UNIVERSIDAD
FRANCISCO GAVIDIA
DIRECCIÓN DE POSTGRADOS Y EDUCACIÓN CONTINUA

“PROPUESTA PARA EL ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD EN REDES INFORMÁTICAS, APLICANDO LAS MEJORES PRÁCTICAS, PARA IMPLEMENTAR EN ALCALDÍAS DE EL SALVADOR. CASO DE ESTUDIO: ALCALDÍA DE NUEVO CUSCATLÁN.”

PRESENTADO POR:

Tobar Moreira, Edwin Orlando	TM100612
Julián López, Guillermo Edgardo	JL100412

Julio de 2016

San Salvador, El Salvador, Centro América.

UNIVERSIDAD
FRANCISCO GAVIDIA
DIRECCIÓN DE POSTGRADOS Y EDUCACIÓN CONTINUA

TRABAJO DE GRADUACIÓN PREPARADO PARA
LA DIRECCIÓN DE POSTGRADOS Y EDUCACIÓN CONTINUA
PARA OPTAR AL TÍTULO DE:

MASTER EN INFORMÁTICA APLICADA EN REDES

ASESOR

Ing. Nelson Antonio Tesorero

JURADO EVALUADOR

Ing. Néstor Yubiny Merino
Ing. Edgar Antonio Peñate Melgar
Ing. Carlos Roberto Mejía Enríquez

Julio de 2016

San Salvador, El Salvador, Centro América.

UNIVERSIDAD
FRANCISCO GAVIDIA
DIRECCIÓN DE POSTGRADOS Y EDUCACIÓN CONTINUA

AUTORIDADES

Ing. Mario Antonio Ruiz Ramírez
RECTOR

Dra. Leticia Andino de Rivera
VICERRECTORA

Licda. Teresa de Jesús Gonzales de Mendoza
SECRETARIA GENERAL

Ing. Mario Antonio Ruiz Ramírez
DIRECTOR INTERINO DE POSTGRADOS Y EDUCACIÓN CONTINUA

Julio de 2016

San Salvador, El Salvador, Centro América.

UNIVERSIDAD FRANCISCO GAVIDIA
Tecnología, Innovación y Calidad

ACTA DE DEFENSA DE TRABAJO DE GRADUACIÓN

Acta N° 03/2016

En el aula de estudio número uno del Edificio de Postgrados y Educación Continua, de la Universidad Francisco Gavidia, a las doce horas del día catorce de mayo del dos mil dieciséis; siendo este el día y la hora señalada para el análisis y la defensa del Trabajo de Graduación Titulado: "***Propuesta para el establecimiento de políticas de seguridad en redes informáticas, aplicando las mejores prácticas, para implementar en alcaldías de El Salvador. Caso de estudio: Alcaldía de Nuevo Cuscatlán",*** presentado por los egresados ***Edwin Orlando Tobar Moreira y Guillermo Edgardo Julián López*** de la Maestría en Informática Aplicada en Redes y estando presente los interesados y el jurado, se procedió a dar cumplimiento a lo estipulado, habiendo llegado el Jurado, después del interrogatorio y las deliberaciones correspondientes, a pronunciarse por este fallo:

Edwin Orlando Tobar Moreira fallo: Aprobado

Guillermo Edgardo Julián López fallo: Aprobado

Y no habiendo más que hacer constar, se da por terminada la presente.

Presidente
Ing. Néstor Yubiny Merino

Vocal
Ing. Edgar Antonio Peñate Melgar

Vocal:
Ing. Carlos Roberto Mejia Henriquez

Lic. Mario Antonio Ruiz Aguilar

OBSERVADOR

A mi madre

Angelita

Página dejada en blanco intencionalmente

Tabla de contenido

Tabla de ilustraciones (Gráficas)

Tabla de ilustraciones (Imágenes)

Tabla de ilustraciones (Diagramas)

Tabla de ilustraciones (Tablas)

Resumen

El presente documento ha sido elaborado con el objetivo de realizar propuestas para el establecimiento de políticas de seguridad dentro de la infraestructura de red informática de las alcaldías de El Salvador, siguiendo las mejores prácticas, ello con el objeto de alinear la tecnología con el negocio, mediante la aplicación de aquellas prácticas que han demostrado ser más efectivas, bajo un marco de trabajo destinado a facilitar la entrega de servicios de tecnologías de la información.

Introducción

El presente estudio ha sido elaborado con el objeto de proveer a los Gobiernos Municipales de El Salvador de un documento base que les colabore en el desarrollo de un manual de Políticas de Seguridad de la Información que forme parte de la cultura organizacional de la institución; donde se plasme la hoja de ruta, el plan de acción y los protocolos a seguir para proteger los activos informáticos de la comuna. Este importante instrumento se fundamenta en un marco de trabajo establecido por las mejores prácticas en materia de seguridad informática orientado a minimizar amenazas en entornos de la información.

El estudio se compone de 7 capítulos conformados según se describe a continuación:

Capítulo I, constituido por el Planteamiento del Problema en el cual se trata de justificar y demostrar como la carencia de un instructivo de Políticas de Seguridad Informática en los Gobiernos Municipales de El Salvador puede permitir manipulaciones indeseadas que ponga bajo riesgo la seguridad de la información digital que es transmitida, administrada y almacenada dentro de la infraestructura de red LAN de las alcaldías, cuyos efectos podrían trascender e incluso comprometer y perjudicar la seguridad nacional.

El Capítulo II lo conforma el Marco de Referencia, donde se fundamenta mediante la teoría, los conceptos que serán utilizados a lo largo del trabajo. En él se incluyen los modelos de buenas prácticas ITIL, COBIT, ISO/IEC 27001 e ISO/IEC 27002 y además se incorporan los Antecedentes Tecnológicos Relacionados.

En el Capítulo III se realiza la Formulación de Hipótesis y sus Variables mientras que en los capítulos IV, V y VI se demuestra, mediante los resultados obtenidos en la investigación de campo, la necesidad de desarrollar un manual para el establecimiento de Políticas de Seguridad en Redes Informáticas que forme parte de la cultura organizacional de los Gobiernos Municipales de El Salvador.

El Capítulo VII lo compone la propuesta de Políticas de Seguridad a implementar, las cuales cubren múltiples aspectos de seguridad sugeridos por la ISO/IEC 27002:2013, código base en el cual se fundamenta el presente documento y del cual se ha considerado lo siguiente: Establecimiento del conjunto de políticas a ser aplicadas; Propuesta del andamiaje estructural y organizacional responsable de garantizar el cumplimiento de los planes y procedimientos propuestos, también dicta el procedimiento a seguir durante los procesos de contratación y cesamiento de personal; planteamiento de los controles sobre el inventario de los activos informáticos y clasificación de la información; gestión y manejo de soportes extraíbles, controles de acceso, cifrado, protección de áreas seguras contra amenazas externas y ambientales, protección y mantenimiento de equipos, protección contra códigos maliciosos, copias de seguridad y seguridad en redes.

Objetivos

Objetivo General

Diseñar políticas, aplicando las mejores prácticas, para la implementación de procesos y metodologías de seguridad dentro de la infraestructura de red informática de los Gobiernos Municipales de El Salvador.

Objetivos Específicos

- Categorizar los gobiernos municipales a fin de estructurarlos en grupos comunes.
- Determinar aquellas áreas dentro de los gobiernos municipales que administren información sensible, en las cuales se concentraran los esfuerzos para el resguardo de los datos.
- Facilitar a las alcaldías políticas basadas en buenas prácticas para la mejor administración y seguridad de su red informática.
- Proponer a los gobiernos municipales un conjunto de herramientas de gestión y seguridad que permitan el mantenimiento óptimo de la infraestructura de red informática.

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Situación problemática identificada

Según consideraciones establecidas en el decreto No. 581, emitido por La Asamblea Legislativa de La República de El Salvador el dieciocho de octubre de dos mil uno; donde se enuncia la importancia que el DUI tiene para las personas naturales al describirlo como: "*el documento suficiente para identificarse fehacientemente en todo acto público o privado*" y que además establece en el literal IV "*Que el DUI constituirá un instrumento de trascendental importancia en el contexto de la seguridad nacional, especialmente referida la seguridad ciudadana y la jurídica*". Es posible entonces inferir el carácter sensible que surge con la obtención de tan importante documento. Para legislar la emisión del mismo, se estableció la Ley Especial Reguladora de la emisión del Documento Único de Identidad cuyo principal objetivo según el Artículo 1 es el de *"…establecer las disposiciones regulatorias generales y especiales del sistema de registro y emisión del Documento Único de Identidad, así como las características del proceso de registro de emisión para su obtención…* " en línea con lo anterior el Artículo 2 dicta que: "*El Registro Nacional de las Personas Naturales, es la entidad responsable de la Administración del Sistema de Registro del Documento Único de identidad…*" y del registro, emisión y entrega del mismo. Como dicho documento es de carácter obligatorio según enuncia el artículo 4 "*El DUI será de uso obligatorio en todo el territorio nacional, para todo salvadoreño mayor de edad…*" se establecen entonces las directrices a seguir para la obtención del mismo según se expresa en el Articulo 4-B el cual dice: "*Toda persona que solicite el DUI por primera vez, que solicite su renovación o modificación, deberá cumplir con los requisitos que a continuación se detallan*": inmediatamente después se enlistan una serie de literales de los cuales habrá que enfocarse en el literal (b) que dice:

b) Presentar certificación de la partida de nacimiento, cuya fecha de emisión no podrá exceder de un año al momento de solicitar el documento, cuando sea solicitado por primera vez; en caso de renovación del DUI, únicamente será exigible

la presentación de la certificación de la partida de nacimiento cuando no existiere la misma en el expediente del ciudadano en el Registro Nacional de las Personas Naturales y, en los casos en que el DUI que se renueva esté respaldado por una partida de nacimiento obtenida mediante diligencias de establecimiento de estado civil subsidiario; ….

