigar el riesgo
		[A.6] Abuso de privilegios de acceso	Medio	Mitigar el riesgo
		[A.7] Uso no previsto	Medio	Mitigar el riesgo
		[I.8] Fallo de servicios de comunicaciones	Medio	Mitigar el riesgo
		[A.12] Análisis de tráfico	Medio	Mitigar el riesgo
HW01	Estaciones de trabajo	[I.6] Corte del suministro eléctrico	Alto	Mitigar el riesgo
		[A.25] Robo	Bajo	Aceptar el riesgo
		[A.11] Acceso no autorizado	Medio	Mitigar el riesgo
		[I.7] Condiciones inadecuadas de temperatura o humedad	Bajo	Aceptar el riesgo
		[I.5] Avería de origen físico o lógico	Medio	Mitigar el riesgo
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Medio	Mitigar el riesgo
		[E.25] Pérdida de equipos	Bajo	Aceptar el riesgo

HW02	Teléfonos o dispositivos móviles	[A.11] Acceso no autorizado	Medio	Mitigar el riesgo
		[E.25] Pérdida de equipos	Medio	Aceptar el riesgo
		[I.5] Avería de origen físico o lógico	Alto	Mitigar el riesgo
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Medio	Mitigar el riesgo
		[A.25] Robo	Bajo	Aceptar el riesgo
HW03	Dispositivos periféricos	[I.6] Corte del suministro eléctrico	Medio	Mitigar el riesgo
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Medio	Mitigar el riesgo
		[E.25] Pérdida de equipos	Medio	Mitigar el riesgo
		[A.25] Robo	Medio	Mitigar el riesgo
		[I.5] Avería de origen físico o lógico	Medio	Mitigar el riesgo
SW01	Servicio web	[A.15] Modificación deliberada de la información	Medio	Mitigar el riesgo
		[A.11] Acceso no autorizado	Alto	Mitigar el riesgo
		[E.20] Vulnerabilidades de los programas (software)	Alto	Mitigar el riesgo
		[E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Mitigar el riesgo
		[A.5] Suplantación de la identidad del usuario	Medio	Mitigar el riesgo
		[A.6] Abuso de privilegios de acceso	Alto	Mitigar el riesgo
		[A.7] Uso no previsto	Medio	Mitigar el riesgo
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo
		[E.8] Difusión de software dañino	Alto	Mitigar el riesgo
SW02	Redes Sociales	[E.20] Vulnerabilidades de los programas (software)	Medio	Mitigar el riesgo
		[E.21] Errores de mantenimiento / actualización de programas (software)	Bajo	Aceptar el riesgo

		[A.5] Suplantación de la identidad del usuario	Medio	Mitigar el riesgo
		[A.6] Abuso de privilegios de acceso	Medio	Mitigar el riesgo
		[A.7] Uso no previsto	Medio	Mitigar el riesgo
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo
		[E.8] Difusión de software dañino	Medio	Mitigar el riesgo
		[A.11] Acceso no autorizado	Medio	Mitigar el riesgo
SW03	Sistemas o aplicaciones	[E.8] Difusión de software dañino	Alto	Mitigar el riesgo
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo
		[E.20] Vulnerabilidades de los programas (software)	Medio	Mitigar el riesgo
		[A.5] Suplantación de la identidad del usuario	Alto	Mitigar el riesgo
		[A.6] Abuso de privilegios de acceso	Alto	Mitigar el riesgo
		[A.7] Uso no previsto	Bajo	Aceptar el riesgo
		[E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Mitigar el riesgo
SW04	Sistema Operativo	[E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Mitigar el riesgo
		[A.5] Suplantación de la identidad del usuario	Bajo	Aceptar el riesgo
		[A.6] Abuso de privilegios de acceso	Alto	Mitigar el riesgo
		[A.7] Uso no previsto	Bajo	Aceptar el riesgo
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo
		[E.8] Difusión de software dañino	Alto	Mitigar el riesgo

Fuente: Elaboración propia.

Una vez definido el tratamiento que se le va a dar a cada riesgo, se procede a asignar los controles que mejor ayudaran a cumplir dicha estrategia, estos controles como se menciono anteriormente están basados en el “Código de mejores prácticas para

apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones” (ISO 27002).

PASO 5: EXPLICACIÓN DE CONTROLES

Se realizó un estudio de todos los controles planteados en la ISO 27002, de los cuales 32 fueron seleccionados como aplicables para este caso; estos controles serán explicados con mayor detalle y en formato de guía para un mayor entendimiento, los mismos serán agrupados según la sección de la ISO 27002.

Para la siguiente explicación es importante saber que un activo es cualquier cosa que tiene valor para la organización. La norma ISO/IEC 27000, define los siguientes tipos de activos:

- información;
- software, como un programa informático;
- físico, como computadora;
- servicios;
- personas, y sus calificaciones, habilidades y experiencia; y
- intangibles, como reputación e imagen

PASO 6: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Asignación de responsabilidades para la seguridad de la información

Se deben definir y asignar claramente todas las responsabilidades para la seguridad de la información. Se propone la siguiente estructura:

ROLES Y RESPONSABILIDADES

- Jefatura
 - Es responsable de la elaboración de la presente política, de su actualización y velar por el cumplimiento de sus disposiciones.
 - Supervisar la implementación de la política de seguridad.

- Ejecutivo de Ventas
 - Cumplir la política.
- Técnico
 - Cumplir la política.
- Mensajero
 - Cumplir la política.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

6.2 Segregación de tareas

Se deben segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización. Se propone la siguiente estructura:

Responsable	Rol	Funciones
Jefatura	Dueño de la empresa y proveedor del capital	<ol style="list-style-type: none"> 1. Desarrollar la estrategia del negocio 2. Asignar recursos según corresponda 3. Toma de decisiones
Ejecutivo de Ventas	Vender productos	<ol style="list-style-type: none"> 1. Buscar nuevos clientes 2. Ofrecer productos
Técnico	Instalar los productos	<ol style="list-style-type: none"> 1. Instalar productos

		2. Brindar mantenimiento a los productos
Mensajero	Entregar los productos	1. Entregar productos de la empresa

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

6.2.1 Política para dispositivos móviles

Se debe establecer una política formal y se debe adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones. Se propone la siguiente estructura para la política:

El personal que haga uso del dispositivo móvil para almacenar o acceder a la información de Optima Seguridad S.A., deberá:

- Solicitar la autorización para ello, aceptando el cumplimiento de la política de dispositivos móviles por medio de correo electrónico.
- Aceptar las configuraciones de seguridad del dispositivo por medio de correo electrónico, y estas no podrán modificarse mientras se acceda o almacene información de empresa.
- Instalar y configurar un software de antivirus.
- Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.

- Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.
- Configurar la opción de borrado remoto de información en los dispositivos móviles, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

PASO 7: SEGURIDAD DE LOS RECURSOS HUMANOS

7.1. Toma de conciencia, educación y formación en la seguridad de la información

Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Algunas acciones para llevar a cabo este control son:

- Sacar tiempo en las reuniones para explicar temas de conocimiento importantes en la seguridad de la información.
- Realizar una capacitación obligatoria como mínimo cada 3 meses basado en temas importantes, por ejemplo, políticas de la empresa.
- Mostrar estadísticas del estado actual de la empresa conforme a la seguridad de la información.

Costo aproximado de implementación:

Tipo de control	Herramienta gratuita
Herramientas	Cursos de instituciones como INCIBE
Tiempo estimado	Depende del curso
Costo	ninguno

7.2. Proceso disciplinario

Debe existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad que se van a tomar en caso de que algún evento específico ocurra. Se propone la siguiente estructura para Optima Seguridad S.A.:

I. Políticas

- Es deber de todo colaborador cumplir con las normas éticas establecidas y con las políticas y procedimientos establecidos, así como con toda disposición complementaria emanada de la Alta Gerencia.
- El proceso disciplinario será administrado por la Alta Gerencia, la cual velará por el fiel cumplimiento de las disposiciones contenidas en este documento sobre Acciones Disciplinarias.
- El proceso disciplinario estipulado en esta guía de Normas y Acciones Disciplinarias es aplicable a todos los colaboradores. La Alta Gerencia se reserva la potestad de recurrir al mismo, pudiendo proceder a la terminación del contrato de trabajo de cualquier colaborador sin tener que someterlo previamente, al indicado proceso disciplinario.
- Es responsabilidad de los supervisores aplicar las acciones disciplinarias a sus colaboradores cuando fuere necesario, siempre que haya la comisión de una o varias faltas.
- Los supervisores incurren en responsabilidad disciplinaria de importancia cuando toleren, encubran o induzcan a colaboradores a cometer faltas.
- En ninguna circunstancia, el supervisor impondrá medidas disciplinarias sin causa justificada.

- Todo colaborador tiene derecho a recurrir ante la Alta Gerencia cuando crea que la causa por la cual ha sido sometido a la acción disciplinaria, no se justifica o cuando considere que el sometimiento ha sido injusto. Para ello, usará los canales oficiales previstos y se abstendrá de hacer comentarios que provoquen intranquilidad en el personal de su área o de otras áreas.

II. Clasificación de las Faltas

Para la aplicación del presente documento, las faltas han sido clasificadas en leves, graves y muy graves.

- Leves

Son aquellas que no constituyen peligro para la correcta operación de la empresa. Generalmente se refieren a problemas que pueden ser corregidos entre el supervisor y el colaborador. Ejemplos:

- Una ausencia en el mes, sin causa justificada.
- Uso parcial del tiempo del trabajo para otros asuntos (por ejemplo: ventas personales, rifas, extensas conversaciones de asuntos personales, diligencias personales fuera de la empresa, entre otras).
- Cuando se incurra hasta en dos tardanzas en un mes sin causa justificada. Las tardanzas se consideran después de la hora de entrada que le corresponda al colaborador.
- No usar el carné de identificación al ingresar a las oficinas y durante las horas laborables.

- Graves

Son las faltas que constituyen una amenaza para el bienestar y la seguridad de los colaboradores. Ejemplos:

- Violentar procedimientos o documentación de la empresa sin autorización.
 - Retrasos, negligencias o descuidos en el cumplimiento de sus funciones.
 - Ausentarse o no asistir a los eventos de capacitación y entrenamiento convocados por la empresa, sin causa justificada y sin la previa autorización del supervisor.
 - Incurrir en dos inasistencias en un mes sin causa justificada.
- **Muy Graves**
 Son aquellos actos que dañan la imagen de la empresa, causan problemas y dificultades al buen funcionamiento de esta. Ejemplos:
 - Incurrir en falta de probidad o de honradez, actos de violencia, injuria o proferir palabras que atenten contra la moral y la dignidad de supervisores, compañeros, clientes y público en general.
 - Abandono del trabajo.
 - Asistir al trabajo en estado de embriaguez o bajo efectos de estupefacientes
 - Divulgar información confidencial de la empresa o de sus clientes.

III. Acciones Disciplinarias

Las acciones disciplinarias para aplicar según la magnitud de las faltas serán las siguientes:

- **Acciones por Faltas Leves**
 - Amonestación oral en privado.
 - Registro de esta amonestación para fines de seguimiento.
 - Luego de tener 3 amonestaciones orales, estas se deberán plasmar por escrito.

- Acciones por Faltas Graves
 - Amonestación escrita.
 - Registro de esta amonestación para fines de seguimiento.
- Acciones por Faltas Muy Graves
 - Término del contrato de trabajo y, si es pertinente, sometimiento a la acción de la justicia.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	2 horas
Costo	ninguno

PASO 8: GESTIÓN DE ACTIVOS

8.1. Inventario de activos

Todos los activos deben estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes. Se propone la siguiente estructura para el inventario:

Nombre	Cantidad	Tipo	Crítico
Personas	4	[P] Personal	No
Teléfono Fijo	2	[COM] Redes de comunicaciones	Si
Router	1	[COM] Redes de comunicaciones	No
Teléfonos celulares	4	[HW] Hardware / Equipos informáticos	Si
Impresora	1	[HW] Hardware / Equipos informáticos	No
Computadoras de escritorio	1	[HW] Hardware / Equipos informáticos	Sí
Computadoras Portátiles	1	[HW] Hardware / Equipos informáticos	Sí
Memoria USB	3	[HW] Hardware / Equipos informáticos	Sí

Página web informativa	1	[SW] Software / Aplicativos	No
Redes Sociales	2	[SW] Software / Aplicativos	No
Sistema Operativo	4	[SW] Software / Aplicativos	No
Correo Electrónico	4	[S] Servicios	No

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

8.2. Uso aceptable de los activos

Se deben identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. Se propone la siguiente estructura:

1. Sobre la autenticación de usuarios en los equipos

En el caso de computadoras y teléfonos móviles, todos los equipos deben tener mecanismos de autenticación de usuario utilizando los mecanismos más seguros disponibles. Si estos mecanismos permiten la diferenciación por usuarios, esta debe estar habilitada. En el caso que un equipo no tenga esta característica, no se puede utilizar para manejar información sensible de la organización.

2. Sobre la configuración de los equipos desatendidos

Todos los equipos que permitan la característica deben tener habilitados métodos de bloqueo automático después de cierto tiempo de inactividad, pudiendo desbloquear de nuevo el equipo utilizando algún método de

autenticación de usuario. Esta característica debe funcionar de forma adecuada en los momentos en que se deja el equipo desatendido. En el caso que un equipo no tenga esta característica, no puede ser utilizado para manejar información sensible de la organización.

3. Uso de equipos para fines diferentes al trabajo de la organización

Sólo se podrá manipular y/o almacenar información relativa a la organización en los equipos propiedad de esta que se designen para ese fin, excluyendo completamente el uso de equipos personales para manipular cualquier información de la organización.

4. Uso de Antivirus y Antimalware

En computadoras de escritorio y portátiles en donde se maneje información de la organización se requiere la instalación, actualización automática constante y ejecución de software antivirus y antimalware, esto incluye tanto dispositivos propiedad de la organización como aquellos de propiedad personal.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	2 horas
Costo	ninguno

8.2.1 Clasificación de la información

La información debe clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la organización; algunos ejemplos de clasificación son: confidencial, interno, público, etc.

Se propone la siguiente estructura para la clasificación:

Información Confidencial	Es toda aquella información que de ser revelada sin autorización o manejada por entes no autorizados, puede causar graves daños a la empresa. El uso de este tipo de información requerirá de previa autorización por parte del responsable asignado de la misma e incluso la firma de acuerdos de confidencialidad para mayor protección.
Uso Interno	Aquella información que es única y exclusivamente para uso interno de la empresa. Esta información incluye toda aquella información que requiere de cierto nivel de protección pero que no cumple con los criterios necesarios para ser clasificada como confidencial.
Información Pública	Aquella información que se genera para su divulgación pública. Para esta información sólo se deben de implementar los controles adecuados para asegurar la integridad y disponibilidad de esta. Ejemplos de este tipo de información lo constituyen: campañas informativas dirigidas a toda la población; información que por ley reviste carácter público, anuncios públicos, entre otros.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

8.2.2 Etiquetado y manipulado de la información

Se debe desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización. Se propone la siguiente estructura:

Costo aproximado de implementación:

Identificador	Nombre	Clasificación
1	Información de clientes	Información Confidencial
2	Información de proveedores	Información Confidencial
3	Información del personal	Información Confidencial
4	Planes estratégicos	Información Confidencial
5	Políticas, estándares, procedimientos, etc.	Uso Interno
6	Reportes financieros	Uso Interno
7	Circulares internas	Uso Interno
8	Directorios internos	Uso Interno
9	Inventario	Uso Interno
10	Publicidad	Información Publica
11	Información en Redes Sociales	Información Publica
12	Información en Página web	Información Publica

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	2 horas
Costo	ninguno

8.2.3 Manejo de activos

Se debe desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización. Se propone la siguiente estructura para el documento:

1. Respaldos de los activos

- Cada activo inventariado deberá contar con una copia en papel y archivo digital, el cual deberá estar debidamente identificado con

el fin de contar con los respaldos correspondientes en caso de pérdida, robo u otro incidente.

2. De la forma de almacenamiento de la información

- Cada activo identificado e inventariado deberá ser almacenado en áreas seguras del recinto, oficina o área de trabajo, con su correspondiente identificación y correcto almacenamiento.
- Cada activo deberá contener los respectivos códigos de uso, códigos de venta, etc. que identifique el activo, situación que a su vez debe acompañar el año de ejecución correspondiente y centro de responsabilidad.
- Cada activo debe contar con copia digital, la cual deberá contar con una carpeta en la computadora del usuario debidamente identificada.

3. De la transmisión de datos vía correo electrónico

- Todo correo electrónico que sea emitido desde la cuenta institucional deberá identificar claramente el contenido de la información enviada, la firma o identificación del funcionario y en el caso que la información adjunta sea de carácter institucional, legal o de alto contenido técnico, deberá ser enviada con copia a la jefatura.

4. De la destrucción de los activos

- Cuando se eliminen datos o información que este respaldada debidamente en formato físico y digital y/o en sus respectivos archivadores o archivos digitales, podrán ser eliminados solo con la aprobación de jefatura.
- La información destruida deberá ser depositada en los basureros del área de trabajo, dicha información debe estar en formato inutilizable, con el fin de que no pueda ser alterada, utilizada o leída en su totalidad por terceros.

5. De la pérdida o robo de los activos

- En caso de pérdida, robo u otra situación que perjudique los activos inventariados, se deberá informar a jefatura mediante un correo interno, en un plazo no mayor a los 3 días hábiles.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	4 horas
Costo	ninguno

8.3. Gestión de medios removibles

Se debe establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización. Se propone la siguiente estructura para el documento:

- Se encuentra restringida la conexión no autorizada de cualquier elemento de almacenamiento.
- Optima Seguridad S.A. asigna los medios removibles de almacenamiento para que puedan ser utilizados por los funcionarios de la entidad, contratistas y demás terceros facultados en los sistemas de información y en la plataforma tecnológica.
- El uso de medios removibles de almacenamiento solamente es autorizado a los funcionarios, contratistas y demás terceros con el aval de jefatura.
- Los medios de almacenamiento removibles como dispositivos USB, que contengan información institucional, deben ser controlados y físicamente protegidos por el funcionario responsable de la información.
- La información que es almacenada en medios removibles y que debe estar disponible por largo tiempo, es protegida y controlada adecuadamente para evitar que ésta se vea afectada por el tiempo de vida útil del medio.

- La responsabilidad de la información contenida en los medios removibles es del funcionario que está a cargo de este.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	2 horas
Costo	ninguno

PASO 9: CONTROL DE ACCESO

9.1. Política de control de acceso

Se debe establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la organización.

Documento general que recopila las diferentes políticas mencionadas dentro del apartado numero 9 “Control de acceso”, este documento debe contener aspectos como:

- Política de usuarios y grupos
- Gestión de permisos
- Gestión de usuarios
- Gestión de contraseñas
- Mecanismos de autenticación

Costo aproximado de implementación:

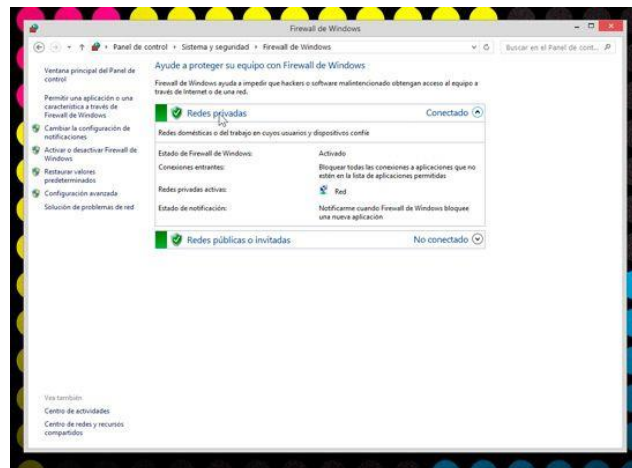
Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word

Tiempo estimado	4 horas
Costo	ninguno

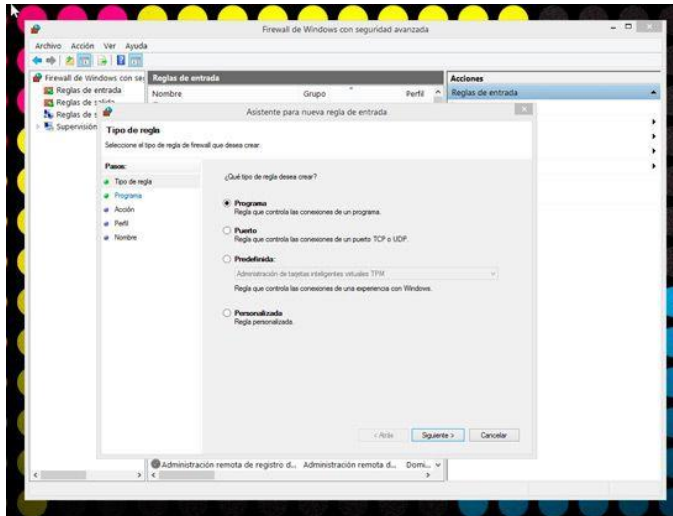
9.1.1. Acceso a redes y a servicios en red

Se debe proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar. Algunas acciones para llevar a cabo este control son:

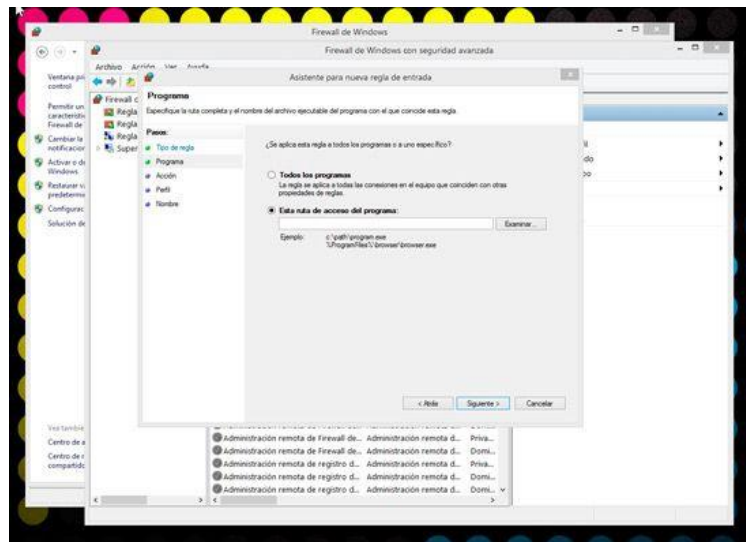
- Utilizar las opciones de configuración del router para bloquear accesos, etc.
 1. Lo primero que tenemos que hacer es ejecutar el Firewall de Windows, lo que podemos hacer fácilmente mediante el Panel de Control.
 2. Una vez en el Panel de Control, nos desplazamos hasta la opción “Sistema y seguridad” y la pulsamos. Luego de ello, presionamos sobre la opción “Firewall de Windows”.
 3. A continuación, en el panel de la izquierda de la ventana, pulsamos sobre el enlace “Configuración avanzada”. Esto abrirá una nueva ventana, en la cual procederemos de la siguiente manera:



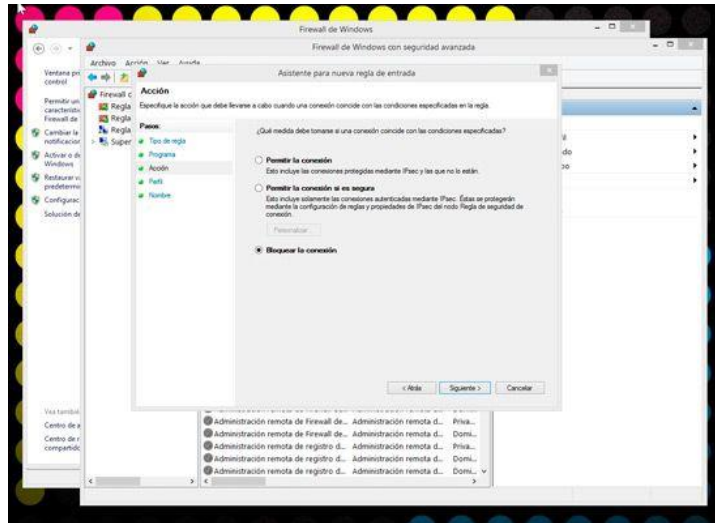
4. Pulsar sobre “Regla de entrada”, opción ubicada en el panel izquierdo.
5. Pulsar, en el panel derecho, sobre la opción “Nueva regla...”.
6. En la ventana que aparece, seleccionamos la opción “Programa” y pulsamos sobre el botón “Siguiente”.



7. A continuación, presionamos sobre la opción “Esta ruta de acceso del programa”. Y buscamos la ubicación del programa a bloquear mediante el botón “Examinar”. Cabe destacar que generalmente los programas se instalan de forma automática en la carpeta “Archivos de programa”.
8. Una vez seleccionado el programa que deseamos bloquear, pulsamos sobre “Siguiente”.



9. En la ventana que aparece, pulsamos sobre la opción “Bloquear la conexión”. Presionamos “Siguiente”.
10. En la nueva ventana que aparece, dejamos seleccionadas las opciones por defecto y presionamos sobre “Siguiente”.



11. Asignamos un nombre que sea fácil de recordar y presionamos sobre el botón “Finalizar”.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Firewall de Windows
Tiempo estimado	30 minutos
Costo	ninguno

9.1.2 Gestión de los derechos de acceso asignados a usuarios

Se debe de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

- La asignación, modificación o revocación de privilegios en el sistema será solicitada por la jefatura.
- Se mantendrá un inventario para control de accesos, en el que se identifiquen los usuarios y los privilegios autorizados y denegados.
- Los soportes y documentos que contengan datos de carácter personal serán accesibles únicamente por el personal autorizado.

- Por tanto, será necesario crear y mantener un inventario de privilegios de acceso, que contenga información relativa a cada usuario y sus privilegios de acceso concedidos.
- La información se creará a la inscripción de un usuario por primera vez y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso.

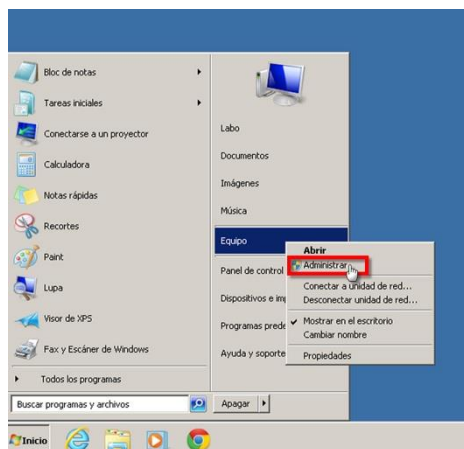
Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

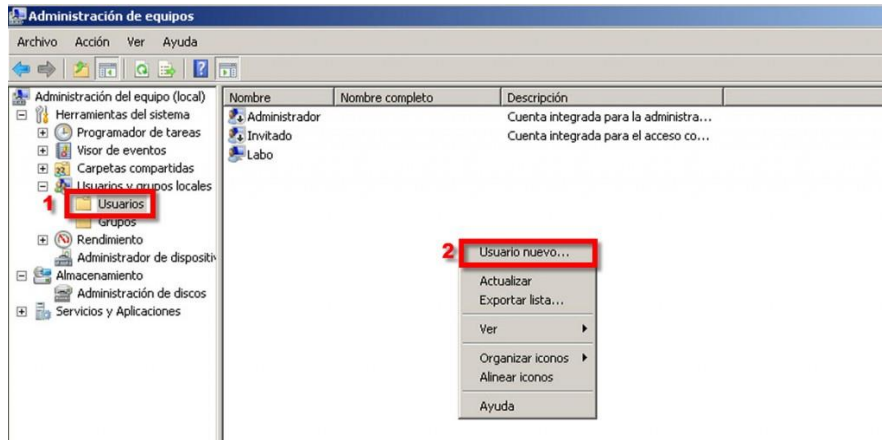
9.1.3 Gestión de los derechos de acceso con privilegios especiales

La asignación y uso de derechos de acceso con privilegios especiales debe ser restringido y controlado. Algunas acciones para llevar a cabo este control son:

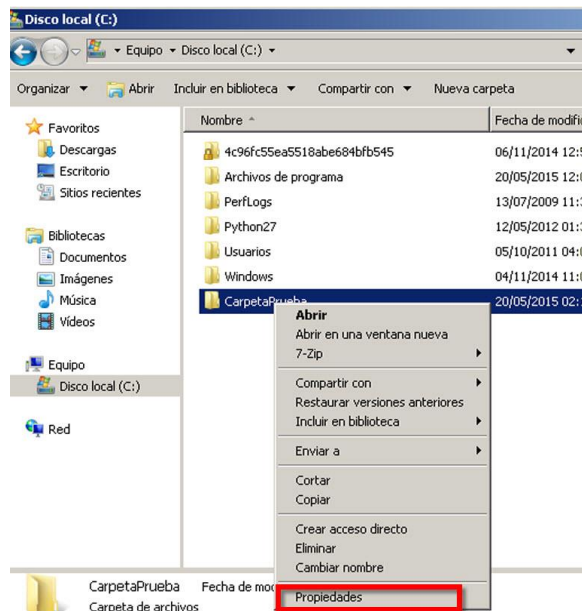
- Como usuario “Administrador”, ir al menú Administrar, al cual se accede mediante clic con el botón derecho sobre el ícono “Mi PC” o “Equipo”.



- Una vez dentro de la carpeta Usuarios (paso 1) se ven los perfiles creados en dicho sistema. Para crear el nuevo, solo basta hacer clic con el botón derecho y seleccionar la primera opción (paso 2).

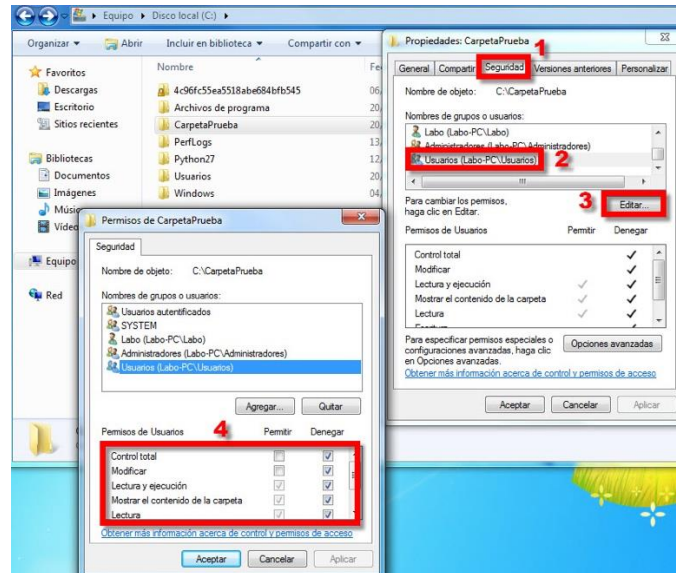


- Definir los permisos en diferentes directorios para tener (o denegar) acceso de escritura o lectura.
 - Se debe hacer clic con el botón derecho en el directorio a modificar los permisos, una vez desplegado el menú, debe accederse a Propiedades.



- Acceder a la pestaña "Seguridad".
- Marcar el grupo a restringir.
- Una vez seleccionado el grupo, hacer clic en el botón "Editar" el cual abrirá una nueva ventana donde permitirá editar los permisos.
- La nueva ventana muestra los permisos que posee ese conjunto de usuarios en este directorio, donde también se puede permitir o

denegar permisos. En este caso, se denegó todos los permisos para que los invitados de este grupo no tengan acceso.



Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Políticas de grupo de Windows
Tiempo estimado	30 minutos
Costo	ninguno

9.1.4 Revisión de los derechos de acceso de usuarios

Se debe revisar de manera periódica que los accesos que tienen los activos sean los correctos. Algunas acciones para llevar a cabo este control son:

- Al menos, cada seis meses, realizar una revisión de los privilegios de acceso de todos los usuarios.
- Cuando se trate de privilegios especiales (administrador), tal revisión de privilegios se deberá realizar, al menos, cada año, y, en cualquier caso, siempre que existan:
 - Alta de nuevos usuarios
 - Baja de usuarios

- Además, los privilegios de acceso de usuarios deben ser revisados siempre que existan cambios en las funciones o responsabilidades.
- Para los tipos de usuarios se tendrán en cuenta, al menos, las siguientes cuestiones:
 - Necesidad de nuevos permisos.
 - Cancelación de antiguos permisos.
 - Segregación de funciones.
 - Modificación de contraseñas de acceso.
 - Notificación al personal implicado de su baja o cambio.
 - Necesidad de retención de registros.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Windows
Tiempo estimado	2 horas
Costo	ninguno

9.1.5 Restricción del acceso a la información

Se debe restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación con la política de control de accesos definida. Aplican las mismas acciones de “Gestión de los derechos de acceso con privilegios especiales”.