Y siendo que las alcaldías de El Salvador son las instituciones regidoras que constituyen la Unidad Política Administrativa primaria dentro de la organización estatal bajo cuya responsabilidad recae la emisión de las partidas de nacimiento, primera etapa para la obtención del DUI, es de vital importancia hacer notar la imperiosa necesidad de mantener bajo estricto resguardo el accesos hacia el Registro del Estado Familiar (REF) que es la unidad donde se generan las partidas de nacimiento.

A lo largo de Latinoamérica se pueden encontrar variados casos en los cuales las alcaldías [1][2] o instituciones gubernamentales[3][4][5][6] son objetos de ataques cibernéticos en su infraestructura de red por parte de personan malintencionadas. Ello podría deberse a la ausencia de medidas de seguridad básica debido a factores varios, entre los que se pueden enunciar: falta de recursos; personal con formación técnica inadecuada en seguridad informática; desatención por parte de la organización interna de la unidad TI; apatía de parte de las autoridades sobre el involucramiento en los planes de seguridad (*aspecto más crítico debido a que la ausencia de compromiso por parte de las altas autoridades, en este caso el consejo municipal, imposibilitara cualquier intento de proteger de manera adecuada los activos informáticos, ya que se requiere la participación activa del mismo para: establecer*

---

1 COLOMBIA: Hackers atacaron portal de la Alcaldía de Cali - El Pueblo http://elpueblo.com.co/hackers-atacaron-portal-de-la-alcaldia-de-cali/

2 BOLIVIA: Sistema informático de Alcaldía de El Alto sufre ataque de hackers - FM Bolivia http://www.fmbolivia.com.bo/noticia61881-sistema-informatico-de-alcaldia-de-el-alto-sufre-ataque-de-hackers.html

3 NICARAGUA: Hackers bloquean varias páginas de internet del gobierno de Nicaragua - La Jornada http://www.lajornadanet.com/diario/archivo/2011/septiembre/15/1.php

4 MEXICO: Anonymous lanza un ataque contra las páginas web del Gobierno de México - El MUNDO.es http://www.elmundo.es/america/2011/09/16/mexico/1316137025.html

5 CHILE: Hackers argentinos se atribuyen hackeo a la web del Ministerio chileno - La Segunda online http://www.lasegunda.com/Noticias/Internacional/2013/02/823871/hackers-argentinos-se-atribuyen-hackeo-a-la-web-del-ministerio-del-interior-chileno

6 EL SALVADOR: Gobierno confirma ataque de hackers - Diario El Mundo http://elmundo.com.sv/gobierno-confirma-ataque-de-hackers

compromisos de seguridad; apoyar la creación de políticas; proponer mejoras aplicables a las mismas; garantizar que se cumplan los planes y procedimientos establecidos; colaborar a revisar periódicamente los niveles de seguridad ante avances tecnológicos; financiar dispositivos y proveer los medios para que todo el personal de la comuna conozca, sea capacitado y concientizado sobre la reglamentación establecida y los beneficios esperados al respetar la misma.); etc. Dicha situación puede desembocar en manipulaciones indeseadas de la red, bien sean desde el exterior o desde el interior de esta, lo cual genera riesgo para la buena salud de la misma.

Entre algunas dolencias técnicas identificadas de manera recurrente se encuentran:

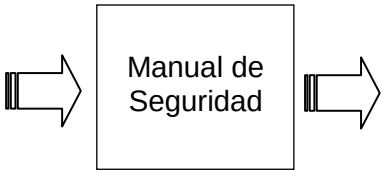
- Carencia de DMZ para la prestación de servicios de Internet.
- Carencia de una política de asignación de IP, categorizada según dispositivos, lo cual ocasiona que los host utilicen cualquier IP disponible, independientemente si es servidor, impresor, computador, tablet, móvil, etc. Situación que acarrea dificultades durante los procesos de administración, mantenimiento o auditoria complicando la identificación de los dispositivos.
- Carencia de políticas de usuario y grupos.
- Las configuraciones para el acceso a Internet desde la red LAN hacia el exterior suelen mantenerse tal cual la brinda el proveedor de Internet ISP, lo cual implica una vulnerabilidad para el resguardo de la información dentro de las alcaldías.
- Algunas configuraciones de dispositivos tales como router, Access point y otros son dejadas en ocasiones con sus valores de fábrica. Por ejemplo: con password “admin”.
- Carencia de herramientas como IDS para el monitoreo en tiempo real.
- Las instalaciones físicas de red usualmente son armadas por pasantes (estudiantes en servicio social) de alguna rama informática quienes en muchas ocasiones estructuran la red sin la supervisión adecuada.

- Utilización de software sin licencias.
- Carencia de un comité de seguridad encargado de crear las políticas de contingencia para la prevención de siniestros en la administración de la red.

1.1.1 Metodología de la Caja Negra

Mediante la metodología de la caja negra se pretende exponer la situación de la problemática identificada.

Carencia de un instructivo para la implementación de políticas y configuración de herramientas en seguridad informática que colaboren a mitigar y/o afrontar riegos de seguridad, a través de mejores prácticas, en la infraestructura de red informática de los Gobiernos Municipales de El Salvador.



Desarrollo de manual que dicte las directrices a seguir para la protección de la infraestructura de red informática de las municipalidades

Diagrama 1: Caja Negra de Manual de Seguridad. [1]

El detalle de los componentes que participan en el diagrama de la caja negra se puede desglosar de la siguiente manera:

Entrada

- Carencia de políticas de seguridad informática siguiendo las mejores prácticas.
- Carencia de una guía de configuración de herramientas en seguridad informática siguiendo las mejores prácticas.
- Infraestructura de red no certificada.
- Carencia de un comité de seguridad contra siniestros informáticos.

Proceso

- Manual de seguridad

Salida

- Políticas de seguridad informática aplicando las mejores prácticas.
- Desarrollo de un manual que establezca los procesos a seguir para la configuración de herramientas en seguridad informática aplicando las mejores prácticas.
- Propuesta para la certificación de redes
- Propuesta para la creación de equipos de respuesta a incidentes de seguridad.

1.1.2 Análisis de causas

Para este proceso en la etapa de la formulación del problema se hará uso del diagrama de Ishikawa, también llamado diagrama de espina de pescado para plasmar las causas que generan las deficiencias identificadas.

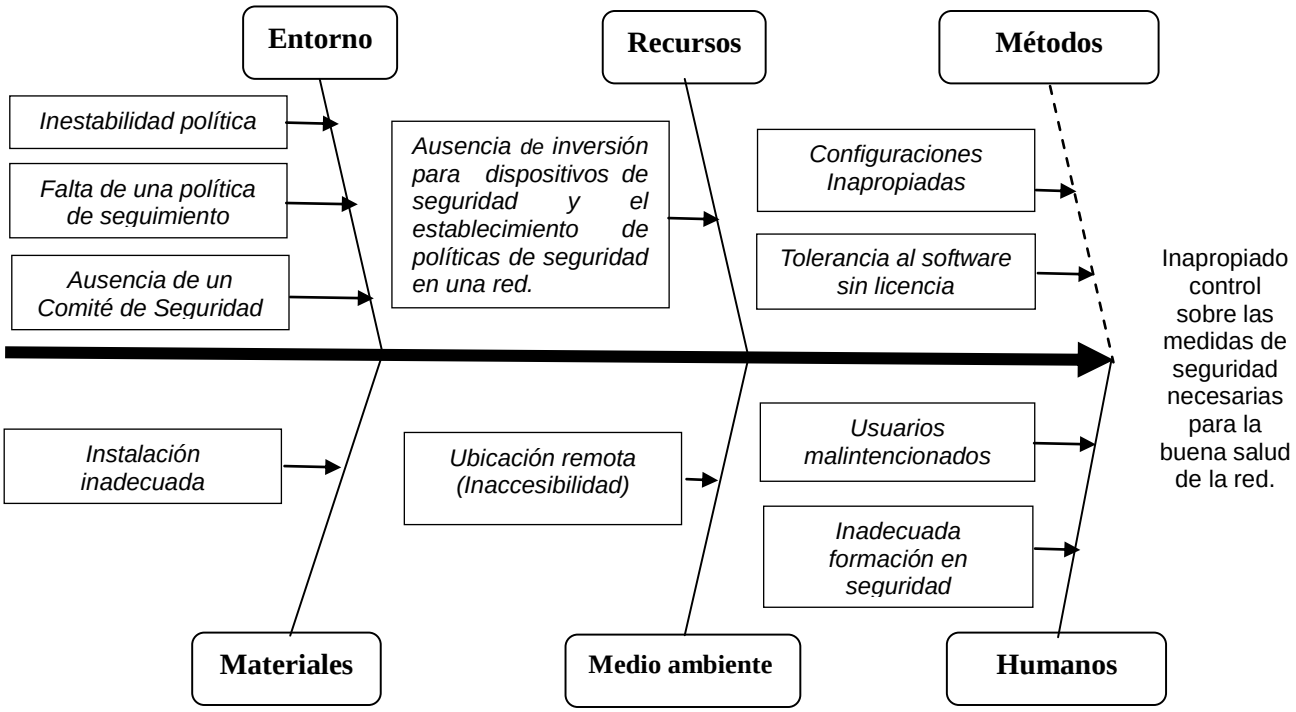


Diagrama 2: Espina de pescado de deficiencias identificadas. [2]

1.1.3 Árbol de problemas

El árbol de problema que se detalla en la gráfica a continuación enmarca la problemática generada por una serie de factores que influyen en el inadecuado manejo de los controles y establecimiento de las políticas de seguridad en las municipalidades.