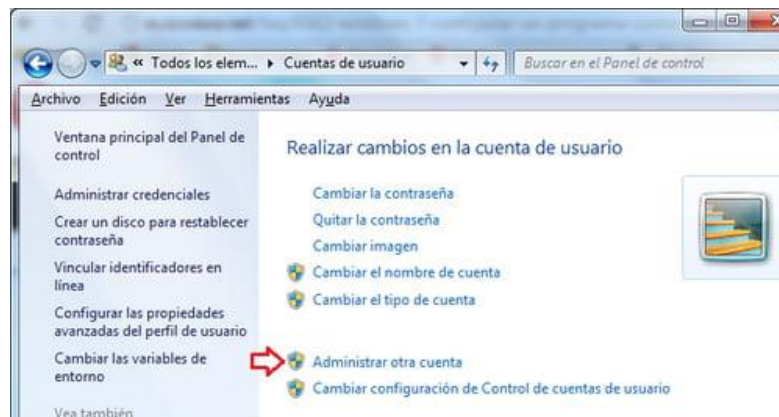
Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Políticas de grupo de Windows
Tiempo estimado	30 minutos
Costo	ninguno

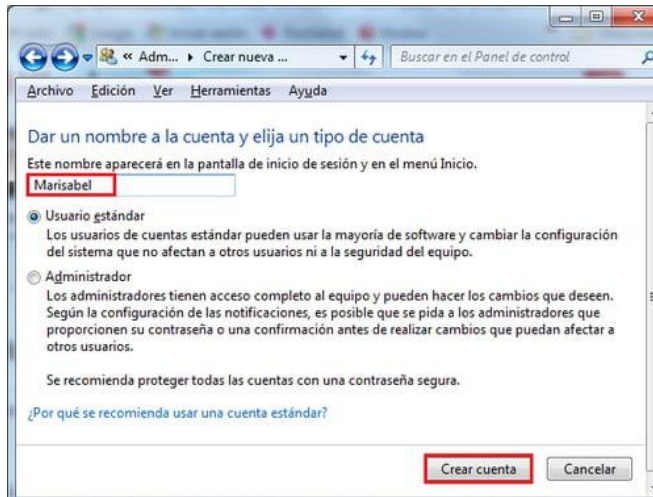
9.2. Procedimiento de ingreso seguro

Cuando sea requerido por la política de control de accesos se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on. Algunas acciones para llevar a cabo este control son:

- Hay que asegurar que todos los equipos y sistemas posean ingresos por medio de usuario y contraseña por cada usuario que exista. Seguidamente se encuentran los pasos para realizar esto:
 - Ir al botón "Inicio > Panel de control > Cuentas de usuario" y hacer clic en el enlace "Administrar otra cuenta".



- En la siguiente ventana, hacer clic en el enlace "Crear una cuenta nueva". En la ventana que se abre, asignar un nombre a la cuenta y elegir un tipo de cuenta: "Usuario estándar" por defecto. Luego hacer clic en "Crear cuenta".



- Finalmente aparece el icono con el nombre del usuario de la cuenta creada.



Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Cuentas de usuario de Windows
Tiempo estimado	20 minutos
Costo	ninguno

9.2.1 Gestión de contraseñas de usuario

Los sistemas de gestión de contraseñas deben ser interactivos y asegurar contraseñas de calidad. Se propone la siguiente estructura:

- Todos los usuarios, independientemente del sistema de información para el que se definan o sean válidas, son responsables de sus contraseñas de acceso a servicios y de los accesos que se produzcan haciendo uso de dichas contraseñas.
- En este sentido, se recomienda a los usuarios observar las siguientes indicaciones en cuanto a la custodia de sus contraseñas:
 - No compartir sus contraseñas con otros usuarios.
 - No anotar sus contraseñas ni introducirlas si alguien está observando.
 - No enviar contraseñas por medios electrónicos o almacenarlas en documentos.
 - El usuario deberá custodiar sus contraseñas de forma efectiva.
 - Todas las contraseñas asignadas a las cuentas activas en el deberán seguir las siguientes restricciones:

Parámetro	Valor
Periodo máximo de rotación	<ul style="list-style-type: none"> • 90 días para cuentas de usuario. • 180 días para cuentas de administración de sistemas.
Caducidad de contraseñas	Automática, al finalizar el periodo máximo de rotación, excepto para contraseñas de administración de sistemas.
Reutilización de contraseñas	Ninguna de las 3 últimas
Longitud mínima	8 caracteres
Requisitos de complejidad	<ul style="list-style-type: none"> • No contener en parte o en su totalidad el nombre de usuario. • Estar compuesta por al menos 3 de los siguientes 4 conjuntos de caracteres: <ol style="list-style-type: none"> 1. Caracteres alfabéticos en mayúsculas.

	<p>2. Caracteres alfabéticos en minúsculas.</p> <p>3. Caracteres numéricos.</p> <p>4. Símbolos/caracteres especiales.</p>
Semántica de contraseñas	<p>Se deberán evitar las contraseñas basadas en:</p> <ul style="list-style-type: none"> • Repetición de caracteres. • Palabras del diccionario. • Secuencias simples de letras, números o secuencias de teclado. • Información fácilmente asociable al usuario como nombres de familiares o mascotas, números de teléfono, matrículas, fechas o en general información biográfica del usuario.

Costo aproximado de implementación:

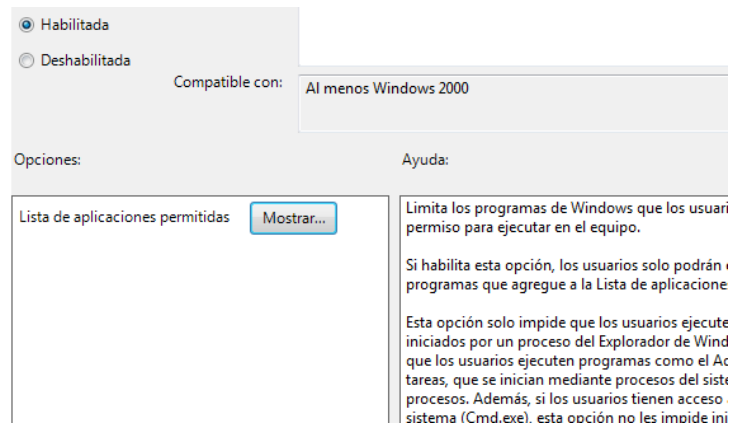
Tipo de control	Herramienta a nivel de equipo
Herramientas	Cuentas de usuario de Windows
Tiempo estimado	30 minutos
Costo	ninguno

9.3. Uso de herramientas de administración de sistemas

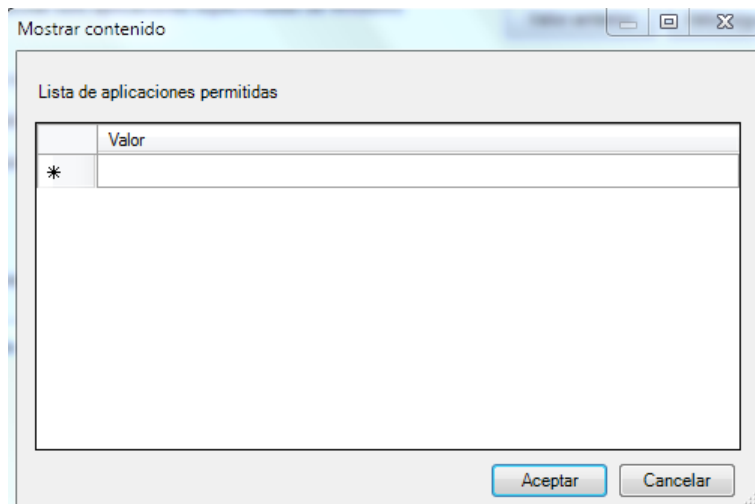
El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deben estar restringidos y estrechamente controlados. Una acción para llevar a cabo este control es:

- Crear políticas de grupo.
 - Iniciar el editor de políticas de grupo, ir al menú de inicio y en el cuadro de búsqueda teclear gpedit.msc.

- Ir a Directiva de equipo local > Configuración de Usuario > Plantillas administrativas > sistema.
- En el panel de la derecha hay una política denominada “ejecutar solo aplicaciones específicas de Windows”; para configurarla, solo se debe hacer doble clic sobre la misma, habilitarla y a hacer clic en el botón “mostrar”.



- A continuación, se nos mostrará un cuadro de dialogo en el que podremos especificar la lista de aplicaciones que queremos permitir y pulsar Aceptar.



Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Políticas de grupo de Windows

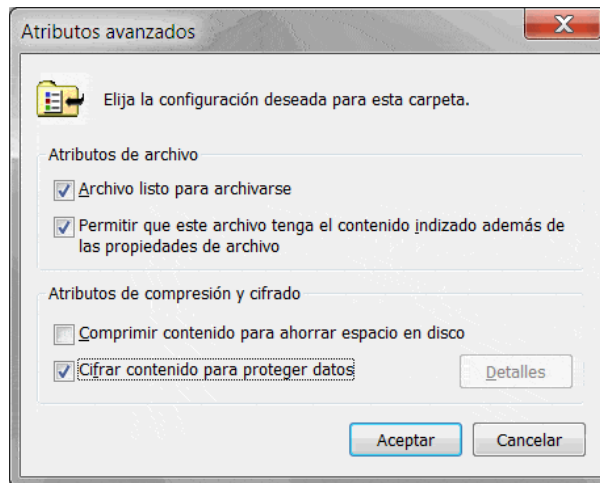
Tiempo estimado	30 minutos
Costo	ninguno

PASO 10: CIFRADO

10.1. Política de uso de los controles criptográficos

Se debe desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información. Una acción para llevar a cabo este control es:

- Utilizar funcionalidades que vienen integradas en Windows.
 - Haz clic con el botón derecho en un archivo o carpeta (o mantenlo presionado) y selecciona “Propiedades”.
 - Selecciona el botón “Avanzados” y haz clic en la casilla de verificación “Cifrar contenido para proteger datos”.



- Pulsa el botón “Aceptar” para cerrar la ventana Atributos avanzados y a continuación, selecciona el botón “Aplicar” y después “Aceptar”.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Cifrado de Windows

Tiempo estimado	10 minutos
Costo	ninguno

PASO 11: SEGURIDAD FÍSICA Y DEL ENTORNO

11.1. Perímetro de seguridad física

Se deben definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica. Para Optima Seguridad S.A. se proponen las siguientes medidas:

- Diseñar paredes sólidas en las áreas críticas.
- Mantener los portones cerrados con llave.
- Identificar claramente las salidas de emergencia en caso de escenarios catastróficos.

Costo aproximado de implementación:

Tipo de control	Infraestructura
Herramientas	Cerraduras
Tiempo estimado	30 min c/u
Costo	Ø25.000 c/u

11.2. Controles físicos de entrada

Las áreas seguras deben estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso. Para Optima Seguridad S.A. se proponen las siguientes medidas:

- Registrar el ingreso de terceros por medio de una bitácora.

Registro de Visitas					
No.	Fecha	Hora de entrada	Nombre Completo	Hora de Salida	Firma

- Todos los funcionarios deben portar el carné que los identifique.

- Está prohibido prestar el carné de identificación.
- La pérdida del carné de identificación debe ser reportado a jefatura inmediatamente.
- El ingreso de computadoras que no sean de propiedad de la empresa debe ser registrado en una bitácora de registro de equipos.

Registro de Equipos	
Fecha	
Hora de entrada	
Hora de salida	
Nombre	
Apellido (s)	
Marca	
Serial	
Firma	

Costo aproximado de implementación:

Tipo de control	Físico
Herramientas	Elaboración de gafetes de identificación
Tiempo estimado	-
Costo	¢2.000 c/u

11.3. Seguridad de oficinas, despachos y recursos

Se debe diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización. Para Optima Seguridad S.A. se proponen las siguientes medidas:

- Los puestos de trabajo deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, esto para evitar el acceso no autorizado a la información.

- Colocar las pantallas de los computadores en una posición en la que se evite que personal no autorizado pueda ver la información que se encuentre desplegada en ellas.
- Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizados por los funcionarios autorizados y no deben ser transferidos a otros funcionarios de la organización.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- No dejar abandonada en las impresoras información confidencial, una vez se haya impreso.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

11.4. Protección contra amenazas externas y ambientales

Se debe diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes. Como medidas físicas contra las amenazas, pueden incluirse medidas de construcción que disminuyen la probabilidad de daño. Entre ellas pueden encontrarse:

- Impedir el ingreso de equipos que registren información, a menos que hayan sido formalmente autorizadas por jefatura.
- No se permite comer, beber y fumar dentro de las instalaciones.
- Contar con al menos un extintor en las instalaciones, en caso de incendio.

Costo aproximado de implementación:

Tipo de control	Físico
Herramientas	Extintor
Tiempo estimado	-
Costo	Ø27.000 c/u

11.2. Ubicación y protección de los equipos

Aplicar protección física a los equipos, por medio de acciones como bloqueo de pantalla, ubicar los equipos en áreas que no sean de fácil acceso, etc. Algunas acciones para llevar a cabo este control son:

- Servicio de vigilancia, donde el acceso es controlado por personal de seguridad que comprueben la identificación de todo aquel que quiera acceder a una ubicación.
- Establecer un perímetro de seguridad física, por ejemplo, cercas para evitar el ingreso a las instalaciones, paredes para cerrar áreas, etc.

Costo aproximado de implementación:

Tipo de control	Personal
Herramientas	Vigilancia
Tiempo estimado	-
Costo	Ø300.000 al mes

11.2.1. Servicios de suministro

Los equipos deben estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo. Una acción para llevar a cabo este control es la instalación de sistemas de alimentación ininterrumpida (SAI), lo siguiente son los pasos para realizar la instalación:

- Identificar los equipos mas críticos.

- Determinar la potencia necesaria en la fuente de alimentación para soportar estos equipos.
- Conectar UPS (fuentes de poder) a los dispositivos.
 - Ubicar el SAI
 - Lo más importante es ubicarlo en un lugar con cierta ventilación y, no pongamos nada sobre o alrededor del SAI, o tapemos las ranuras de ventilación, impidiendo su normal refrigeración.
 - Conectar equipos y corriente eléctrica
 - El siguiente paso será conectar los equipos y corriente eléctrica. Para evitar problemas se recomienda conectar primero todos los equipos, dejando la conexión eléctrica para el final.
 - Encender el SAI
 - Cuando tengamos todos nuestros cables conectados, procederemos a encender el SAI. Según el modelo, es posible que se enciendan múltiples luces o alarmas sonoras. Probablemente se trate de los avisos de que la batería está baja, aunque también puede avisarnos de sobrecarga, pues habremos conectado al SAI equipos que consumen más de lo permitido.
 - Conectar el SAI al PC
 - Lo primero que tendremos que hacer será conectar el SAI a nuestro PC gracias al puerto USB, utilizando para ello un cable específico que nos entrega el fabricante.
 - Hecho esto, nuestra máquina detectará automáticamente el nuevo componente.
 - Una vez instalada la aplicación, aparecerá un nuevo icono con forma de enchufe en la barra de tareas, junto al reloj. Haciendo doble clic sobre él se cargará la ventana de Opciones de energía, que también podemos encontrar en el

Panel de Control de Windows. Ahí obtendremos un vistazo del estado general del SAI, la carga de la batería, la carga de trabajo y el estado.

- Realizar ajustes
 - Sin salir de la ventana en la que nos encontramos, el primer ajuste que podremos realizar es el momento en que nuestro equipo se apagará en caso de corte eléctrico. Para ello, no tendremos más que deslizar la barra que se encuentra bajo el indicador de batería, siendo el 30% la cifra que por defecto se nos marcará. Ello quiere decir que, funcionando con baterías, el equipo comenzará automáticamente el proceso de apagado cuando a la batería le reste un 30% de capacidad.
 - Haciendo clic sobre Settings podremos acceder a más funciones. Podremos decidir el apagado por tiempo, decidir el tipo de apagado (suspensión, hibernación o apagado), ejecutar un script determinado al apagar la máquina, e incluso indicar el apagado del SAI para que este vuelva a funcionar cuando vuelva la corriente.

Costo aproximado de implementación:

Tipo de control	Físico
Herramientas	UPS
Tiempo estimado	-
Costo	€30.000 c/u

11.2.2. Seguridad del cableado

Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deben proteger contra la interceptación, interferencia o posibles daños. Algunas acciones para llevar a cabo este control son:

- Asegurar que existan las conexiones adecuadas para la energía eléctrica y la red de datos.
- Solicitar fibra óptica al proveedor de servicio con el fin de evitar posibles interferencias o daños.

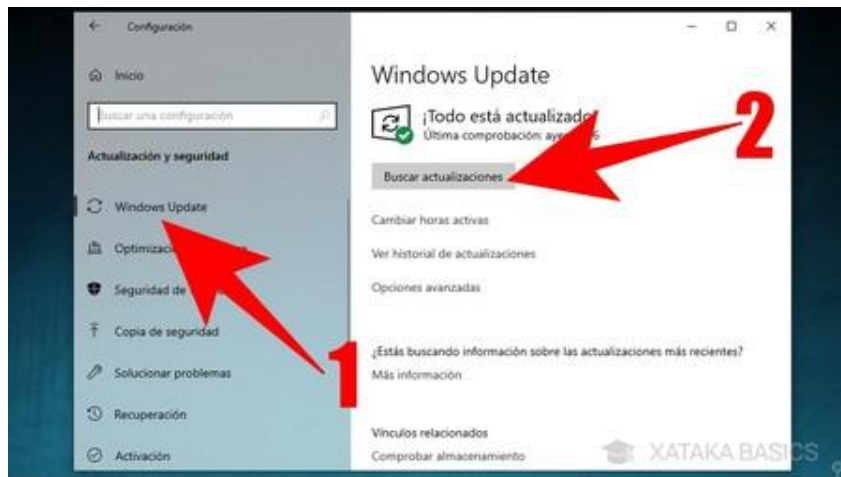
Costo aproximado de implementación:

Tipo de control	Físico
Herramientas	Fibra Óptica
Tiempo estimado	-
Costo	€20.000 al mes

11.2.3. Mantenimiento de equipos

Mantener los equipos actualizados, en la mayoría de los casos los dispositivos traen herramientas de actualización automática por lo que facilita esta tarea. Algunas acciones para llevar a cabo este control son:

- Descargar las últimas versiones de los programas desde sitios oficiales.
- Utilizar herramientas integradas como Windows Update para aplicar actualizaciones de manera automática.
 - En la barra de tareas Inicio, buscar Windows Update.
 - Aparecerá la siguiente ventana, en la cual debemos hacer clic en Buscar actualizaciones.



- Realizado lo anterior, se desplegará una pantalla donde debemos hacer clic en Comprobar e instalar actualizaciones.
- Concluido este paso, se encuentra en condiciones de instalar las actualizaciones.
- Una vez finalizado el proceso de descarga, debe reiniciar su PC.
- Cada mes Microsoft lanza actualizaciones de seguridad, se recomienda instalarlas y mantener siempre nuestro equipo actualizado.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Windows Update
Tiempo estimado	30 minutos
Costo	ninguno

11.2.4. Salida de activos fuera de las dependencias de la empresa

Los equipos, la información o el software no se deben retirar del sitio sin previa autorización. Algunas medidas para llevar a cabo este control son:

- El uso de equipos de cómputo, portátiles, etc. fuera de las instalaciones, será autorizado por el responsable.
- El usuario que está autorizado a retirar un equipo de cómputo o portátil debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de la entidad.

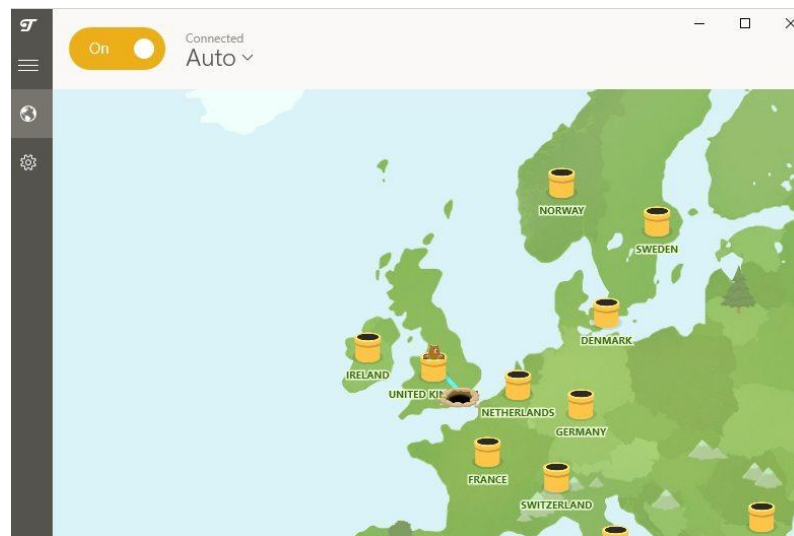
Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	30 minutos
Costo	ninguno

11.2.5. Seguridad de los equipos y activos fuera de las instalaciones

Se debe aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos. Algunas medidas para llevar a cabo este control son:

- Uso de aplicaciones gratuitas como TunnelBear para conexiones seguras por medio de VPN (sirve tanto para computadoras como para dispositivos móviles).
 - Descargar la aplicación.
 - Iniciar la aplicación.
 - Crear una cuenta gratuita.
 - Dar permisos a la aplicación.
 - Marcar el país donde se encuentra en la parte inferior de la pantalla.
 - Activar o desactivar el servidor VPN con el botón ubicado en la parte superior.



Costo aproximado de implementación:

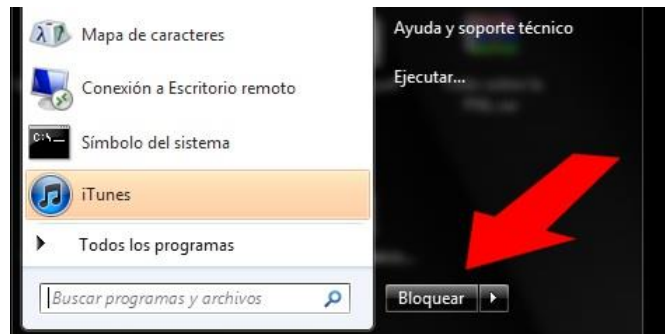
Tipo de control	Herramienta gratuita
Herramientas	TunnelBear
Tiempo estimado	30 minutos
Costo	ninguno

11.2.6. Equipos de usuario desatendidos

Los usuarios se deben de asegurar que los equipos que no se estén utilizando cuenten con la protección adecuada, por ejemplo, acciones como: contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos.

Algunas medidas para llevar a cabo este control son:

- Bloquear la sesión de los equipos de cómputo cuando no se encuentren en su lugar de trabajo.
 - Ir al Menú Inicio y seleccionar “Bloquear”.



- Cerrar sesión en los equipos de cómputo al finalizar la jornada laboral.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Bloqueo de Windows
Tiempo estimado	30 minutos
Costo	ninguno

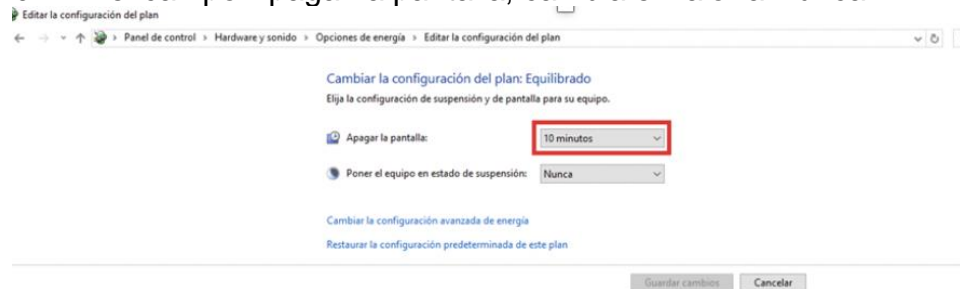
11.2.7. Política de escritorio y pantalla limpios

Se debe adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información. Algunas medidas para llevar a cabo este control son:

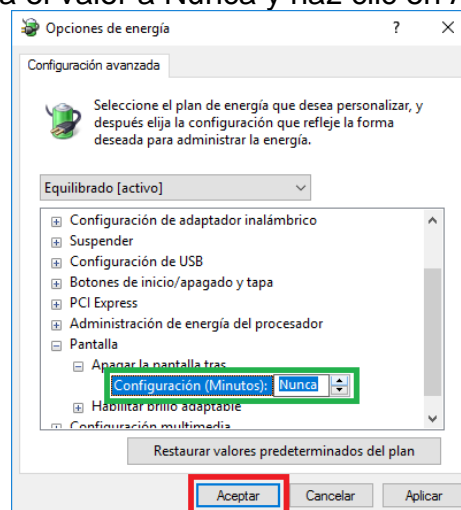
- Conservar el escritorio del equipo libre de información de uso interno o confidencial.
- Aplicar un protector de pantalla estándar en todas las estaciones de trabajo y equipos portátiles, de forma que se active luego de 2 minutos sin uso.
 - Presiona las teclas de [Windows] + [R], escribe el comando control y haz clic en Aceptar.
 - Selecciona: Hardware y sonido > Opciones de energía > Elegir cuándo la pantalla se apaga.



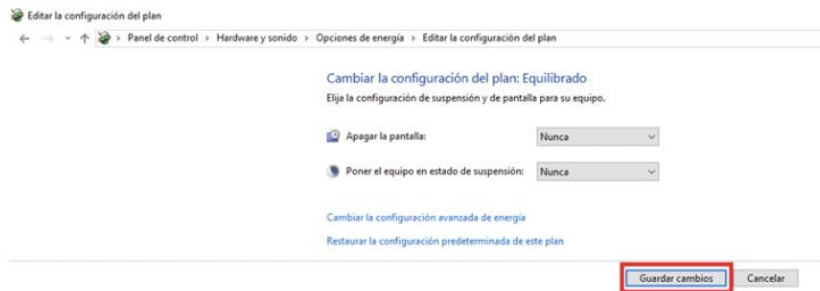
- En el campo Apagar la pantalla, cambia el valor a Nunca.



- Haz clic en Cambiar la configuración avanzada de energía.
- Busca la rama Pantalla > Apagar la pantalla tras > Configuración.
- Luego cambia el valor a Nunca y haz clic en Aceptar.



- Finalmente, en la ventana Editar la configuración del plan, haz clic en Guardar cambios.



- Guardar en un lugar seguro cualquier documento, “llave maya”, etc. que contenga información confidencial o de uso interno.
- No dejar en el escritorio físico documentos de uso confidencial sin custodia.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Opciones de energía de Windows
Tiempo estimado	30 minutos
Costo	ninguno

PASO 12: SEGURIDAD DE LAS OPERACIONES

12.1. Procedimientos de operación documentados

Se deben documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten. Se propone la siguiente estructura para los procedimientos:

Titulo	Proceso De Venta
Frecuencia	Diario
Responsable	Ejecutivo de Ventas

Procedimiento	<ol style="list-style-type: none"> 1. Se establece el contacto del cliente con la empresa a través del ejecutivo. 2. El ejecutivo de ventas asesora al cliente sobre el producto y las diferentes formas de compra (contado, crédito). 3. El cliente realiza el pedido. 4. Jefatura aprueba el pedido. 5. Se elabora la factura. 6. El producto es enviado al cliente por medio del mensajero. 7. El técnico se desplaza a las instalaciones del cliente para realizar la instalación.
---------------	---

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	4 horas
Costo	ninguno

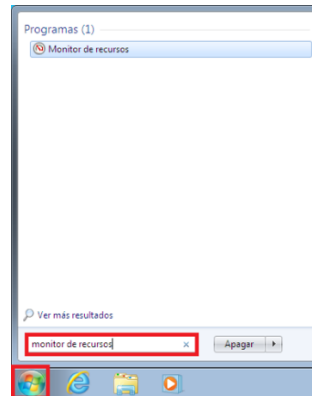
12.2. Gestión de capacidad

Se debe monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas. Algunas medidas para llevar a cabo este control son:

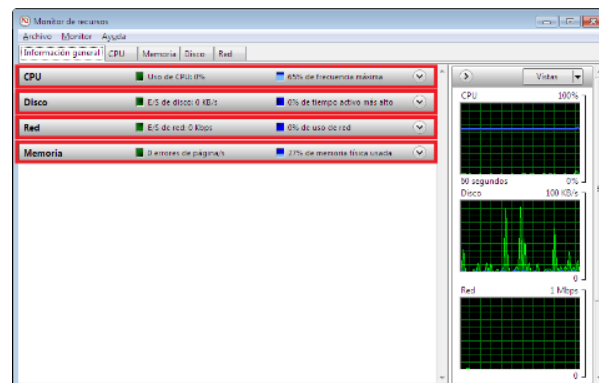
- Utilizar herramientas integradas en Windows como el administrador de tareas para monitorear aspecto como porcentaje de utilización del CPU,

porcentaje de uso de memoria, porcentaje de uso de disco, porcentaje de uso de red, entre otros.

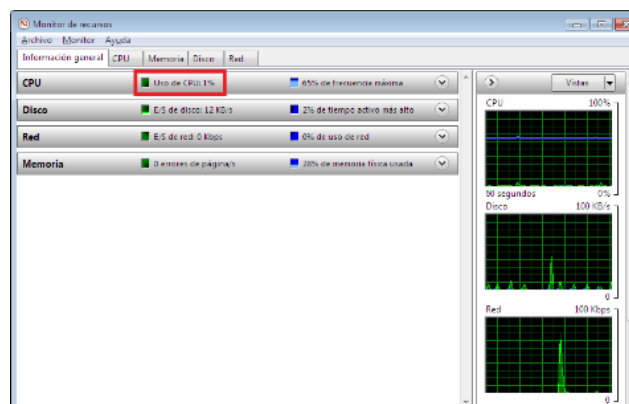
- Haz clic en Inicio y, en el cuadro de búsqueda, escribe monitor de recursos. A continuación, presiona “Enter”.



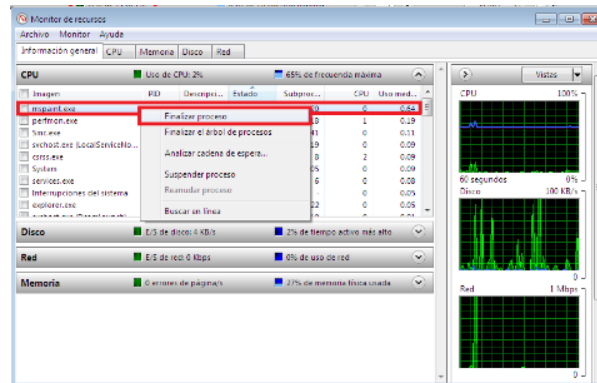
- En la ventana principal del monitor de recursos, aparecen los cuatro recursos que puedes monitorear: CPU, Memoria, Disco y Red. Aquí puedes obtener un breve resumen del estado de cada recurso.



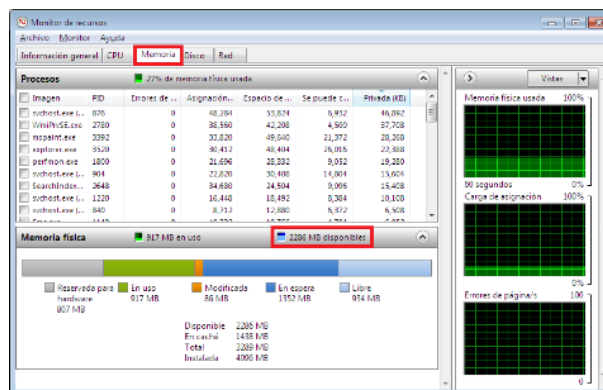
- Asegúrate de que el uso de CPU se mantenga por debajo del 70%. De lo contrario, ingresa en la pestaña CPU para comprobar qué proceso está consumiendo más recursos.



- Cuando detectes el proceso que desees cerrar, haz clic derecho y selecciona Finalizar proceso.