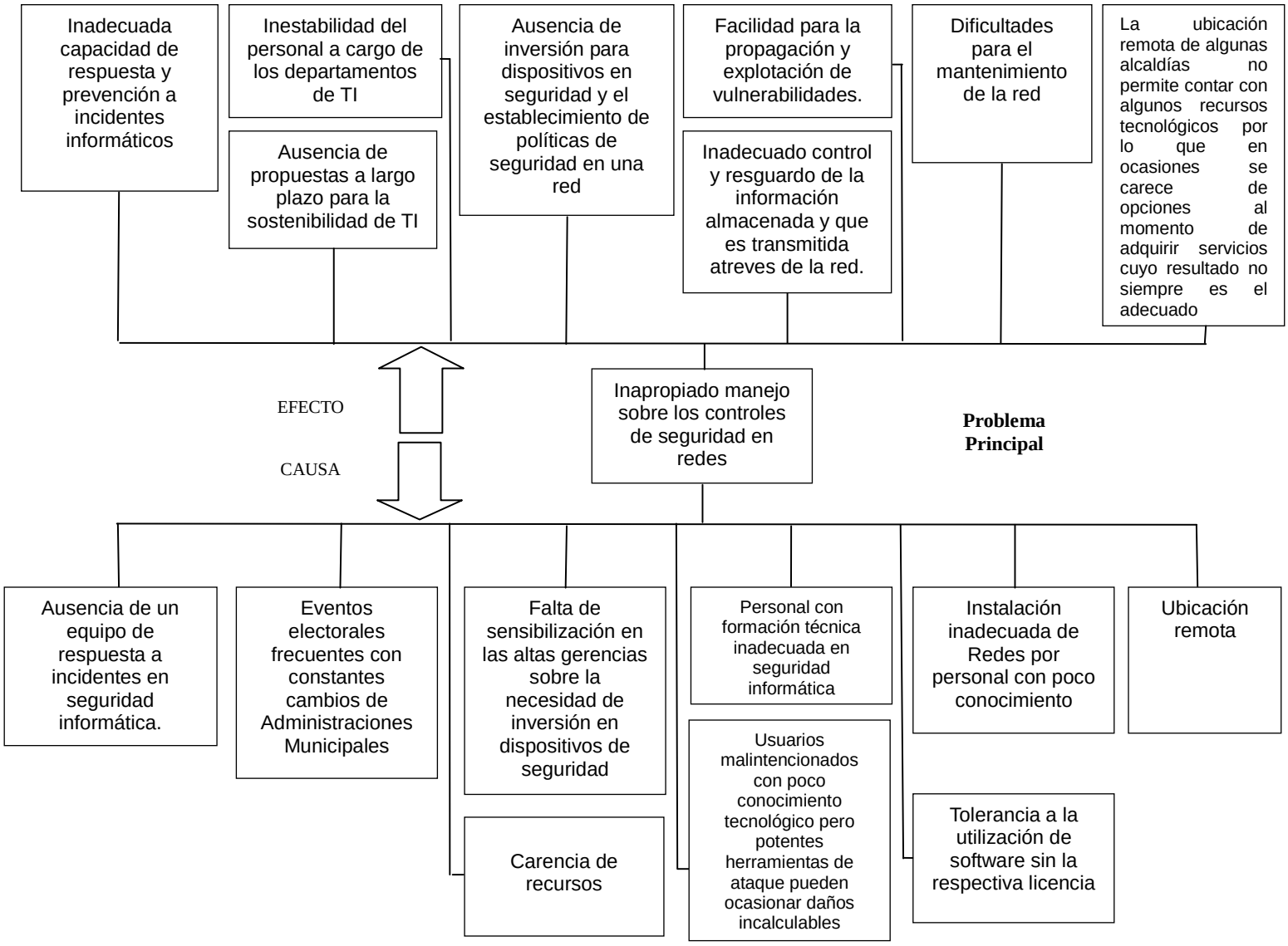


Diagrama 3: Árbol de problemas de deficiencias identificadas.

1.2 Justificación del proyecto

Las necesidades de implantación de políticas de seguridad en las redes informáticas han tenido que ir evolucionando de manera inquietante para hacerle frente al creciente número de ataques informáticos y a la sofisticación de los mismos. En la línea del tiempo se encuentra que ya en los años 70´s se registran los primeros ataques a los sistemas informáticos[7], el término Hacker aparece y es entonces que inicia la carrera en seguridad de redes informáticas.

Posteriormente en los 80´s; El Internet se comienza a difundir a partir del surgimiento de la computadora personal de Apple e IBM.

En los 90´ se dan los ataques más famosos y de mayor daño económico.

En la actualidad los virus han cedido su puesto a los troyanos, gusanos y spyware que son malware cuya finalidad primaria es la de obtener información confidencial sobre los usuario (datos personales o financieros como claves, números de cuentas bancarias, etc.) o bien ocasionar un sabotaje al hacer colapsar las redes informáticas (mediante por ejemplo: ataques masivos de denegación de servicio) y otros.

En las alcaldías de El Salvador se administra información sensible la cual es utilizada para la emisión de partidas de nacimiento[8]. Se comprende entonces que el fin de los gobiernos locales es el de enfocarse en otorgar a sus pobladores una mejor calidad de vida, lo cual incluye llevar registros informáticos fidedignos de cada uno de los habitantes del municipio para un control certero sobre cada una de las gestiones que los pobladores realizan (impuestos pagados, propiedades, partidas de nacimiento y otros). Resulta entonces imperativo el establecimiento de estrictas medidas de seguridad, haciendo uso de herramientas eficaces, que tomen en cuenta los procedimientos y las mejores prácticas existentes a fin de que colaboren para hacerle frente a las actividades delictivas. Procurando con ello reducir el campo de acción de ataques a través de la obtención de un adecuado nivel de seguridad ante accesos no autorizados.

---

7 http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/default.htm

8 Véase: Situación problemática identificada, pág. 15

1.3 Metas

Las metas que se pretenden alcanzar con la ejecución del establecimiento de políticas de seguridad en las redes informáticas dentro de las alcaldías de El Salvador; Suponen un logro importante para la realización de los objetivos finales. Por lo que se detallan a continuación:

- Establecer políticas de administración de usuarios para regular, clasificar y establecer obligaciones del personal que haga uso y/o ingrese a aquellas áreas donde se aloje equipo informático, que contengan información sensible, a fin de reducir en un 99% los accesos indebidos y evitar acciones inadecuadas.
- Establecer políticas para la gestión de software y hardware con el objetivo de proteger en un 95% los activos institucionales.
- Establecer políticas orientadas a priorizar la seguridad y protección de los datos; la información que se almacena y/o es transmitida a través de la red con el objeto de evitar en un 95% amenazas a la integridad de la misma.
- Procurar que al menos un 85% de las herramientas por sugerir a implantar dentro de la infraestructura de redes de las municipalidades cumplan con los procesos de buenas prácticas.

1.4 Impacto del proyecto

Se ha propuesto elaborar un proyecto de políticas que colabore con los Gobiernos Municipales de El Salvador en el establecimiento de una infraestructura de red segura que cumpla con un marco de trabajo establecidos por las mejores prácticas en materia de seguridad informática. Ello a partir de Determinar aquellas áreas dentro de las municipalidades que administren información sensible, en las cuales se centralizaran los esfuerzos para el resguardo de los datos.

El impacto del documento a elaborar permitirá a las municipalidades generar dentro de la población la confianza en que la información que es administrada por la comuna permanece integra, es manejada de manera confidencial y solo es accedida por personal autorizado.

1.4.1 Impacto Social

Tres son los actores beneficiados con la estructuración de este proyecto, a saber:

- **Beneficio para la población residente del municipio:**

  Dentro de cada Gobierno Municipal se encuentra resguardado el registro de asentamiento de todos y cada uno de los pobladores nacidos y/o residentes del municipio entre los que se pueden mencionar: registro y asentamiento de partidas de nacimiento; registro de trámites por adopción, marginaciones por matrimonio, divorcios y actas de defunción.

  Documentación que paulatinamente, en la mayoría de alcaldías del país, ha sido migrada de formato físico a digital, lo cual ha generado eficiencia en la administración de los mismos. Indudablemente esta información tan crucial de cada uno de los ciudadanos debe ser protegida, resguardada y transferida de forma segura para evitar que personas malintencionadas accedan a ella y generen algún acto vandálico sobre la misma. Para ello se ha proyectado diseñar las políticas de seguridad apropiadas para prevenir actos indebidos,

intencionales o no sobre dicha data. Lo anterior permitirá lograr generar certeza y garantizara que cada uno de los residentes del municipio tenga la plena confianza que su información está asegurada por la alcaldía que la administra.

- **Beneficio para El Gobierno municipal:**

  Según el Código Municipal en el Art. 31 dentro de las 2 primeras obligaciones de un Consejo Municipal se exige el cumplimiento de las actividades siguientes:

  1. Llevar al día mediante registros adecuados el inventario de los bienes del municipio.
  2. Proteger y conservar los bienes del municipio y establecer los casos de responsabilidad administrativa y patrimonial para quienes los tengan a su cargo, cuidado y custodia.

  Y siendo que cada Alcaldía es la representación política y legal de cada municipio, que tiene como principal misión administrar los intereses de la ciudadanía. Es de vital importancia que en todo momento la información que atañe a los pobladores sea mantenida segura, además debe cuidar y proteger adecuadamente los activos tecnológicos y la información que como institución administra. Por este motivo el presente documento pretende facilitar a los administradores de TI que adopten un conjunto de buenas prácticas en materia de seguridad informática para el establecimiento de una red saludable, para que puedan anticiparse a los riesgos y sepan cómo afrontarlos.