- Asegúrate de que la cantidad de memoria disponible sea mayor a 100 mb. Para ello, haz clic en la pestaña Memoria y verifica el valor que se muestre en la barra Memoria física.



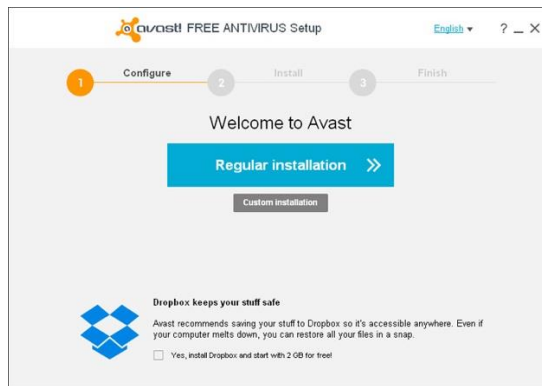
Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Administrador de tareas de Windows
Tiempo estimado	30 minutos
Costo	ninguno

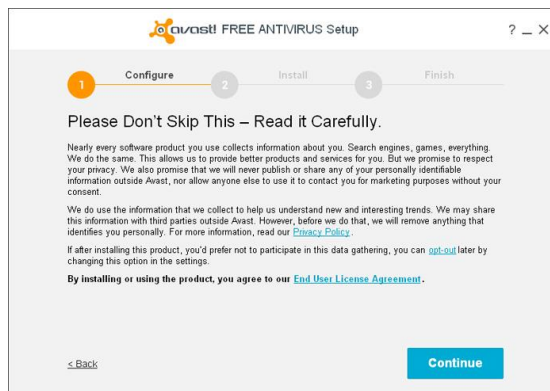
12.2.1. Controles contra códigos maliciosos

Se deben implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios. Algunas acciones para llevar a cabo este control son:

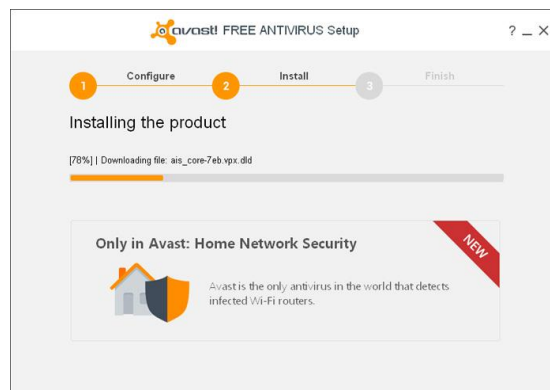
- Instalación de antivirus gratuitos que pueden instalarse de manera individual en los equipos, por ejemplo, AVAST Antivirus.
 - Descargar el programa de la página oficial de Avast.
 - Ejecutar el archivo llamado “avast_free_antivirus_setup.exe”, o “avast_free_antivirus_setup_online.exe”.
 - Elegir el tipo de instalación “Regular”, que es el recomendado.



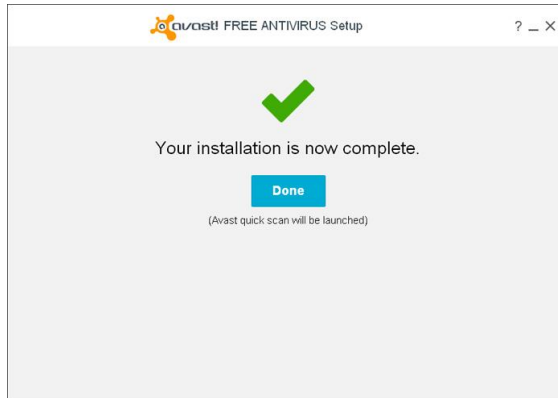
- Aceptar los términos y condiciones.



- El proceso de instalación inicia.



- Una vez finalizado aparece el siguiente mensaje y el equipo está protegido.



Nota: En este caso, a pesar de que existe cierto grado de protección con la versión gratuita, se recomienda comprar la versión Premium con el fin de ampliar las áreas de seguridad y evitar que queden posibles áreas en exposición.

Costo aproximado de implementación:

Tipo de control	Herramienta gratuita
Herramientas	AVAST Antivirus
Tiempo estimado	1 hora por computadora
Costo	€40.000 al año

12.3. Gestión de las vulnerabilidades técnicas

Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados. Algunas acciones para llevar a cabo este control son:

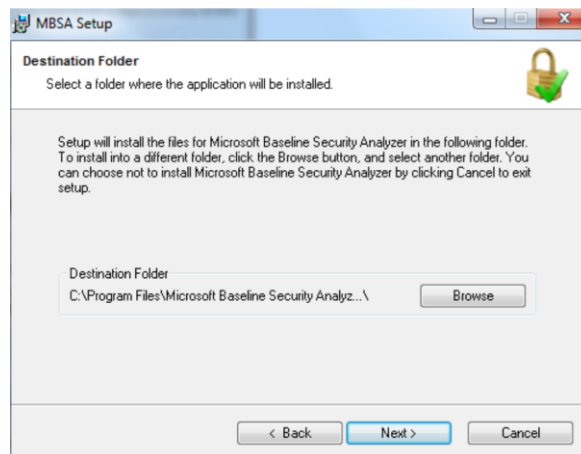
- Utilizar herramientas integradas de Microsoft como Microsoft Baseline Security Analyzer (MBSA) para comprobar las vulnerabilidades de los sistemas.
 - Descargar la aplicación del sitio oficial de Microsoft.
 - Ejecutar el instalador (archivo .exe) y haga clic en “next”.



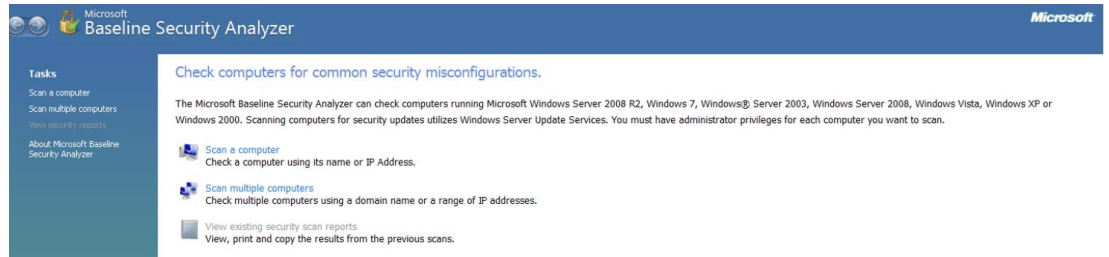
- Acepte los términos de la licencia y haga clic en “next”.



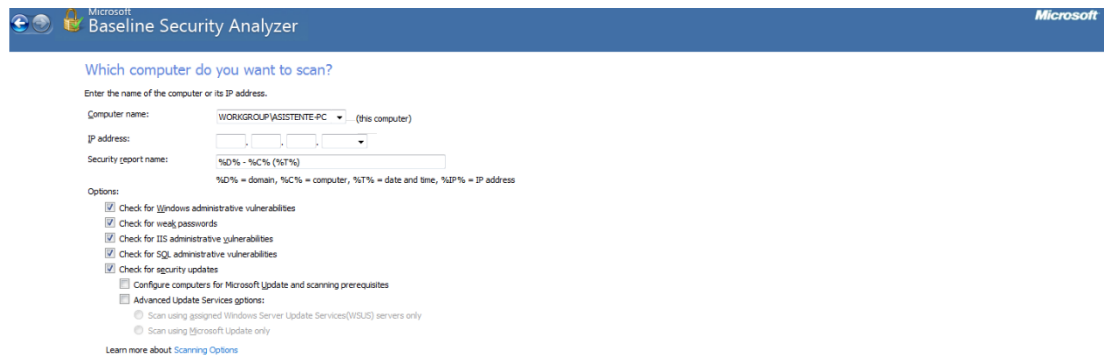
- Escoja el lugar de instalación y haga clic en “next”.



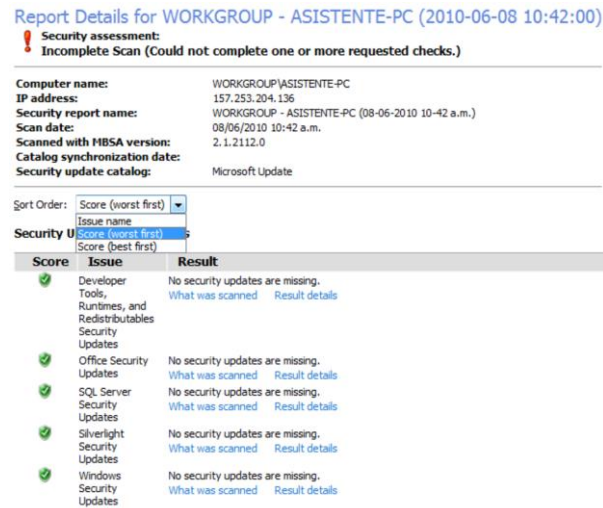
- Para finalizar haga clic en Instalar, a continuación, el programa se desplegará.
- Seleccionar la opción escaneo de computadora.



- Escoger la computadora que se quiere analizar.



- Se despliega el resultado del análisis.



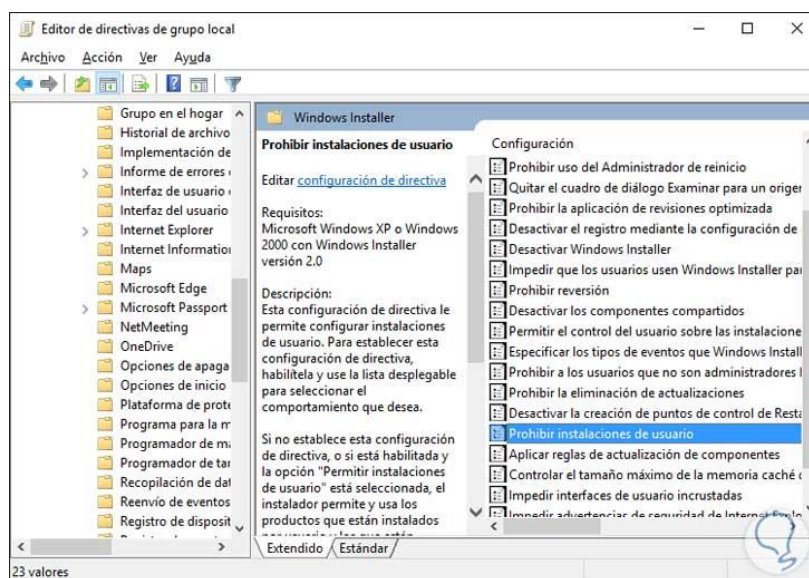
Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Baseline Security Analyzer (MBSA)
Tiempo estimado	1 hora por computadora
Costo	ninguno

12.4. Restricciones en la instalación de software

Se deben establecer e implementar las reglas que regulen la instalación de software por parte de los usuarios. Algunas acciones para llevar a cabo este control son:

- Utilizar herramientas integradas de Microsoft como Windows Installer.
 - Pulsar en el botón de inicio (Windows) y pulsar la letra R.
 - Escribir en esta ventana de ejecutar el siguiente comando: gpedit.msc
 - Ir a Configuración del Equipo > Plantillas Administrativas > Componentes de Windows > Windows Installer.
 - Ahora aparecerán opciones para gestionar, selecciona: Prohibir instalaciones del usuario.



- Seleccionar “Habilitada”.
-

Costo aproximado de implementación:

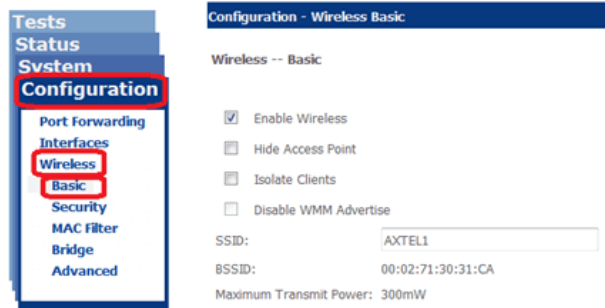
Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Windows Installer
Tiempo estimado	30 minutos por computadora
Costo	ninguno

PASO 13: SEGURIDAD DE LAS COMUNICACIONES

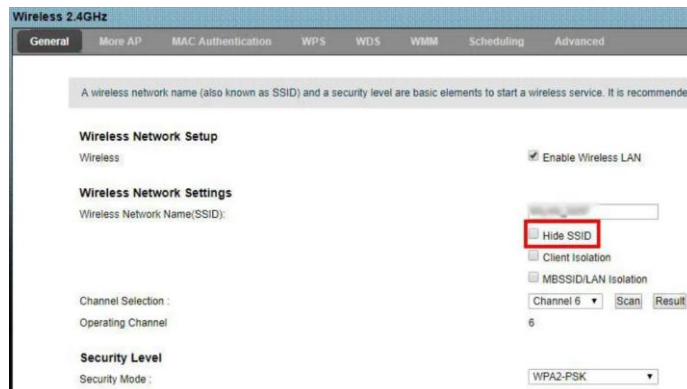
13.1. Controles de redes

Se deben administrar y controlar las redes para proteger la información en sistemas y aplicaciones. Algunas acciones para llevar a cabo este control son:

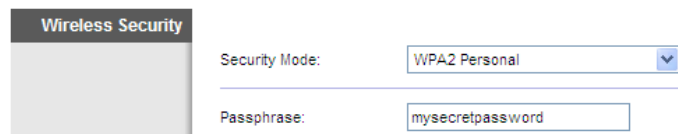
- Cambiar el nombre de la red (SSID)
 - Acceder a los ajustes del router.
 - Ir al apartado “Wireless”.
 - En SSID Settings, modificar el nombre en SSID Name.



- Dale a “Guardar”.
- Ocultar el nombre de la red (SSID)



- Asegurarse de que se utiliza el protocolo de seguridad WPA2



- Modificar las credenciales que vienen configuradas por defecto



Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Ajustes del router
Tiempo estimado	30 minutos
Costo	ninguno

13.1.1. Mecanismos de seguridad asociados a servicios en red

Se deben identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados. Se presenta la siguiente estructura para los acuerdos de servicios:

a. Alcance y objetivos

El presente acuerdo establece los términos y condiciones a las que _____RAZON SOCIAL PROVEEDOR_____, en adelante PROVEEDOR, está sujeto en el ámbito de la prestación del servicio de _____SERVICIO PRESTADO_____ a _____RAZON SOCIAL CLIENTE_____, en adelante Óptima Seguridad S.A. Este acuerdo persigue establecer unos niveles de calidad en la prestación del servicio proporcionado por PROVEEDOR.

b. Partes

A continuación, se identifican las partes que suscriben el presente acuerdo:
De una parte, Óptima Seguridad S.A., con C.I.F. _____CIF CLIENTE_____ y domicilio social en _____DOMICILIO SOCIAL CLIENTE_____, representada por _____NOMBRE DEL REPRESENTANTE CLIENTE_____ actuando en nombre y representación de esta entidad en virtud de su condición de _____CARGO REPRESENTANTE CLIENTE_____. De otra parte, PROVEEDOR como prestadora del servicio _____SERVICIO_____, con C.I.F. _____CIF PROVEEDOR_____ y domicilio social en _____DOMICILIO SOCIAL PROVEEDOR_____, representada por _____NOMBRE DEL REPRESENTANTE PROVEEDOR_____ actuando en nombre y representación de esta entidad en virtud de su condición de _____CARGO REPRESENTANTE PROVEEDOR_____.

c. Duración

El presente acuerdo se inicia con fecha efectiva de _____DD de MM del AAAA_____, siendo la duración de este la establecida hasta la fecha de finalización del contrato.

d. Descripción del servicio

El servicio prestado por PROVEEDOR a Óptima Seguridad S.A. y al cual se encuentra vinculado el presente acuerdo es _____SERVICIO PRESTADO_____ consistente en _____DESCRIPCION DEL SERVICIO_____.

Dentro de este servicio, a continuación, se describen las tareas que se encuentra incluidas:

_____TAREA 1 - DESCRIPCION DE LA TAREA_____

_____TAREA 2 - DESCRIPCION DE LA TAREA_____

...

_____TAREA N - DESCRIPCION DE LA TAREA_____

e. Disponibilidad

Los componentes del servicio destinados a cada una de las tareas tendrán asociada una disponibilidad de acuerdo con la siguiente tabla:

Tarea	% de Disponibilidad	Horario del Servicio
Ejemplo: 1	Ejemplo: 99,99	Ejemplo: 24x7

Los servicios prestados se ofrecerán con la disponibilidad citada con anterioridad a excepción de las franjas establecidas para las ventanas de mantenimiento.

f. Continuidad

PROVEEDOR se compromete a restablecer el servicio los niveles de servicio ofertados, ante la materialización de una contingencia grave en un plazo no superior a _____XX horas/días_____ desde el momento del siniestro.

g. Seguimiento del servicio

Todas las tareas descritas en el apartado “d” de este acuerdo dispondrán de monitorización que permita un seguimiento en tiempo real del grado de cumplimiento de los niveles de servicio. Por otra parte, se proporcionará a Óptima Seguridad S.A. informes mensuales que indicarán el rendimiento de los niveles de servicio. Este informe se pondrá a disposición de Óptima Seguridad S.A. durante la primera semana de cada mes.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	2 horas
Costo	ninguno

13.2. Mensajería electrónica

Se debe proteger adecuadamente la información referida en la mensajería electrónica. Algunas acciones para llevar a cabo este control son:

- Hacer uso de aplicaciones gratuitas como ProtonMail que permiten enviar correos cifrados, con encriptación de extremo a extremo para que los mensajes sólo puedan ser vistos por usted y el destinatario.
 - Registrarse y seleccionar la cuenta gratuita.



Seleccione su tipo de cuenta de ProtonMail

ProtonMail es un servicio gratuito para el bien público. Puede ayudar a proteger la privacidad en línea eligiendo una cuenta de pago. Su contribución nos ayuda a mantener más usuarios y a continuar desarrollando ProtonMail como software libre y de código abierto.


GRATIS	Cuenta básica con funciones limitadas	▼
PLUS	Correo electrónico seguro con funciones avanzadas	4.00 € /Mes ▲

Con un plan Plus, puede tener la cuenta de correo electrónico más avanzada y segura al tiempo que apoya nuestra misión de proteger la privacidad en línea.

Nuestras cuentas PLUS incluyen:

- ✓ 5 GB de almacenamiento
- ✓ 1000 mensajes enviados por día

- Crear y validar cuenta.



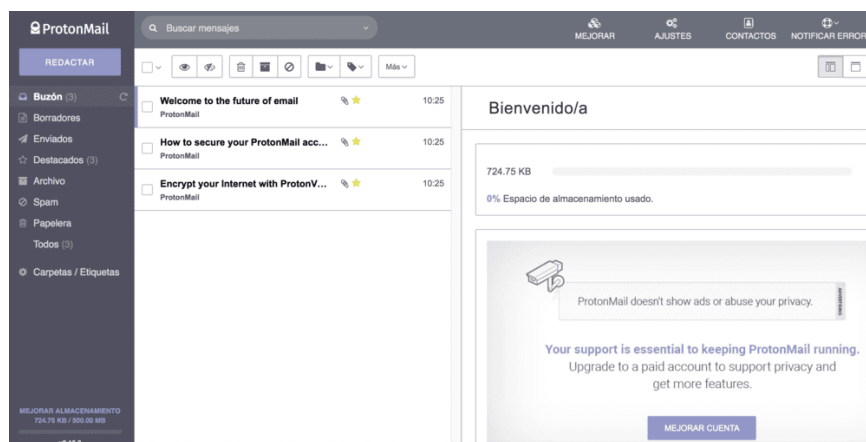
ProtonMail
CREE SU CUENTA

¡Recupere su privacidad! Crear su cuenta de correo electrónico seguro toma menos de 2 minutos.

- Nombre de usuario y dominio**
Esta será su nueva dirección de correo electrónico de ProtonMail.
Elija un nombre de usuario: @ protonmail.com
- Contraseña**
Elija una contraseña
Confirmar contraseña

Si pierde su contraseña, no será capaz de leer sus correos electrónicos.

- Y lista para enviar correos.



ProtonMail

Buscar mensajes

MEJORAR AJUSTES CONTACTOS NOTIFICAR ERROR

REDACTAR

Buzón (3)
Borradores
Enviados
Destacados (3)
Archivo
Spam
Papelera
Todos (3)
Carpetas / Etiquetas

MEJORAR ALMACENAMIENTO
724.75 KB / 500.00 MB
v1.15.3

Welcome to the future of email
ProtonMail 10:25

How to secure your ProtonMail acc...
ProtonMail 10:25

Encrypt your Internet with ProtonV...
ProtonMail 10:25

Bienvenido/a

724.75 KB

0% Espacio de almacenamiento usado.

ProtonMail doesn't show ads or abuse your privacy.

Your support is essential to keeping ProtonMail running.
Upgrade to a paid account to support privacy and get more features.

MEJORAR CUENTA

Costo aproximado de implementación:

Tipo de control	Herramienta gratuita
Herramientas	ProtonMail
Tiempo estimado	1 hora por usuario
Costo	ninguno

PASO 15: RELACIONES CON SUMINISTRADORES

15.1. Cadena de suministro en tecnologías de la información y comunicaciones

Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones. Se proponen las siguientes condiciones:

1. Optima Seguridad S.A. no aceptará ningún producto y/o servicio que no haya sido solicitado a través de una orden de compra. Será requisito referenciar debidamente el número de orden de compra en la factura.
2. Los productos y/o servicios sólo se entenderán aceptados una vez que jefatura verifique que se ajustan a las especificaciones estipuladas en la orden de compra. En caso contrario serán rechazados o considerados no entregados o prestados.
3. Optima Seguridad S.A. se reserva el derecho de devolver los productos o considerar no prestado los servicios, si se determinara posteriormente que no cumplen las condiciones especificadas en la orden de compra y sus adjuntos, aun cuando Optima Seguridad S.A. haya pagado todo o parte de los productos o servicios incluidos en la orden de compra.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	1 hora
Costo	ninguno

15.2. Supervisión y revisión de los servicios prestados por terceros

Las organizaciones deben monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.

Aplican las acciones del apartado “g” de “13.1.1. Mecanismos de seguridad asociados a servicios en red”.

Costo aproximado de implementación:

Tipo de control	Herramienta a nivel de equipo
Herramientas	Microsoft Word
Tiempo estimado	2 horas
Costo	ninguno

La siguiente tabla muestra el costo total aproximado de implementación:

Costo Total Aproximado de Implementación				
Control	Herramienta	Costo	Cantidad	Costo Total
6.1.1 Asignación de responsabilidades para la segur. de la información	Microsoft Word	-	-	-
6.1.2 Segregación de tareas	Microsoft Word	-	-	-
6.2.1 Política de uso de dispositivos para movilidad	Microsoft Word	-	-	-
7.2.2 Concienciación, educación y capacitación en segur. de la informac	Cursos de instituciones como INCIBE	-	-	-
7.2.3 Proceso disciplinario	Microsoft Word	-	-	-
8.1.1 Inventario de activos	Microsoft Word	-	-	-
8.1.3 Uso aceptable de los activos	Microsoft Word	-	-	-
8.2.1 Directrices de clasificación	Microsoft Word	-	-	-
8.2.2 Etiquetado y manipulado de la información	Microsoft Word	-	-	-
8.2.3 Manipulación de activos	Microsoft Word	-	-	-
8.3.1 Gestión de soportes extraíbles	Microsoft Word	-	-	-
9.1.1 Política de control de accesos	Microsoft Word	-	-	-
9.1.2 Control de acceso a las redes y servicios asociados	Firewall de Windows	-	-	-

9.2.2 Gestión de los derechos de acceso asignados a usuarios	Microsoft Word	-	-	-
9.2.3 Gestión de los derechos de acceso con privilegios especiales	Políticas de grupo de Windows	-	-	-
9.2.5 Revisión de derechos de acceso de usuarios	Microsoft Word	-	-	-
9.4.1 Restricción del acceso a la información	Políticas de grupo de Windows	-	-	-
9.4.2 Procedimientos seguros de inicio de sesión	Cuentas de usuario de Windows	-	-	-
9.4.3 Gestión de contraseñas de usuario	Cuentas de usuario de Windows	-	-	-
9.4.4 Uso de herramientas de administración de sistemas	Políticas de grupo de Windows	-	-	-
10.1.1 Política de uso de los controles criptográficos	Cifrado de Windows	-	-	-
11.1.1 Perímetro de seguridad física	Cerraduras	25,000	3	75,000
11.1.2 Controles físicos de entrada	Elaboración de gafetes de identificación	2,000	4	8,000
11.1.3 Seguridad de oficinas, despachos y recursos	Microsoft Word	-	-	-
11.1.4 Protección contra las amenazas externas y ambientales	Extintor	27,000	1	27,000
11.2.1 Emplazamiento y protección de equipos	Vigilancia	300,000	1	300,000
11.2.2 Instalaciones de suministro	UPS	30,000	1	30,000
11.2.3 Seguridad del cableado	Fibra Óptica	20,000	1	20,000
11.2.4 Mantenimiento de los equipos	Windows Update	-	-	-
11.2.5 Salida de activos fuera de las dependencias de la empresa	Microsoft Word	-	-	-
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	TunnelBear	-	-	-
11.2.8 Equipos de usuario desatendidos	Bloqueo de Windows	-	-	-
11.2.9 Política de escritorio y pantalla limpios	Opciones de energía de Windows	-	-	-
12.1.1 Documentación de procedimientos de operación	Microsoft Word	-	-	-
12.1.3 Gestión de capacidades	Administrador de tareas de Windows	-	-	-
12.5.1 Instalación del software en sistemas en producción	AVAST Antivirus	40,000	1	40,000
12.6.1 Gestión de las vulnerabilidades técnicas.	Microsoft Baseline Security Analyzer (MBSA)	-	-	-

12.6.2 Restricciones en la instalación de software	Microsoft Windows Installer	-	-	-
13.1.1 Controles de redes	Ajustes del router	-	-	-
13.1.2 Mecanismos de seguridad asociados a servicios en red	Microsoft Word	-	-	-
13.2.3 Mensajería electrónica	ProtonMail	-	-	-
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	Microsoft Word	-	-	-
15.2.1 Supervisión y revisión de los servicios prestados por terceros	Microsoft Word	-	-	-
				500,000

La Tabla 9 muestra los controles aplicados por activo y sus amenazas.

TABLA 9: TABLA CONTROLES

CÓDIGO	ACTIVO	AMENAZA	TOTAL CUALITATIVO	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	CONTROL
D01	Datos	[E.19] Fugas de información	Medio	Mitigar el riesgo	7.2.2 Concienciación, educación y capacitación en segur. de la informac 8.3.1 Gestión de soportes extraíbles 11.2.8 Equipos de usuario desatendidos 11.2.9 Política de escritorio limpio y pantalla limpia
		[A.18] Destrucción de información	Medio	Mitigar el riesgo	8.1.1 Inventario de activos 8.2.1 Directrices de clasificación 8.2.2 Etiquetado y manipulado de la información

					8.2.3 Manipulación de activos 9.2.5 Revisión de derechos de acceso de usuarios
		[A.15] Modificación deliberada de la información	Medio	Mitigar el riesgo	8.1.1 Inventario de activos 8.2.1 Directrices de clasificación 8.2.2 Etiquetado y manipulado de la información 8.2.3 Manipulación de activos 9.1.2 Control de acceso a las redes y servicios asociados 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios
		[E.15] Alteración accidental de la información	Alto	Mitigar el riesgo	9.1.2 Control de acceso a las redes y servicios asociados 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo	7.2.2 Concienciación,

					educación y capacitación en segur. de la informac 12.1.1 Documentación de procedimientos de operación
P01	Personal	[A.28] Indisponibilidad del personal	Medio	Mitigar el riesgo	6.1.2 Segregación de tareas 7.2.2 Concienciación, educación y capacitación en segur. de la informac 7.2.3 Proceso disciplinario
		[A.30] Ingeniería social (picaresca)	Medio	Mitigar el riesgo	7.2.2 Concienciación, educación y capacitación en segur. de la informac
		[E.7] Deficiencias en la organización	Alto	Mitigar el riesgo	6.1.1 Asignación de responsabilidades para la segur. de la información 6.1.2 Segregación de tareas
		[E.28] Indisponibilidad del personal	Medio	Mitigar el riesgo	6.1.2 Segregación de tareas 7.2.2 Concienciación, educación y capacitación en segur. de la informac 7.2.3 Proceso disciplinario
S01	Correo Electrónico	[A.11] Acceso no autorizado	Medio	Mitigar el riesgo	9.1.1 Política de control de accesos 9.2.2 Gestión de

					<p>los derechos de acceso asignados a usuarios</p> <p>9.2.3 Gestión de los derechos de acceso con privilegios especiales</p> <p>9.2.5 Revisión de los derechos de acceso de los usuarios</p> <p>9.4.2 Procedimientos seguros de inicio de sesión</p> <p>9.4.3 Gestión de contraseñas de usuario</p>
		[E.1] Errores de los usuarios	Medio	Mitigar el riesgo	<p>7.2.2 Concienciación, educación y capacitación en segur. de la informac</p> <p>12.1.1 Documentación de procedimientos de operación</p>
		[E.19] Fugas de información	Alto	Mitigar el riesgo	<p>7.2.2 Concienciación, educación y capacitación en segur. de la informac</p> <p>8.3.1 Gestión de soportes extraíbles</p> <p>11.2.8 Equipos de usuario desatendidos</p> <p>11.2.9 Política de escritorio y pantalla limpios</p> <p>13.2.3 Mensajería electrónica</p>

S02	Servicios en la nube	[A.11] Acceso no autorizado	Medio	Mitigar el riesgo	<p>9.1.1 Política de control de accesos</p> <p>9.2.2 Gestión de los derechos de acceso asignados a usuarios</p> <p>9.2.3 Gestión de los derechos de acceso con privilegios especiales</p> <p>9.2.5 Revisión de los derechos de acceso de los usuarios</p> <p>9.4.2 Procedimientos seguros de inicio de sesión</p> <p>9.4.3 Gestión de contraseñas de usuario</p>
		[A.15] Modificación deliberada de la información	Bajo	Aceptar el riesgo	<p>8.1.1 Inventario de activos</p> <p>8.2.1 Directrices de clasificación</p> <p>8.2.2 Etiquetado y manipulado de la información</p> <p>8.2.3 Manipulación de activos</p> <p>9.1.2 Control de acceso a las redes y servicios asociados</p> <p>9.2.3 Gestión de los derechos de acceso con privilegios especiales</p> <p>9.2.5 Revisión de los derechos de acceso de los usuarios</p>

		[A.24] Denegación de servicio	Medio	Mitigar el riesgo	11.2.1 Emplazamiento y protección de equipos
		[E.18] Destrucción de información	Alto	Mitigar el riesgo	9.1.2 Control de acceso a las redes y servicios asociados 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo	7.2.2 Concienciación, educación y capacitación en segur. de la informac 12.1.1 Documentación de procedimientos de operación
COM01	Recursos de conectividad	[A.14] Interceptación de información (escucha)	Medio	Mitigar el riesgo	11.2.3 Seguridad del cableado
		[A.24] Denegación de servicio	Medio	Mitigar el riesgo	11.2.1 Emplazamiento y protección de equipos
		[E.24] Caída del sistema por agotamiento de recursos	Alto	Mitigar el riesgo	12.1.3 Gestión de capacidades
		[A.5] Suplantación de la identidad del usuario	Medio	Mitigar el riesgo	9.4.3 Gestión de contraseñas de usuario

		[A.6] Abuso de privilegios de acceso	Medio	Mitigar el riesgo	<p>9.1.1 Política de control de accesos</p> <p>9.2.2 Gestión de los derechos de acceso asignados a usuarios</p> <p>9.2.3 Gestión de los derechos de acceso con privilegios especiales</p> <p>9.2.5 Revisión de los derechos de acceso de los usuarios</p> <p>9.4.3 Gestión de contraseñas de usuario</p>
		[A.7] Uso no previsto	Medio	Mitigar el riesgo	<p>6.2.1 Política de uso de dispositivos para movilidad</p> <p>8.1.3 Uso aceptable de los activos</p>
		[I.8] Fallo de servicios de comunicaciones	Medio	Mitigar el riesgo	<p>13.1.2 Mecanismos de seguridad asociados a servicios en red</p> <p>15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones</p> <p>15.2.1 Supervisión y revisión de los servicios prestados por terceros</p>
		[A.12] Análisis de tráfico	Medio	Mitigar el riesgo	<p>10.1.1 Política de uso de los controles criptográficos</p>