- **Beneficio para El Estado Salvadoreño**

  El Código Municipal en el Art. 2, enuncia sobre los Gobiernos municipales que “El municipio constituye la Unidad Política Administrativa primaria dentro de la organización estatal, establecida en un territorio determinado que le es propio,…” y siendo el ente responsable de la emisión de las partidas de nacimiento, a través de las cuales se gestiona el Documento Único de

Identidad DUI, comprobante único que permite al residente identificarse como ciudadano de nacionalidad Salvadoreña, con todos los derecho que ello conlleva tanto a nivel nacional como internacional[9], y que la obtención fraudulenta del mismo significa un riesgo para la nación, resulta valioso impedir que personas mal intencionadas puedan acceder a la obtención de una partida de nacimiento de manera impropia. En cuanto el presente documento servirá como una guía base sobre las políticas a establecer para minimizar los riesgos en las redes informáticas, para evitar modificaciones de registros municipales que puedan perjudicar la seguridad nacional.

1.4.2 Impacto Económico

Los alegatos que se esgrimen en ocasiones para justificar el postergar la implantación de sólidas y reales medidas de seguridad empleándose declaraciones tales como: falta de recursos por el costo que esto conlleva; o la incomodidad generada de establecer y constituir una cultura de seguridad en las organizaciones. Puede al final acarrear incalculables consecuencias económicas. Las siguientes publicaciones pueden ampliar mejor el panorama:

“Las pérdidas de Sony por ciberataque superarán los US$ 200 millones”, El País, 23-12-2014 . [10]

“Ciberatraco multimillonario al sistema de la Reserva Federal de los EE.UU.“ lavanguardia.com, 11-3-2016. [11]

Con la propuesta de políticas se pretende disminuir el riesgo de ataques y pérdida de información de carácter confidencial de las municipalidades. Y lograr alcanzar un nivel de seguridad donde la red informática de cada una de las instituciones se encuentre lo menos expuesta a vulnerabilidades posible. Además la implementación de políticas tendrá un impacto económico en las alcaldías debido a que reducirá los

[9] http://www.laprensagrafica.com/2014/11/12/california-aceptara-dui-para-otorgar-licencias

[10] http://www.elpais.com.uy/economia/empresas/perdidas-sony-ciberataque-superaran-us.html

[11] http://www.lavanguardia.com/economia/20160311/40360777065/ciberataque-hackers-ciberatraco-banco-central-bangladesh-reserva-federal-ciberseguridad-transferencias-bancarias-transacciones.html

costos generados por la pérdida y/o la alteración de información sensible o por los costos que podrían ser generados por una gestión inadecuada en los procesos de configuración de los recursos de la infraestructura de red informática.

1.4.3 Impacto Tecnológico

El impacto tecnológico por implementar políticas y estándares de seguridad en las redes informáticas dentro de Alcaldías municipales se presentara a través de dos aspectos.

- Software: La alcaldía obtendrá un valioso insumo para el establecimiento de políticas de seguridad mediante la propuesta de instalación de herramientas de seguridad lo cual generara sistemas operativos mucho más robustos al instaurar protección con antivirus, sistemas de alerta temprana y/o detección de intrusos IDS o IPS; delimitación de privilegios de cuentas; política de almacenamiento de datos; políticas de red que permitan el control del acceso de la red pública, red privada y viceversa.
- Hardware: En este ámbito, el gobierno municipal obtendrá la propuesta de algunos insumos tecnológicos en seguridad informática a los cuales podría acceder para fortalecer su infraestructura de red sin incurrir en onerosas inversiones.

Las propuestas a tratar se regirán bajo los conceptos de buenas prácticas informáticas. Las cuales guiarán el proceso de ejecución y puesta en marcha de seguridad dentro de las redes de las municipalidades.

1.5 Aspectos Financieros

Recursos (Presupuesto)

Recurso Humano

Descripción del Recurso	Cantidad	Duración (Días)	Horas de Trabajo por día	Horas Proyecto	Costo Hora	Costo Total
Investigadores	2	150	3	900	$ 7,00	$6,300.00
Asesor	1			12	$ 12,50	$150.00
Encuestador	1	30	8	240	$ 4,00	$960.00
Digitador	1	45	8	360	$ 4,00	$1440.00
Redactor	1	45	4	180	$ 5,50	$990.00
					Total	**$9,840.00**

Tabla 1: Recurso Humano.

Recurso Tecnológico

Descripción del Recurso	Cantidad	Duración (Días)	Horas de Trabajo por día	Horas Proyecto	Costo Hora / unitario	Costo Total
Computadora (alquiler/depreciación)	2	150		300	$0.41	$123.00
Impresor	1					$50.00
Fotocopiadora	1					$120.00
Comunicación	2	150	0,5	150	$ 1,80	$270.00
Switch y red	1					$120.00
Conexión a Internet	1	150				$220.00
					Total	**$903.00**

Tabla 2: Recurso Tecnológico.

Recursos Materiales

Descripción del Recurso	Cantidad	Costo Unitario	Costo Total
Papel (resmas)	6	3,5	$21.00
Impresor (tinta)	8	25	$200.00
Artículos Varios de oficina (lápiz, fólder, etc.)			$25.00
Artículos Varios (CD, Memoria USB, etc.)			$45.00
Otros varios (viáticos, trasporte, etc.)			$300.00
		Total	**$ 591.00**

Tabla 3: Recursos Materiales.

Resumen

Ítem	Costo del Recurso
Recurso Humano	**$9,840.00**
Recurso Tecnológico	**$903.00**
Recursos Materiales	**$ 591.00**
Sub Total	**$11,334.00**
Imprevisto (10%)	**$1133.40**
TOTAL	**$12,467.40**

Tabla 4: Resumen Financiero.

CAPITULO II: MARCO DE REFERENCIA

2.1 Buenas Prácticas

El concepto de buenas prácticas es utilizado bajo un entorno de múltiples contextos para referirse a las formas óptimas de ejecutar un proceso, que al ser replicado deberá generar los mismos bueno resultados dentro cualquier organización. Las buenas prácticas sistematizadas permiten aprender de las experiencias y aprendizajes de otros. Con un agregado de versatilidad que al aplicarlos de manera más amplia en otros contextos puede ocasionar la generación de nuevas ideas o surgir adaptaciones novedosas al proporcionar una orientación sobre la manera más efectiva de visibilizar los diversos impactos de una intervención en las instituciones.
En suma el concepto de buenas prácticas se refiere a toda experiencia que se guía por principios, objetivos y procedimientos apropiados o pautas aconsejables que se adecuan a una determinada perspectiva normativa o a un parámetro consensuado, así como también toda experiencia que ha arrojado resultados positivos, demostrando su eficacia y utilidad en un contexto concreto[12].

2.1.1 COBIT

COBIT (Common Objectives for Business Information Technology) Es un modelo de procesos que dictamina el plan de acción a seguir para la alineación de los recursos de las tecnologías de la información TI con los objetivos estratégicos de la empresa; su entorno es apoyado y se complementa por otros marcos de referencia tales como: ITIL, PMBOK, CMMI, ISO/IEC 9000, ISO/IEC 27000, ISO/IEC 38500, etc. Su finalidad principal es el de proponer las necesidades de control y medidas que aseguren el éxito de los objetivos de la organización a través de un marco de trabajo de dominios y procesos mediante: directivas de aseguramiento, objetivos de control, medidas de desempeño y resultados, factores críticos de éxito y modelos de

[12] http://www.paho.org/saludyescuelas/index.php?option=com_docman&task=doc_download&gid=88&Itemid=

madurez. Se conforma por 37 procesos aglutinados en torno a dos áreas clave (Gobierno y Gestión) que corresponden al ciclo de vida del sistema de información. Se encuentra constituido de la siguiente forma:

Dominio de Gobierno

Permite que todos los componentes participantes tengan una lectura organizada sobre el abanico de opciones existentes, definición de la ruta a seguir y el monitoreo sobre el cumplimiento de los planes establecidos. Incluyen:

- EDM (Evaluate, Direct and Monitor)
  Evaluar, Dirigir y Monitorear – Relacionado con proporcionar Gobierno de TI

Dominios de Gestión

Establece la utilización sensata de los recursos, procesos y prácticas para el logro de los objetivos. Lo conforman:

- APO (Aling, Plan and Organise)
  Alinear, Planificar y Organizar - Relacionado con las Estrategias para TI.
- BAI (Build, Acquire and Implement)
  Construir, Adquirir e Implementar – Relacionado con los Recursos: planes y puesta en producción.
- DSS (Deliver, Service and Support)
  Entregar, dar Servicio y Soporte – Relacionado con el Servicio al cliente.
- MEA (Monitor, Evaluate and Assess)
  Supervisar, Evaluar y Valorar – Relacionado con el Control y Seguimiento.

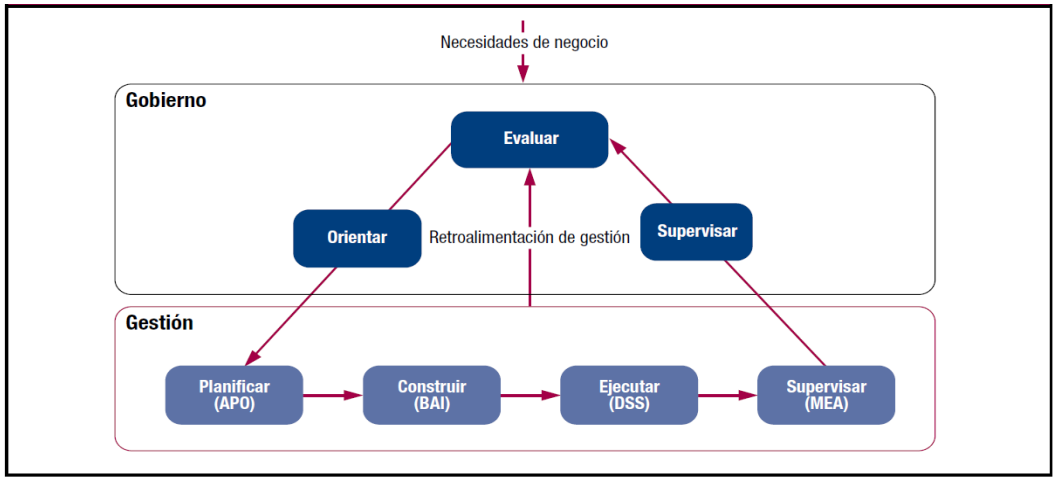


Diagrama 4: Áreas Clave de Gobierno y Gestión de COBIT 5. [13]

Los procesos incluidos en los Dominios de Gobierno y de Gestión se desglosan de la siguiente forma:

- **Dominio de Gobierno: EDM**

  El Dominio de Gobierno EDM contiene cinco procesos; dentro de cada proceso se definen las prácticas para Evaluar, Dirigir y Monitorear las cuales puede generar respuestas a interrogantes tales como:

  ¿La gerencia es capaz de asegurar que los controles aplicados son efectivos y eficientes?

  ¿Se puede asegurar que el riesgo de valor de la empresa en relación al uso de las TI es identificado y gestionado?

  ¿Está definido el marco de trabajo para la Gobernanza?

  ¿Se puede garantizar la trasparencia de los terceros interesados?

  Procesos a seguir respecto al Dominio: Evaluar, Dirigir y Monitorear

  EDM01 Asegurar que se fija el Marco de Gobierno y su Mantenimiento

  EDM02 Asegurar la Entrega de Valor

  EDM03 Asegurara la Optimización de los Riesgos

  EDM04 Asegurar la Optimización de los Recursos

  EDM05 Asegurar la Transparencia a las partes interesadas

[13] http://www.isaca.org/cobit/pages/default.aspx /

- **Dominio de Gestión: APO**

  El Dominio Alinear, Planificar y Organizar establece las formas mediante las cuales las TI deben generar su aporte al logro de los objetivos del negocio. Ello basados en una serie de cuestionamientos, a saber:

  ¿Las estrategias de TI se encuentran alineadas con las estrategias del negocio?

  ¿Los recursos de la empresa están siendo utilizados de manera óptima?

  ¿Los costos de ti son óptimos?

  ¿El personal puede utilizar los sistemas TI de manera eficiente y segura?

  ¿Los objetivos de TI son comprensibles para todos los miembros de la organización?

  ¿Se comprenden y administran los riesgos de TI?

  ¿La calidad de los sistemas TI cumple con los requerimientos y necesidades del negocio?

  Procesos a seguir respecto al Dominio: Alinear, Planificar y Organizar

  APO01 Administrar el Marco de la Administración de TI

  APO02 Administrar la Estrategia

  APO03 Administrar la Arquitectura Corporativa

  APO04 Administrar la Innovación

  APO05 Administrar el Portafolio

  APO06 Administrar el Presupuesto y los Costos

  APO07 Administrar el Recurso Humano de TI

  APO08 Administrar las Relaciones

  APO09 Administrar los Contratos de Servicios

  APO10 Administrar los Proveedores

  APO11 Administrar la Calidad

  APO12 Administrar los Riesgos

  APO13 Administrar la Seguridad

- **Dominio de Gestión: BAI**

  Para que un proceso de negocio logre sus objetivos se ha de identificar las soluciones que has de ser desarrolladas o adquiridas; las cuales posteriormente deberán de ser implementadas e integradas. Se ha de considerar además el desarrollo de un plan de mantenimiento para prolongar la vida de los sistemas TI y sus componentes. Este dominio deberá responder a una serie de cuestionamientos que se plantean a continuación:

  ¿Al iniciar un proyecto nuevo las soluciones responderán satisfactoriamente a las necesidades del negocio?

  ¿Se cumplirán los tiempos de entrega de los proyectos bajo el presupuesto establecido?

  ¿Al implantar los nuevos sistemas operaran eficientemente?

  ¿Las operaciones que en el presente se realizan se verán afectadas al aplicar cambios?

  Procesos a seguir respecto al Dominio: Construir, Adquirir e Implantar

  BAI01 Administrar Programas y Proyectos
  BAI02 Administrar la Definición de Requerimientos
  BAI03 Administrar la Identificación y Construcción de Soluciones
  BAI04 Administrar la Disponibilidad y Capacidad
  BAI05 Administra la Habilitación del Cambio
  BAI06 Administrar Cambios
  BAI07 Administrar la Aceptación de Cambios y Transiciones
  BAI08 Administrar el Conocimiento
  BAI09 Administrar los Activos
  BAI10 Administrar la Configuración

- **Dominio de Gestión: DSS**

  Este dominio se enfoca en los aspectos de entrega de los servicios requeridos, cubriendo operaciones tradicionales; entrenamiento, seguridad y

aspectos de continuidad. Además considera la administración de los datos por sistema de aplicación. Y ello se logra respondiendo a las siguientes interrogantes:

¿Los servicios de TI son entregados según prioridades establecidas por el negocio?

¿Se cumplen los criterios de Confidencialidad, integridad y disponibilidad?

Procesos a seguir respecto al Dominio: Entregar, Servir y Dar Soporte

DSS01 Administrar las Operaciones

DSS02 Administrar las Solicitudes de Servicios y los Incidentes

DSS03 Administrar Problemas

DSS04 Administrar la Continuidad

DSS05 Administrar los Servicios de Seguridad

DSS06 Administrar los Controles en los Procesos del Negocio

- **Dominio de Gestión: MEA**

  El dominio de Monitorear, Evaluar y Valorar se enfoca en los procedimientos a seguir para evaluar de manera frecuente los procesos establecidos; con el fin de corroborar la calidad y suficiencia de los mismos, verificando: integridad y confidencialidad. Y ello se logra al plantearse las siguientes preguntas:

  ¿Los controles de desempeño TI se efectúan frecuentemente para detectar los problemas antes que surjan?

  ¿El desempeño de TI está relacionado con las metas del negocio?

  ¿Se evalúan y reportan el cumplimiento, el control, el desempeño y los riegos?

  Procesos a seguir respecto al Dominio: Supervisar, Evaluar y Valorar

  MEA01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento

  MEA02 Monitorear, Evaluar y Valorar el Sistema de Control Interno

  MEA03 Monitorear, Evaluar y Valorar el Cumplimiento de los Requisitos Externos

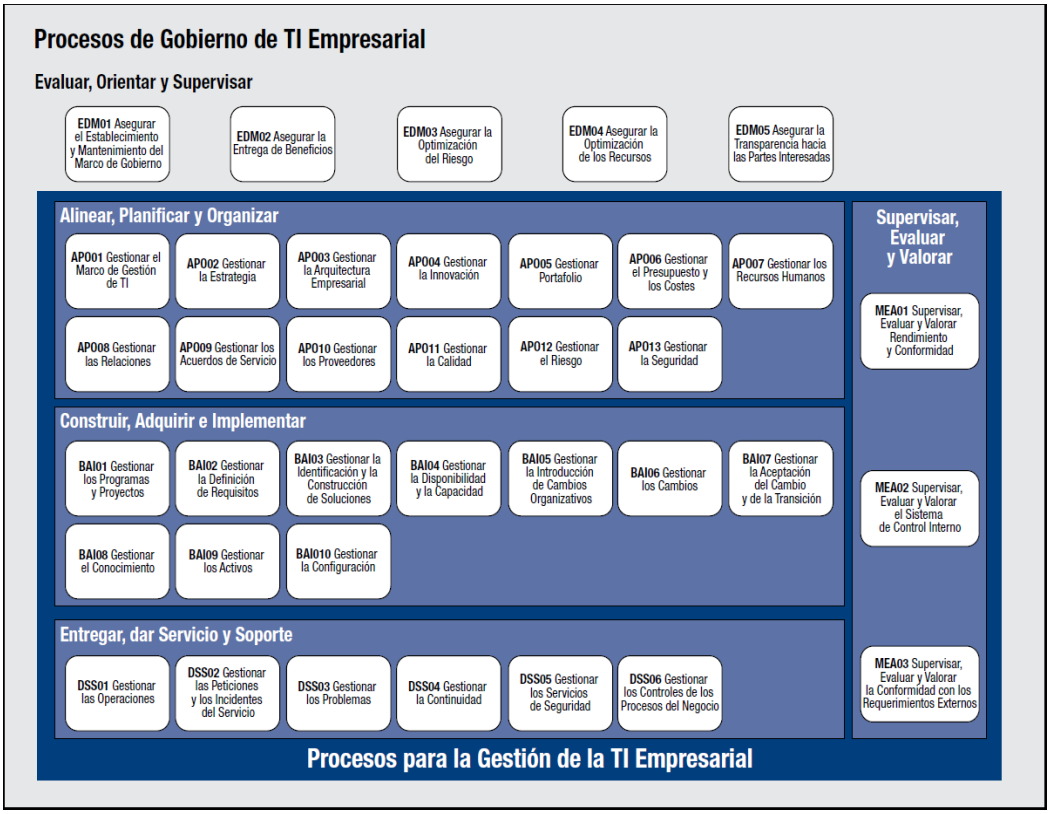


Diagrama 5: Procesos Facilitadores de COBIT 5. [14]

2.1.1.1 COBIT 5 y los marcos referenciales base de ISACA

- **Val IT**: Marco de referencia de gobierno que incorpora principios reconocidos y procesos de soporte inherentes a la evaluación y selección de inversiones de negocios de TI.
- **Risk IT**: Marco de referencia normativo establecido en un conjunto de principios guías que dictaminan la mejor forma de afrontar riesgos TI.
- **BMIS (Business Model for Information Security):** Realiza un análisis global de todos los componentes del negocio encaminado a la buena Gestión de la Seguridad informática.
- **ITAF (IT Assurance Framework):** Marco de referencia orientado al diseño, ejecución y reporte de evoluciones de cumplimiento y auditorías TI.