					11.2.3 Seguridad del cableado
HW01	Estaciones de trabajo	[I.6] Corte del suministro eléctrico	Alto	Mitigar el riesgo	11.2.2 Instalaciones de suministro
		[A.25] Robo	Bajo	Aceptar el riesgo	11.1.1 Perímetro de seguridad física 11.1.2 Controles físicos de entrada 11.1.3 Seguridad de oficinas, despachos y recursos 11.2.1 Emplazamiento y protección de equipos
		[A.11] Acceso no autorizado	Medio	Mitigar el riesgo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de contraseñas de usuario
		[I.7] Condiciones inadecuadas de	Bajo	Aceptar el riesgo	11.1.4 Protección contra las amenazas externas y ambientales

		temperatura o humedad			11.2.1 Emplazamiento y protección de equipos 11.2.4 Mantenimiento de los equipos
		[I.5] Avería de origen físico o lógico	Medio	Mitigar el riesgo	8.1.1 Inventario de activos 11.2.4 Mantenimiento de los equipos
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Medio	Mitigar el riesgo	11.2.4 Mantenimiento de los equipos
		[E.25] Pérdida de equipos	Bajo	Aceptar el riesgo	11.2.1 Emplazamiento y protección de equipos 11.2.5 Salida de activos fuera de las dependencias de la empresa 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones
HW02	Teléfonos o dispositivos móviles	[A.11] Acceso no autorizado	Medio	Mitigar el riesgo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los

					usuarios 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de contraseñas de usuario
		[E.25] Pérdida de equipos	Medio	Aceptar el riesgo	11.2.1 Emplazamiento y protección de equipos 11.2.5 Salida de activos fuera de las dependencias de la empresa 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones
		[I.5] Avería de origen físico o lógico	Alto	Mitigar el riesgo	8.1.1 Inventario de activos 11.2.4 Mantenimiento de los equipos
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Medio	Mitigar el riesgo	11.2.4 Mantenimiento de los equipos
		[A.25] Robo	Bajo	Aceptar el riesgo	11.1.1 Perímetro de seguridad física 11.1.2 Controles físicos de entrada 11.1.3 Seguridad de oficinas, despachos y recursos 11.2.1 Emplazamiento y protección de equipos

HW03	Dispositivos periféricos	[I.6] Corte del suministro eléctrico	Medio	Mitigar el riesgo	11.2.2 Instalaciones de suministro
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Medio	Mitigar el riesgo	11.2.4 Mantenimiento de los equipos
		[E.25] Pérdida de equipos	Medio	Mitigar el riesgo	11.2.1 Emplazamiento y protección de equipos 11.2.5 Salida de activos fuera de las dependencias de la empresa 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones
		[A.25] Robo	Medio	Mitigar el riesgo	11.1.1 Perímetro de seguridad física 11.1.2 Controles físicos de entrada 11.1.3 Seguridad de oficinas, despachos y recursos 11.2.1 Emplazamiento y protección de equipos
		[I.5] Avería de origen físico o lógico	Medio	Mitigar el riesgo	8.1.1 Inventario de activos 11.2.4 Mantenimiento de los equipos
SW01	Servicio web	[A.15] Modificación deliberada de la información	Medio	Mitigar el riesgo	8.1.1 Inventario de activos 8.2.1 Directrices de clasificación 8.2.2 Etiquetado y manipulado de la

					<p>información</p> <p>8.2.3 Manipulación de activos</p> <p>9.1.2 Control de acceso a las redes y servicios asociados</p> <p>9.2.3 Gestión de los derechos de acceso con privilegios especiales</p> <p>9.2.5 Revisión de los derechos de acceso de los usuarios</p>
		[A.11] Acceso no autorizado	Alto	Mitigar el riesgo	<p>9.1.1 Política de control de accesos</p> <p>9.2.2 Gestión de los derechos de acceso asignados a usuarios</p> <p>9.2.3 Gestión de los derechos de acceso con privilegios especiales</p> <p>9.2.5 Revisión de los derechos de acceso de los usuarios</p> <p>9.4.2 Procedimientos seguros de inicio de sesión</p> <p>9.4.3 Gestión de contraseñas de usuario</p>
		[E.20] Vulnerabilidades de los programas (software)	Alto	Mitigar el riesgo	12.6.1 Gestión de las vulnerabilidades técnicas.

		[E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Mitigar el riesgo	11.2.4 Mantenimiento de los equipos
		[A.5] Suplantación de la identidad del usuario	Medio	Mitigar el riesgo	9.4.3 Gestión de contraseñas de usuario
		[A.6] Abuso de privilegios de acceso	Alto	Mitigar el riesgo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios 9.4.3 Gestión de contraseñas de usuario
		[A.7] Uso no previsto	Medio	Mitigar el riesgo	6.2.1 Política de uso de dispositivos para movilidad 8.1.3 Uso aceptable de los activos
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo	7.2.2 Concienciación, educación y capacitación en segur. de la informac 12.1.1 Documentación

					de procedimientos de operación
		[E.8] Difusión de software dañino	Alto	Mitigar el riesgo	12.5.1 Instalación del software en sistemas en producción 12.6.2 Restricciones en la instalación de software
SW02	Redes Sociales	[E.20] Vulnerabilidades de los programas (software)	Medio	Mitigar el riesgo	12.6.1 Gestión de las vulnerabilidades técnicas.
		[E.21] Errores de mantenimiento / actualización de programas (software)	Bajo	Aceptar el riesgo	11.2.4 Mantenimiento de los equipos
		[A.5] Suplantación de la identidad del usuario	Medio	Mitigar el riesgo	9.4.3 Gestión de contraseñas de usuario
		[A.6] Abuso de privilegios de acceso	Medio	Mitigar el riesgo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios 9.4.3 Gestión de contraseñas de usuario

		[A.7] Uso no previsto	Medio	Mitigar el riesgo	6.2.1 Política de uso de dispositivos para movilidad 8.1.3 Uso aceptable de los activos
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo	7.2.2 Concienciación, educación y capacitación en segur. de la informac 12.1.1 Documentación de procedimientos de operación
		[E.8] Difusión de software dañino	Medio	Mitigar el riesgo	12.5.1 Instalación del software en sistemas en producción 12.6.2 Restricciones en la instalación de software
		[A.11] Acceso no autorizado	Medio	Mitigar el riesgo	9.4.1 Restricción del acceso a la información 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de contraseñas de usuario 9.4.4 Uso de herramientas de administración de sistemas
SW03	Sistemas o aplicaciones	[E.8] Difusión de software dañino	Alto	Mitigar el riesgo	12.5.1 Instalación del software en sistemas en producción 12.6.2 Restricciones en

				la instalación de software
		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo 7.2.2 Concienciación, educación y capacitación en segur. de la informac 12.1.1 Documentación de procedimientos de operación
		[E.20] Vulnerabilidades de los programas (software)	Medio	Mitigar el riesgo 12.6.1 Gestión de las vulnerabilidades técnicas.
		[A.5] Suplantación de la identidad del usuario	Alto	Mitigar el riesgo 9.4.3 Gestión de contraseñas de usuario
		[A.6] Abuso de privilegios de acceso	Alto	Mitigar el riesgo 9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios 9.4.3 Gestión de contraseñas de usuario
		[A.7] Uso no previsto	Bajo	Aceptar el riesgo 6.2.1 Política de uso de dispositivos para movilidad 8.1.3 Uso

					aceptable de los activos
		[E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Mitigar el riesgo	11.2.4 Mantenimiento de los equipos
SW04	Sistema Operativo	[E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Mitigar el riesgo	11.2.4 Mantenimiento de los equipos
		[A.5] Suplantación de la identidad del usuario	Bajo	Aceptar el riesgo	9.4.3 Gestión de contraseñas de usuario
		[A.6] Abuso de privilegios de acceso	Alto	Mitigar el riesgo	9.1.1 Política de control de accesos 9.2.2 Gestión de los derechos de acceso asignados a usuarios 9.2.3 Gestión de los derechos de acceso con privilegios especiales 9.2.5 Revisión de los derechos de acceso de los usuarios 9.4.3 Gestión de contraseñas de usuario
		[A.7] Uso no previsto	Bajo	Aceptar el riesgo	6.2.1 Política de uso de dispositivos para movilidad 8.1.3 Uso aceptable de los activos

		[E.1] Errores de los usuarios	Alto	Mitigar el riesgo	7.2.2 Concienciación, educación y capacitación en segur. de la informac 12.1.1 Documentación de procedimientos de operación
		[E.8] Difusión de software dañino	Alto	Mitigar el riesgo	12.5.1 Instalación del software en sistemas en producción 12.6.2 Restricciones en la instalación de software

Fuente: Elaboración propia.

CAPÍTULO VI: CONCLUSIONES

- Detallar los elementos que componen el concepto de seguridad de la información en las organizaciones.

Existen gran cantidad de conceptos de seguridad de la información que las empresas no tienen conocimiento de que existen y que son de suma importancia para el desarrollo y continuidad de estas. En muchos casos, las empresas afirman que la seguridad de la información es un tema muy importante, sin embargo, la mayoría no tienen la mas mínima idea lo que eso conlleva y la mayoría no cuenta con las medidas necesarias para evitar situaciones de riesgo tecnológico que puedan comprometer sus activos, operación, etc.

- Analizar los riesgos de seguridad de la información que presentan las PYMES.

Se puede concluir que la gran mayoría de PYMES del país están expuestas a un sin número de riesgos tecnológicos que de llegar a materializarse podrían llegar a impactar sus activos, procesos críticos y el cumplimiento de los objetivos estratégicos, de allí radica la importancia de la implementación del concepto de seguridad de la información en este tipo de organizaciones.

El análisis de riesgos de seguridad de la información para las PYMES permitió evidenciar cuales son algunas de las debilidades y deficiencias existentes en la infraestructura tecnológica, haciendo evidente la necesidad de implementar un plan de tratamiento de riesgos que permita disminuir los riesgos a los cuales está expuesta la información de la organización.

- Identificar las barreras organizacionales para la gestión de la seguridad de la información.

Como resultado del análisis de barreras realizado durante la investigación, se concluye que existen un sinnúmero de causas por las que muchas empresas en la actualidad

no toman en cuenta temas tan vitales como seguridad de la información en sus organizaciones, en mi opinión, considero que las de mayor peso son primero el desconocimiento, ya que si no se tiene idea de que algo existe es imposible implementarlo, por esto es de suma importancia que los funcionarios de una organización se mantengan informados con las últimas noticias, etc. Otro de los factores que sin duda pesa es la falta de presupuesto, así como, la falta de personal, sin embargo, como se puede ver en la guía de controles propuesta, existen una gran cantidad y variedad de medidas que se pueden implementar en dichas empresas sin necesidad de incurrir en gastos económicos extras y además, son medidas que cualquier persona puede implementar siguiendo los pasos.

- Diseñar una guía de controles para la gestión de la seguridad de la información.

Se ha comprobado que las PYMES tienen características y necesidades distintas a las de una empresa grande, no solo en cuanto a los recursos financieros, de personal y de conocimiento, sino también con respecto a los tipos de activo de información con los que cuentan, la criticidad de determinados activos, entre otros factores.

Con el presente trabajo se ha buscado brindar a las micro, pequeñas y medianas empresas (PYMES) una manera de fortalecer su seguridad de una forma integral, efectiva y práctica, a través de una guía de controles de ciberseguridad, teniendo en cuenta que las PYMES representan un sector fundamental de la economía, que se encuentra expuesto a ciberataques muy diversos y que, muchas veces, no cuentan con los recursos necesarios para protegerse adecuadamente.

Ficha de Proceso			
Asignación de responsabilidades para la seguridad de la información			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Definir y asignar todas las responsabilidades de cada puesto en la organización			
Entradas del Proceso		Salidas del Proceso	
Lista de puestos de la organización		Asignación de funciones según cada puesto	
Definición de roles para cada puesto			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Obtener la lista de puestos dentro de la organización	Jefatura	
Actividad #2	Obtener la definición de roles para cada puesto	Jefatura	
Actividad #3	Asignar las funciones según cada puesto	Jefatura	
Actividad #4	Documentar	Jefatura	

Ficha de Proceso			
Segregación de tareas			
Dependencias de otros procedimientos: Asignación de responsabilidades para la seguridad de la información			
Responsable: Jefatura			
Objetivo(s) del proceso: Segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés			
Entradas del Proceso		Salidas del Proceso	
Lista de puestos de la organización		Segregación de tareas	
Definición de roles para cada puesto			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Obtener la lista de puestos dentro de la organización	Jefatura	
Actividad #2	Obtener la definición de roles para cada puesto	Jefatura	
Actividad #3	Asignar las funciones según cada puesto	Jefatura	
Actividad #4	Documentar	Jefatura	

Ficha de Proceso			
Política para dispositivos móviles			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Establecer una política formal para el correcto uso de los recursos de informática móvil y las telecomunicaciones			
Entradas del Proceso		Salidas del Proceso	
Dispositivos Móviles		Política para dispositivos móviles	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los requerimientos para el uso adecuado de dispositivos móviles	Jefatura	

Actividad #2	Documentar dichos requerimientos	Jefatura	
Actividad #3	Implementar los requerimientos	Jefatura	

Ficha de Proceso			
Toma de conciencia, educación y formación en la seguridad de la información			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Brindar entrenamiento apropiado a todos los funcionarios			
Entradas del Proceso		Salidas del Proceso	
Funcionarios		Funcionarios formados y concientes	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar opciones de mejora en la formación de los funcionarios	Jefatura	
Actividad #2	Explicar temas de conocimiento importantes	Jefatura	
Actividad #3	Realizar capacitaciones	Jefatura	

Ficha de Proceso			
Proceso disciplinario			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Definir un proceso formal disciplinario y comunicado a todos los empleados			
Entradas del Proceso		Salidas del Proceso	
Políticas		Proceso disciplinario	
Faltas			
Acciones Disciplinarias			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar las políticas	Jefatura	
Actividad #2	Identificar las faltas	Jefatura	
Actividad #3	Identificar las acciones disciplinarias según la falta	Jefatura	
Actividad #4	Documentar	Jefatura	

Ficha de Proceso			
Inventario de activos			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Identificar, confeccionar y mantener un inventario de todos los activos			
Entradas del Proceso		Salidas del Proceso	
Activos		Inventario de activos	

Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los activos de la empresa	Jefatura	
Actividad #2	Ingresar los datos en un inventario	Jefatura	
Actividad #3	Actualizar dicho inventario	Jefatura	

Ficha de Proceso Uso aceptable de los activos

Dependencias de otros procedimientos: No

Responsable: Jefatura

Objetivo(s) del proceso: Identificar, documentar e implantar regulaciones para el uso adecuado de los activos

Entradas del Proceso

Requerimientos

Activos

Salidas del Proceso

Uso adecuado de los activos

Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los requerimientos para el uso adecuado de los activos	Jefatura	
Actividad #2	Documentar dichos requerimientos	Jefatura	
Actividad #3	Implementar los requerimientos	Jefatura	

Ficha de Proceso Clasificación de la información

Dependencias de otros procedimientos: No

Responsable: Jefatura

Objetivo(s) del proceso: Clasificar los activos en relación con su valor, requisitos legales, sensibilidad y criticidad para la organización

Entradas del Proceso

Activos

Salidas del Proceso

Información clasificada de manera adecuada

Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los activos	Jefatura	
Actividad #2	Clasificar los activos según valor, requisitos legales, sensibilidad y criticidad	Jefatura	
Actividad #3	Documentar la clasificación	Jefatura	

Ficha de Proceso Etiquetado y manipulado de la información

Dependencias de otros procedimientos: No

Responsable: Jefatura

Objetivo(s) del proceso: Desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información

Entradas del Proceso

Salidas del Proceso

Requerimientos		Etiquetado y manipulado de la información adecuado	
Información			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los requerimientos para el etiquetado y tratamiento de la información	Jefatura	
Actividad #2	Documentar dichos requerimientos	Jefatura	
Actividad #3	Implementar los requerimientos	Jefatura	