[14] http://www.isaca.org/cobit/pages/default.aspx /

2.1.1.2 Los principios de COBIT 5

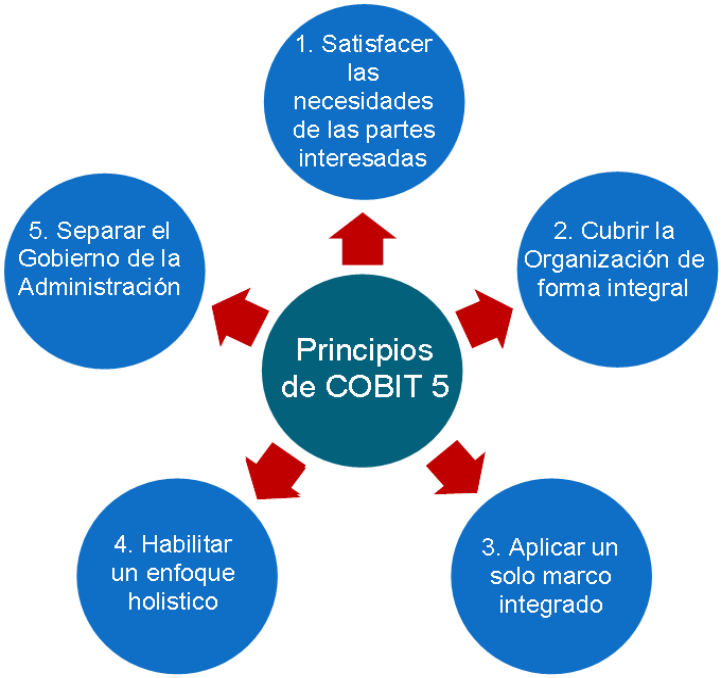


Diagrama 6: Principios de COBIT 5. [15]

Principio 1: Satisfacer las necesidades de las Partes Interesadas

Indica que el fin de las instituciones es ***crea valor*** para las partes interesadas.

Principio 2: Cubrir la Compañía de Forma Integral

En ella se enlaza el gobierno de la TI corporativa con cualquier sistema de gobierno siempre y cuando este se rija por lineamientos COBIT 5. Además instruye que las tecnologías de la información deben ser administradas como un valioso activo dentro la Institución.

Principio 3: Aplicar un solo Marco Integrado

COBIT 5 considera la mayoría de normas relevantes existentes; lo que incluye las normas corporativas (COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000) así como las relacionadas con TI (ISO/IEC 38500, ITIL, TOGAF, PMBOK/PRINCES2, CMMI, la

[15] https://www.isaca.org

serie ISO/IEC 27000)[16] de este modo puede ser utilizado como integrador macro de gobierno y administración

Principio 4: Habilitar un Enfoque Holístico

Conjunto de catalizadores que contribuye al logro de metas dentro de la institución; estas se define por siete categorías, entre las que se pueden mencionar: Principios, políticas y marcos de trabajo; Estructuras Organizativas; Cultura, ética y comportamiento; información, etc.

Principio 5: Separar el Gobierno de la Administración

Denota una clara diferencia entre ambas entidades debido a que ambas difieren en cuanto a su propósito; tipo de actividad y estructura organizacional (como comparar entre Junta directiva - presidencia versus Gerencia ejecutiva - CEO).

2.1.1.3 Conclusión

COBIT 5 ha sido desarrollado para controlar y auditar TI, para dar respuesta a la alta gerencia, a los accionistas de una empresa, su entorno es apoyado por múltiples herramientas como la medición de metas y desempeño aplicados a los procesos TI; de modo que se pueda comprender la forma en que los procesos satisfacen las necesidades del negocio; posee además, actividades clave; matriz de asignación de responsabilidades RACI; entre otras: a través de las cuales los directivos pueden comprender qué se debe auditar dentro de la organización. Por ello COBIT está orientado para grandes corporaciones o instituciones, como son aquellas que cotizan en bolsa o las que deben presentar estados financieros y están obligadas a tener acreditados sus mecanismos de control interno para asegurar que dentro de la empresa no se genera fraude. En El Salvador existen algunas alcaldías que han Titularización a través de la Bolsa de Valores de El Salvador tal es el caso de la alcaldía de San Miguel, San Salvador, Sonsonate, Santa Tecla y Antiguo Cuscatlán.

[16] http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt, lamina 22.

Gobiernos Municipales que debido al recurso que administran podrían implantar COBIT como una forma de control ya que los Valores de Titularización emitidos son respaldados por los flujos financieros futuros de una porción de los ingresos del Municipio y estos deben ser auditados por entes externos. Sin embargo debido a que es un modelo muy ambicioso que requiere un profundo estudio para su implementación COBIT resultaría prohibitivo para la gran mayoría de alcaldías de El Salvador.

2.1.2 ITIL

ITIL (Information Technology Infrastructure Library).

Conjunto de prácticas estándar desarrollado en los 80s, por el gobierno del Reino Unido, como un requerimiento donde se instituyeran las prácticas habituales a implementar en la dirección y gestión de servicios de tecnologías de la información. Es el entorno de trabajo de aplicación de buenas prácticas más ampliamente adoptado que está orientado a propiciar la gestión de entrega de servicios de las TI; Facilitando un marco práctico y prudente sobre que se ha de planificar, entregar y apoyar.

ITIL se enfoca en exponer que los servicios TI deben mantener la misma línea de acción que el de la institución. Estableciendo las pautas que faciliten la estrategia para la mejora, transformación y desarrollo del negocio.

2.1.2.1 Surgimiento de ITIL y sus publicaciones

A finales del siglo pasado, el desarrollo de la tecnología informática evoluciono de Instituciones de TI centralizadas a un concepto más disperso en donde los dispositivos se distribuían en múltiples zonas geográficas, situación que acarreaba la incompatibilidad en la aplicación de procesos y entrega de servicios. Ante dicha situación el gobierno del Reino Unido (basándose en investigaciones realizadas por la Central Computer and Telecommunications Agency CCTA y el apoyo de IBM)

pronostico que estableciendo practicas homogéneas para cada uno de los aspectos del ciclo de vida de los servicios TI podría colaborar en la dirección de la institución de manera eficaz, así como la obtención de servicios predecibles. A partir de entonces surge ITIL como una plataforma eficaz y coherente que se encarga de promover la excelencia en el negocio de la gestión de servicios de TI.

En sus inicios se introducen diez libros centralizados en el Soporte de Servicio y Prestación del Servicio. Posteriormente en los 90s se relanza una segunda versión, conocida como ITIL V2 (enfocado en la alineación de TI al negocio), compuesta por treinta libros la cual evoluciona a ITIL V3 (enfocado en la integración de TI al negocio). Cuyo núcleo principal (Alineado con ISO 20000 y otros estándares como ASL, eTOM, COBIT, Six Sigma) se concentra en cinco publicaciones, donde se ofrece una perspectiva sistemática y profesional para la gestión de TI; a saber:

- Estrategia de servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

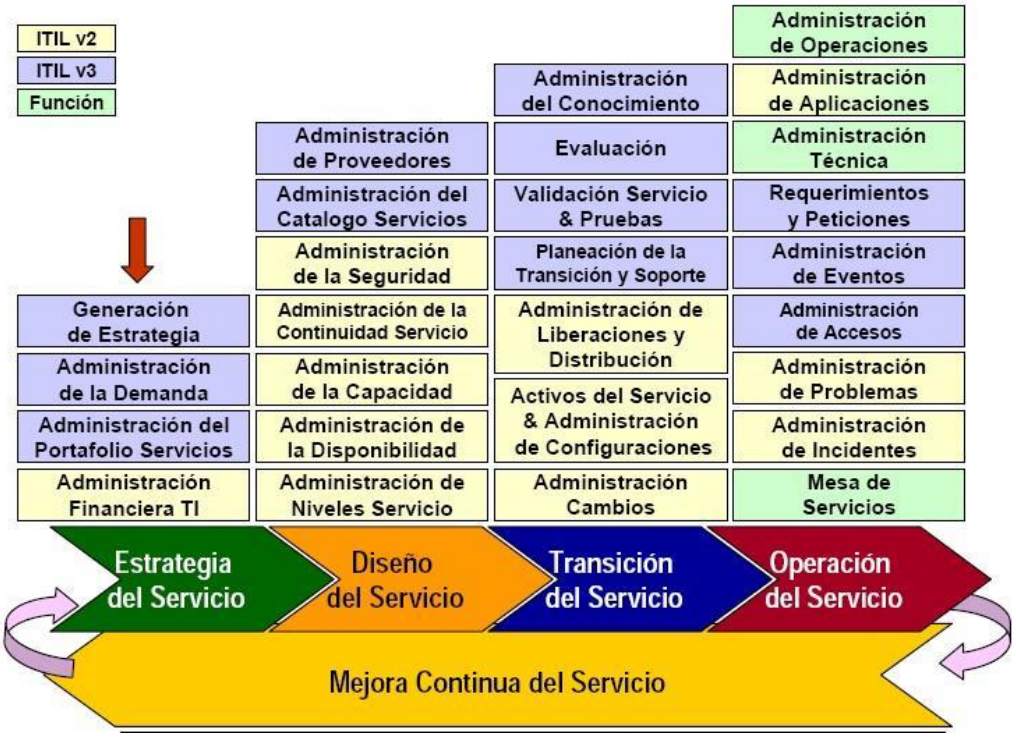


Diagrama 7: Procesos y funciones ITIL. [17]

- **Estrategia de Servicio (Service Strategy):**

  Es el eje central al ciclo de vida de servicio cuyo principal objetivo es el de transformar la Gestión de Servicio en un activo estratégico al mismo tiempo que provee lineamientos, que serán utilizados para el diseño de los servicios TI.

- **Diseño del Servicio (Service Design)**

  Establece el diseño, la creación o modificación del servicio TI que habrán de incorporarse al catálogo de servicios. Además de proponer la arquitectura de infraestructura que habrá de cumplir con los requerimientos del negocio alineándola a las necesidades del mismo.

[17] http://shop.pultorak.com/

- **Transición del Servicio (Service Transition)**

  Encausa la transición de los productos y servicios planteados en la fase de diseño para incorporarlos al entorno de producción. Garantizando que estos nuevos servicios cumplan con los requisitos y estándares de calidad definidos y exigidos.

- **Operación del Servicio (Service Operation)**

  Es la culminación de todos los procesos; debido que es a través de la operación del servicio que el cliente mide la eficiencia del servicio prestado y emite juicio sobre si la prestación del servicio llena las expectativas acordadas según los niveles de calidad solicitados.

- **Mejora Continua del servicio (Continual Service Improvement):**

  Crea y mantiene el valor a los clientes a través de evaluaciones y mejoras continuas de la calidad de los servicios. Ello a través del modelo PDCA (Plan, Do, Check, Act) del inglés: Planificar, Hacer, Verificar y Actuar. Da seguimiento a los SLAs contratados y aplica fundamentos que incluyen Administración de Calidad, Administración de Cambios y mejora de capacidades, todo enmarcado en la constante mejorar de los servicios, procesos y actividades involucradas en la gestación y prestación de servicios TI.

2.1.2.2 ITIL en la práctica

Un ejemplo de un servicio de negocio que suele ser un proceso común en muchas industrias es el de la planilla de pagos. La planilla es un servicio de TI que se utiliza para consolidar información, calcular la compensación y generar los cheques de pago de forma regular. Dichos procesos se basan en otros servicios empresariales. Tales como: el seguimiento del tiempo de trabajo o la administración de beneficios

los cuales proporcionar toda la información necesaria para la realización de los cálculos.

Para que se ejecute la nómina de pago, este se ha de apoyar en una serie de tecnologías o servicios de infraestructura. Un servicio de infraestructura hace su trabajo en un segundo plano, de manera que el negocio no interactúa directamente con él. Sin embargo este servicio es necesario como parte de la cadena global de valor para el servicio del negocio. Algunas de las tecnologías que intervienen y aportan información a la planilla de pagos son: Administración de servidor, administración de base de datos y administración de almacenamiento. [18]

2.1.2.3 Conclusión

Aunque ITIL es un marco de trabajo de las mejores prácticas, comúnmente aceptadas, ideadas para facilitar la entrega de servicios TI a las organizaciones independientemente de su tamaño, su versión v3 se ha robustecido de manera considerable, tanto que su aplicación resulta muy compleja por lo que pocas instituciones tratarían de aplicarlo de manera global. Su utilización practica requiere que cada organización seleccione solo aquellos procesos que le permitan añadir valor a la misma, situación que dificultaría la propuesta y selección de procesos que sean comunes a las necesidades de cada alcaldía, aunado a lo anterior debe considerarse el tiempo de adopción que podría rondar al menos los 5 años, requiere mucho esfuerzo y participación activa de todo el personal junto con la asignación de recursos para la contratación de personal certificado. Por lo anterior se determina que la utilización de ITIL v3 para el ***desarrollo de políticas comunes,*** que abarquen a la mayoría de los gobiernos municipales de El Salvador, resultaría muy complejo.

[18] Traducido de http://www.best-management-practice.com/gempdf/itil_the_basics.pdf, pág. 3.

2.1.3 ITIL Y COBIT (diferencias)

Ambas propuestas difieren en el sentido que: COBIT tiene por principio planear; organizar, dirigir y controlar la función informática. Colaborando a estandarizar la organización a través de: Evaluar, Formular, Definir, Justificar y Auditar. Por lo que al ser más completo y sistematizado indica a la dirigencia ¿qué? se debe controlar. Mientras que ITIL indica ¿cómo? se debe de hacer el control que se ha de ejercer sobre los procesos, mediante la mejora del servicio de la organización y la medición del mismo[19]**.**

2.1.4 Estándares ISO en seguridad de la información.

2.1.4.1 BSI Group

En 1901 es fundado en Londres el primer organismo de normas en el mundo; Inicialmente se denomina Comité de Ingeniería de Normas pero ante el importante crecimiento, diversificación y expansión global de la empresa se modifica su nombre y es renombrada como BSI Group (en inglés: British Standards Institution). Se constituye con la finalidad de garantizar el desarrollo de productos y servicios fiables y seguros; Ello a través de colaborar con las organizaciones a hacer de la excelencia un hábito (según su eslogan: "...making excellence a habit"). Su fortaleza se basa en ser reconocida como una súper marca del Reino Unido; una fuente desarrolladora de Normalización y estandarización de procesos y es un asociado de la Organización Internacional de Normalización ISO (en inglés: International Organization for Standardization) institución que establece la creación de Normas Internacionales de fabricación de productos y servicios; comercio y comunicación, la cual pretende facilitar el comercio mundial de bienes, servicios, información y tecnología.

[19] Cervantes Rodríguez, Adalberto. La diferencia entre ITIL® y COBIT, en pocas palabras www.bitcompany.biz/diferencia-itil-y-cobit/

2.1.4.2 Normativas BSI

Las normativas desarrolladas por BSI cubren múltiples disciplinas y están orientadas a mejorar el desempeño de las organizaciones; reducir el riesgo comercial; ser más sustentable y fomentan la seguridad e innovación. Entre las más destacadas se pueden enunciar:

- Aeroespacial AS 9100
- Automotriz ISO/TS 16949
- Dispositivos Médicos ISO 13485
- Gestión de Calidad ISO 9001
- Gestión de la Continuidad del Negocio ISO 22301
- Gestión de Energía ISO 50001
- Gestión Medioambiental ISO 14001
- Gestión de Riesgos ISO 31000
- Inocuidad Alimentaria ISO 22000
- Responsabilidad Social SA 8000
- Seguridad y Salud Ocupacional BS OHSAS 18001
- Seguridad de la información ISO/IEC 27001
- Seguridad en la Nube Certificación STAR
- Servicios de TI ISO/IEC 20000
- Sistemas Integrados PAS 99

En la siguiente imagen puede observarse el crecimiento a nivel mundial de entidades o personas que han obtenido certificaciones ISO durante los últimos 2 años y que han sido desarrolladas por BSI Group.

Standard	number of certificates in 2014	number of certificates in 2013	evolution	evolution in %
ISO 9001	1 138 155	1 126 460	11 695	1 %
ISO 14001	324 148	301 622	22 526	7 %
ISO 50001	6 778	4 826	1 952	40 %
ISO/IEC 27001	23 972	22 349	1 623	7 %
ISO 22000	30 500	26 847	3 653	14 %
ISO/TS 16949	57 950	53 723	4 227	8 %
ISO 13485	27 791	25 655	2 136	8 %
ISO 22301	1 757			
TOTAL	**1 609 294**	**1 561 482**	**47 812**	**3 %**

Imagen 1: Crecimiento de Certificaciones ISO años 2013 y 2014. [20]

2.1.4.3 ISO/IEC 27001

ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements.

La ISO 27001 es el Estándar internacionalmente reconocido, como el marco de las mejores prácticas, que especifica los requisitos mínimos necesarios que se han de cumplir para controlar que en la Gestión de Seguridad de la Información: se analicen y evalúen los riesgos; se planifique, se implemente, revise y corrija la estrategia a seguir a fin de promover la mejora continua del Sistema de Gestión (cumpliéndose el ciclo: Plan, Do, Check, Act).

2.1.4.4 ISO/IEC 27002

ISO/IEC 27002 Information Tecnology – Security techniques – Code of practice for security management.

La ISO 27002 es el código de buenas prácticas de seguridad de la información desarrollado con la finalidad de proveer una guía para la implementación de controles para el Sistema de Gestión de Seguridad de la Información ISO 27001. La versión

[20] http://www.iso.org//

más reciente (ISO/IEC 27002:2013) consta de 14 Dominios, 35 Objetivos de control y 114 controles.

Diagrama 5-2: Evolución del Estándar ISO/IEC 27002

2.1.4.5 Conclusión

La ISO 27001 especifica los requisitos para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información los cuales de ser cubiertos en su totalidad permiten aspirar a la organización que los aplica poder certificarse; lo anterior exige que en la gestión: se adquieran responsabilidades específicas; que se deben establecer objetivos (los cuales deben medirse, revisarse y actualizarse); se deben efectuar auditorías internas y otra serie de obligaciones adicionales que resultarían onerosa para la mayoría de la Alcaldías de El Salvador. Las anteriores exigencias no están establecidas en el código de buenas prácticas de la ISO 27002, por lo que es más factible su adopción para cualquier institución independientemente de su tamaño y recurso.

El presente documento únicamente toma como guía el listado de dominios ofrecidos por la ISO 27002 para tener un bosquejo de los elementos que se deben de considerar a la hora de establecer políticas, más no está dentro del alcance del mismo: certificar, ni adoptar, ni proponer la implementación de ninguna norma o estándar de seguridad informática en los Gobiernos Municipales de El Salvador.

2.2 Antecedentes tecnológicos relacionados

2.2.1 Redes y componentes

Red de Área Local / Local Área Networking (LAN)

Las redes de área local se desarrollan a nivel privado por lo que tienen un rango de acción reducido (ejemplo compañías con distancia menor de un kilómetro). Este tipo de red es diseñada para conectar computadoras con el objetivo de compartir recursos e intercambiar información.