Ficha de Proceso Manejo de activos

Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Desarrollar e implantar procedimientos para la manipulación de los activos según la clasificación de la información			
Entradas del Proceso		Salidas del Proceso	
Requerimientos		Manejo adecuado de activos	
Activos			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los requerimientos para la manipulación de los activos	Jefatura	
Actividad #2	Documentar dichos requerimientos	Jefatura	
Actividad #3	Implementar los requerimientos	Jefatura	

Ficha de Proceso Gestión de medios removibles

Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Establecer procedimientos para la gestión de los medios removibles según la clasificación de la información			
Entradas del Proceso		Salidas del Proceso	
Requerimientos		Manejo adecuado de medios removibles	
Medios Removibles			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los requerimientos para la gestión de medio removibles	Jefatura	
Actividad #2	Documentar dichos requerimientos	Jefatura	
Actividad #3	Implementar los requerimientos	Jefatura	

Ficha de Proceso

Política de control de acceso

Dependencias de otros procedimientos: No

Responsable: Jefatura

Objetivo(s) del proceso: Establecer, documentar y revisar una política de control de accesos

Entradas del Proceso

Requerimientos
Accesos

Salidas del Proceso

Política de control de acceso

Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los requerimientos para el control de acceso	Jefatura	
Actividad #2	Documentar dichos requerimientos	Jefatura	
Actividad #3	Revisar los requerimientos constantemente	Jefatura	

Ficha de Proceso

Acceso a redes y a servicios en red

Dependencias de otros procedimientos: No

Responsable: Jefatura

Objetivo(s) del proceso: Proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar

Entradas del Proceso

Firewall

Salidas del Proceso

Uso adecuado de acceso a redes y servicios de red

Actividad	Descripción	Responsable	Comentarios
Actividad #1	Bloquear accesos por medio del Firewall de Windows	Jefatura	

Ficha de Proceso

Gestión de los derechos de acceso asignados a usuarios

Dependencias de otros procedimientos: No

Responsable: Jefatura

Objetivo(s) del proceso: Implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuario

Entradas del Proceso

Accesos
Usuarios

Salidas del Proceso

Uso adecuado de derechos de acceso

Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar regulaciones para la asignación de accesos a los usuarios	Jefatura	
Actividad #2	Documentar dichas regulaciones	Jefatura	
Actividad #3	Implementar las regulaciones	Jefatura	

Ficha de Proceso			
Gestión de los derechos de acceso con privilegios especiales			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Restringir y controlar la asignación y uso de derechos de acceso con privilegios especiales			
Entradas del Proceso		Salidas del Proceso	
Usuarios		Uso adecuado de accesos con privilegios	
Accesos			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Definir los permisos de acceso para cada usuario	Jefatura	
Actividad #2	Implementar dichos permisos	Jefatura	

Ficha de Proceso			
Revisión de los derechos de acceso de usuarios			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Revisar de manera periódica que los accesos que tienen los activos sean los correctos			
Entradas del Proceso		Salidas del Proceso	
Activos		Revisión de accesos	
Accesos			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Revisar periódicamente los accesos de cada activo	Jefatura	

Ficha de Proceso			
Restricción del acceso a la información			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Restringir el acceso de los usuarios y funciones de los sistemas de aplicaciones, en relación con la política de control de accesos			
Entradas del Proceso		Salidas del Proceso	
Usuarios		Restricción de acceso	
Accesos			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Definir los permisos de acceso para cada usuario	Jefatura	
Actividad #2	Implementar dichos permisos	Jefatura	

Ficha de Proceso			
Procedimiento de ingreso seguro			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on			
Entradas del Proceso		Salidas del Proceso	
Computadora		Ingresos seguros	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Habilitar ingresos por medio de usuario y contraseña para cada usuario	Jefatura	

Ficha de Proceso			
Gestión de contraseñas de usuario			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Los sistemas de gestión de contraseñas deben ser interactivos y asegurar contraseñas de calidad			
Entradas del Proceso		Salidas del Proceso	
Regulaciones		Contraseñas de calidad	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar requisitos de gestión de contraseñas de usuario	Jefatura	
Actividad #2	Documentar dichos requisitos	Jefatura	
Actividad #3	Implementar los requisitos	Jefatura	

Ficha de Proceso			
Uso de herramientas de administración de sistemas			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Restringir y controlar el uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas			
Entradas del Proceso		Salidas del Proceso	
Computadora		Bloqueo de uso de herramientas de administración de sistemas	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Crear políticas de grupo de Windows	Jefatura	

Ficha de Proceso			
Política de uso de los controles criptográficos			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información			

Entradas del Proceso		Salidas del Proceso	
Computadora		Información cifrada	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Habilitar cifrado de datos en las computadoras	Jefatura	

Ficha de Proceso			
Perímetro de seguridad física			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica			
Entradas del Proceso		Salidas del Proceso	
Infraestructura		Áreas seguras	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar perímetros de seguridad para la protección de áreas	Jefatura	
Actividad #2	Implementar dichos perímetros	Jefatura	

Ficha de Proceso			
Controles físicos de entrada			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Proteger las áreas seguras mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso			
Entradas del Proceso		Salidas del Proceso	
Infraestructura		Controles físicos de entrada	
Equipo			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar controles de entrada adecuados para el control de acceso.	Jefatura	
Actividad #2	Documentar dichos controles	Jefatura	
Actividad #3	Aplicar los controles	Jefatura	

Ficha de Proceso			
Seguridad de oficinas, despachos y recursos			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización			
Entradas del Proceso		Salidas del Proceso	
Regulaciones		Seguridad en oficinas, despachos y recursos	

Infraestructura			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar regulaciones de seguridad física a las oficinas, salas e instalaciones de la organización	Jefatura	
Actividad #2	Documentar dichas regulaciones	Jefatura	
Actividad #3	Aplicar las regulaciones	Jefatura	

Ficha de Proceso Protección contra amenazas externas y ambientales			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes			
Entradas del Proceso		Salidas del Proceso	
Medidas de protección		Protección contra amenazas externas y ambientales	
Infraestructura			
Equipos			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar medidas de protección física contra desastres naturales, ataques maliciosos o accidentes	Jefatura	
Actividad #2	Documentar dichas medidas	Jefatura	
Actividad #3	Aplicar las medidas	Jefatura	

Ficha de Proceso Ubicación y protección de los equipos			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Aplicar protección física a los equipos			
Entradas del Proceso		Salidas del Proceso	
Infraestructura		Infraestructura segura	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Implementar servicio de vigilancia	Jefatura	
Actividad #2	Establecer perímetros de seguridad física	Jefatura	

Ficha de Proceso Servicios de suministro			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Proteger los equipos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo			

Entradas del Proceso		Salidas del Proceso	
Equipos		Equipos protegidos contra cortes de suministros	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar equipos críticos	Jefatura	
Actividad #2	Instalar sistemas de alimentación ininterrumpida (SAI)	Jefatura	

Ficha de Proceso			
Seguridad del cableado			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Proteger los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información contra la interceptación, interferencia o posibles daños			
Entradas del Proceso		Salidas del Proceso	
Conexiones		Cableado seguro	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Solicitar fibra óptica al proveedor de servicios	Jefatura	
Actividad #2	Verificar conexiones adecuadas para la energía eléctrica y la red de datos	Jefatura	

Ficha de Proceso			
Mantenimiento de equipos			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Mantener los equipos actualizados			
Entradas del Proceso		Salidas del Proceso	
Computadora		Equipos actualizados	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Utilizar Windows Update para aplicar actualizaciones automáticas	Jefatura	

Ficha de Proceso			
Salida de activos fuera de las dependencias de la empresa			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: No retirar activos del sitio sin previa autorización			
Entradas del Proceso		Salidas del Proceso	
Regulaciones		Protección de equipos fuera de la empresa	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar las regulaciones para protección de activos fuera de la empresa	Jefatura	
Actividad #2	Documentar dichas regulaciones	Jefatura	

Ficha de Proceso			
Seguridad de los equipos y activos fuera de las instalaciones			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización			
Entradas del Proceso		Salidas del Proceso	
Computadora		Servicio VPN activo	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Descargar la aplicación gratuita TunnelBear	Jefatura	
Actividad #2	Crear una cuenta gratuita	Jefatura	
Actividad #3	Dar permisos a la aplicación	Jefatura	
Actividad #4	Activar o desactivar el servidor VPN	Jefatura	

Ficha de Proceso			
Equipos de usuario desatendidos			
Dependencias de otros procedimientos: No			
Responsable: Cada usuario			
Objetivo(s) del proceso: Asegurar que los equipos que no se estén utilizando cuenten con la protección adecuada			
Entradas del Proceso		Salidas del Proceso	
Computadora		Equipos protegidos	
Regulaciones			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Bloquear sesiones cuando no se esté ocupando el dispositivo	Cada usuario	
Actividad #2	Cerrar sesión al finalizar la jornada	Cada usuario	

Ficha de Proceso			
Política de escritorio y pantalla limpios			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones			
Entradas del Proceso		Salidas del Proceso	
Regulaciones		Política de escritorio y pantalla limpios	

Computadora			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Documentar las regulaciones pertinentes	Jefatura	
Actividad #2	Configurar protectores de pantalla en todas las computadoras	Jefatura	

Ficha de Proceso			
Procedimientos de operación documentados			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten			
Entradas del Proceso		Salidas del Proceso	
Procedimientos de operación		Documentación de todos los procesos operativos	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los procedimientos operativos de la empresa	Jefatura	
Actividad #2	Documentar dichos procedimientos	Jefatura	
Actividad #3	Habilitar la documentación a todos los usuarios para que los puedan acceder	Jefatura	

Ficha de Proceso			
Gestión de capacidad			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Monitorear y ajustar el uso de los recursos			
Entradas del Proceso		Salidas del Proceso	
Computadora		Monitoreo de recursos	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Monitorear los recursos por medio del Administrador de tareas de Windows	Jefatura	

Ficha de Proceso			
Controles contra códigos maliciosos			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Implementar controles para la detección, prevención y recuperación ante afectaciones de malware			
Entradas del Proceso		Salidas del Proceso	
Computadora		Antivirus activo en los computadores	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Descargar el programa gratuito Avast Antivirus	Jefatura	
Actividad #2	Instalar el programa	Jefatura	

Ficha de Proceso			
Gestión de las vulnerabilidades técnicas			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Obtener información sobre las vulnerabilidades técnicas de los sistemas de información			
Entradas del Proceso		Salidas del Proceso	
Computadora		Escaneo de vulnerabilidades	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Configurar Microsoft Baseline Security Analyzer (MBSA) para analizar vulnerabilidades	Jefatura	

Ficha de Proceso			
Restricciones en la instalación de software			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios			
Entradas del Proceso		Salidas del Proceso	
Computadora		Restricción para instalar software	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Configurar la computadora para que no permita la instalación de software	Jefatura	

Ficha de Proceso			
Controles de redes			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Administrar y controlar las redes para proteger la información en sistemas y aplicaciones			
Entradas del Proceso		Salidas del Proceso	
Router		Router configurado	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Cambiar el nombre de la red (SSID)	Jefatura	
Actividad #2	Ocultar el nombre de la red (SSID)	Jefatura	
Actividad #3	Asegurarse de que se utiliza el protocolo de seguridad WPA2	Jefatura	
Actividad #4	Modificar las credenciales que vienen configuradas por defecto	Jefatura	

Ficha de Proceso			
Mecanismos de seguridad asociados a servicios en red			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red			
Entradas del Proceso		Salidas del Proceso	
Requisitos		Documentación de requisitos en los acuerdos de servicio	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Identificar los requisitos necesarios para la organización	Jefatura	
Actividad #2	Documentar los requisitos en los acuerdos de servicio	Jefatura	
Actividad #3	Verificar dichos requisitos con las partes interesadas	Jefatura	

Ficha de Proceso			
Mensajería electrónica			
Dependencias de otros procedimientos: No			
Responsable: Cada usuario			
Objetivo(s) del proceso: Proteger adecuadamente la información referida en la mensajería electrónica			
Entradas del Proceso		Salidas del Proceso	
ProtonMail		Correos encriptados	
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Registrarse y seleccionar la cuenta gratuita en ProtonMail	Cada usuario	
Actividad #2	Crear y validar cuenta	Cada usuario	
Actividad #3	Realizar el envío de correos electrónicos por medio de la herramienta	Cada usuario	

Ficha de Proceso			
Cadena de suministro en tecnologías de la información y comunicaciones			
Dependencias de otros procedimientos: No			
Responsable: Jefatura			
Objetivo(s) del proceso: Incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios en los acuerdos con proveedores			
Entradas del Proceso		Salidas del Proceso	
Requisitos		Documentación de requisitos	
Actividad	Descripción	Responsable	Comentarios

Actividad #1	Identificar los requisitos por parte de la organización	Jefatura	
Actividad #2	Documentar dichos requisitos en los acuerdos con los proveedores	Jefatura	
Actividad #3	Verificar los requisitos con los proveedores	Jefatura	

Ficha de Proceso			
Supervisión y revisión de los servicios prestados por terceros			
Dependencias de otros procedimientos: Cadena de suministro en tecnologías de la información y comunicaciones			
Responsable: Jefatura			
Objetivo(s) del proceso: Monitorear, revisar y auditar la presentación de servicios del proveedor regularmente			
Entradas del Proceso		Salidas del Proceso	
Proveedores		Revisión de los servicios dados por proveedores	
Servicios			
Actividad	Descripción	Responsable	Comentarios
Actividad #1	Obtener la lista de proveedores	Jefatura	
Actividad #2	Obtener la lista de servicios	Jefatura	
Actividad #3	Verificar que se cumplan los servicios acordados	Jefatura	
Actividad #4	Documentar los hallazgos	Jefatura	

BIBLIOGRAFÍA

- Center for Internet Security (CIS). CIS Controls Spanish Translation. https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf
- Cervantes, M. Ballesteros, B. y Hernández, F. (2012). Mercado de trabajo para los profesionistas de la Contaduría y la administración: una visión global. <http://www.eumed.net/cursecon/ecolat/mx/2012/vic.html>
- Cisco (2018). SMB Security Service. Disponible en: <https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf>
- Cortés, M. e Iglesias, M. (2004). Generalidades sobre Metodología de la Investigación. <http://www.unacar.mx/contenido/gaceta/ediciones/contenido2.pdf>
- ENISA. National Cyber Security Strategies. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools>
- F. López, M.A. Amutio, J. Candauy J.A. Mañas. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, versión 2. Ministerio de Administraciones Públicas, 2006. <http://publicaciones.administracion.es>
- Instituto Nacional de Estándares y Tecnología (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmillrev_20181102mn_clean.pdf
- International Telecommunication Union (2010). Measuring the Information Society 2010. https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-WTDR-2010-PDF-E.pdf
- ISACA. COBIT 5 español. <http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>
- ISO27000. ES. ISO 27001. <https://www.iso27000.es/iso27000.html>
- ISO27000. ES, Sistema de Gestión de la Seguridad de la Información. <https://www.iso27000.es/sgsi.html>

- M. Dini y G. Stumpo (coords.). "Mi pymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento". Documentos de Proyectos (LC/TS.2018/75), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2018.
- Ministerio de Economía, Industria y Comercio. PYMES Costa Rica. <http://www.pyme.go.cr/cuadro5.php?id=1>
- M. Kuwayama, Y. Ueki y M. Tsuji (eds.) (2005), Information Technology for Development of Small and Medium-sized Exporters in Latin America and East Asia, (LC/W.27), Comisión Económica para América Latina y el Caribe (CEPAL).
- Naresh, M. Investigación de Mercados Un Enfoque Aplicado, Cuarta Edición, Pearson Educación de México, S.A. de C.V., 2004.
- Patiño, L. Ventajas y desventajas de las Pymes. https://www.academia.edu/11802402/Ventajas_y_desventajas_de_las_Pymes
- Remolina, N. (2014). América Latina y la protección de datos personales: hechos y cifras (1985-2014). <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/2014-Latinoamerica-proteccion-datos-en-cifras-1985-2014-Remolina.pdf>
- Universidad de Costa Rica (UCR). Informe De Resultados III Encuesta Nacional De La Micro, Pequeña Y Mediana Empresa En Costa Rica 2018. <http://odd.ucr.ac.cr/sites/default/files/MiPymes/Informe-Tercera-Encuesta-Mipymes-Observaciones-para-divulgar.pdf>