Las características de una red de área local son:

- Alcance corto o limitado
- Para edificio o empresa pequeña.
- Un único propietario.
- Altas velocidades de transmisión de datos.
- Generalmente la transmisión es en Banda Base (Base Band).

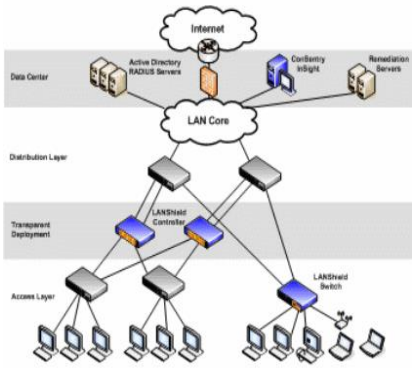


Imagen 2: Red de área local.

Topología de una red

Las topologías de redes son variadas, su función es la de generar un efecto directo sobre el comportamiento y el rendimiento de la estructura de red en la cual se dispongan. Existen varios tipos de topología de red; entre las más conocidas se tienen: árbol, estrella, anillo, bus, malla, etc. La más difundida debido a su versatilidad y escalabilidad es la topología estrella.

Topología Estrella

Las redes en estrella están estructuradas en una topología dentro de la cual cada estación está directamente conectada a un nodo central generalmente denominado concentrador o hub, a través del cual, se transmite la data que transita por la red.

La conexión entre dispositivos en la red es independiente entre sí por lo que la desconexión de un equipo conectado a la misma no afecta la conexión con los restantes dispositivos. Empero si el nodo central falla toda la red queda sin servicio.

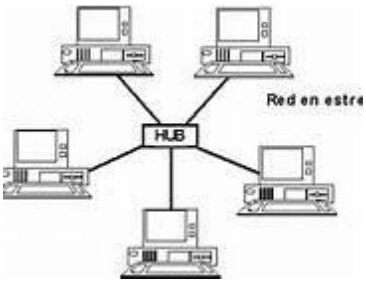


Imagen 3: Topología en estrella.

Cableado de red

La mayoría de las redes se conectan a través de algún tipo de cable, el cual opera como medio de transmisión por donde pasan las señales entre los distintos dispositivos. Existen una gran cantidad de tipos de cables para cubrir las necesidades y tamaños de las diferentes redes, desde las más pequeñas a las más grandes. Entre los tipos de cables más frecuentemente utilizados se tienen: cable coaxial, cable par trenzado, y fibra óptica.

Cable de par trenzado (UTP)

El cable par trenzado consiste en un arreglo de alambres de cobre (en ocasiones de aluminio) dispuestos como tramas entrelazadas con el propósito de reducir la interferencia eléctrica de sus pares similares cercanos. Se protegen con una cubierta de PVC en compuestos multipares de pares trenzados de 2, 4, 8 y hasta 300 pares. El Cable UTP con categoría 5e (que es un cable de cobre par trenzado de cuatro hilos de 100 OHMIOS), Con la especificación 100BaseT, que soporta transmisiones

de 100 Mbps, es el tipo más conocido y de uso más extendido de cable de par trenzado. Su segmento máximo de longitud recomendada es de 100 metros y aunque en la práctica se ha comprobado que se puede extender un poco más el fabricante lo desaconseja.

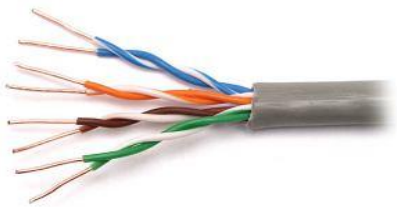


Imagen 4: Cable de par trenzado UTP.

Cable de fibra óptica

Los cables de fibra óptica han sido diseñados para soportar señales digitales de datos, las cuales son transmitidas en forma de pulsos modulados de luz. Las transmisiones a través de este tipo de cable tienden a ser más seguras si se les compara con las emitidas a través de un cable de cobre; ello es debido a que estas últimas trasladan los datos en forma de señales electrónicas.

Los cables de fibra óptica transportan impulsos no eléctricos. Esto significa que el cable de fibra óptica no se puede pinchar por lo que sus datos transferidos no se pueden interceptar. El cable de fibra óptica es apropiado para transmitir datos (Full-Duplex: transmisión de datos en ambos sentidos simultáneamente) a velocidades muy altas y con grandes capacidades debido a la carencia de atenuación de la señal y a su pureza.

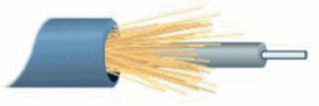


Imagen 5: Cable de Fibra Óptica.

Norma EIA TIA 568A/568B

Es el referente estándar de cableado estructurado más utilizado el cual está definido por la Electronics Industries Association / Telecommunications Industries Association (EIA/TIA), de Estados Unidos. Este estándar especifica un conjunto de normas que permiten optimizar las conexiones de las estaciones de trabajo que conforman una red cableada estructurada. Ello queda enunciado en la Norma de la siguiente forma:

"Esta norma específica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifabricante. También proporciona directivas para el diseño de productos de telecomunicaciones para empresas comerciales.

El propósito de esta norma es permitir la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad. La instalación de sistemas de cableado durante la construcción o renovación de edificios es significativamente menos costosa y desorganizadora que cuando el edificio está ocupado." [21]

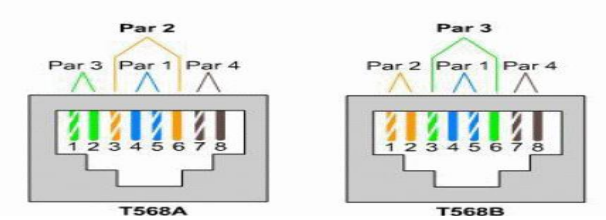


Imagen 6: Estándar T568A y T568B. .

Router: Es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

[21] Norma EIA/TIA 568-A

Las dos principales funciones de los routers son la determinación de la mejor ruta y la conmutación de paquetes a la interfaz correcta, con el protocolo de comunicación correcto, en este caso la implementación del protocolo de comunicación TCP/IP.

Imagen 7: Router.

Switch: (En castellano “interruptor” o “conmutador”) es un dispositivo de interconexión de redes de ordenadores/computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Imagen 8: Switch.

Tarjeta de Interfaz de Red: (Network Interface Card, NIC -Denominadas también adaptadores de red o sólo tarjetas de red-) Dispositivo que permite la comunicación entre distintos host interconectados entre sí a través de una red. Todo computador debe contar con una tarjeta NIC de interfaz de red para poder compartir recursos con otros equipos.

Imagen 9: Tarjeta de red NIC.

Conector RJ 45: Interfaz física que contiene ocho pines que interconectan conexiones de cable par trenzado con los puertos Ethernet.

Imagen 10: Conector RJ-45.

CAPITULO III: FORMULACION DE HIPÓTESIS

3.1 Hipótesis General

La carencia de políticas establecidas para la seguridad de las redes informáticas en las alcaldías de El Salvador podrá acarrear riesgos en los activos informáticos ocasionando pérdidas económicas y/o fuga de información.

3.2 Hipótesis Particular

La ausencia de políticas de seguridad en las redes informáticas dentro de las alcaldías de El Salvador trae como resultado que los riesgos asociados a los activos informáticos ocasionen daños y puedan interrumpir las operaciones.

3.3 Hipótesis nula (H0)

El establecimiento de políticas de seguridad en redes informáticas, aplicando las mejores prácticas, para instaurar en las alcaldías de El Salvador. No trae ningún beneficio para la alcaldía.

3.4 Variables

Variables Independientes

Para el presente estudio se supondrá que los gobiernos municipales no tienen establecidas políticas de seguridad de la información que forme parte de la cultura organizacional de la alcaldía donde se plasmen la hoja de ruta o el plan de acción a seguir para minimizar amenazas a la red y proteger sus activos informáticos. A partir de ello se propone la siguiente variable independiente:

- No tener establecidas políticas de seguridad en las redes informáticas.

Variables Dependientes

Ante el supuesto de la ausencia de un manual de políticas de seguridad en las alcaldías de el Salvador y con el fin de verificar si estas han sido objeto de incidentes, que han expuesto y comprometido la seguridad de la información digital que administran, lo cual implica danos económicos y ante la ausencia de controles que crean un escenario que dificulta la posibilidad de mantener una infraestructura de red estable, segura y saludable; que no garantiza el apropiado resguardo de los activos informáticos institucionales, se enuncian las siguientes variables dependientes:

- Riesgos ocasionados por pérdidas económicas.
- Fuga de información.

CAPITULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1 Generalidades

El estudio tiene como propósito desarrollar un diagnóstico sobre los resultados obtenidos en la investigación de campo realizada dentro de las Alcaldías de El Salvador.

Entre los propósitos de la elaboración del estudio se encuentra el de identificar el nivel de seguridad que los encargados de TI aplican a la red informáticas bajo su cargo; conocer el grado de compromiso que los mismos poseen respecto al resguardo de la información que circula a través de la red; establecer el grado de concientización que la alta gerencia tiene sobre la necesidad de inversión en dispositivos o herramientas de seguridad y finalmente, tener un parámetro del nivel de aceptación que tendría la propuesta de un documento donde se sugiera la implementación de políticas de seguridad dentro de la infraestructura de red de los Gobiernos Municipales de El Salvador. Fundamentando entonces las conclusiones basados en el análisis y la tabulación de los datos obtenidos.

4.1.1 Objetivos de la Investigación de Campo

General

Establecer los criterios para categorizar los gobiernos municipales según su tamaño. Conocer el grado académico de los encargados de TI y si conocen de irrupciones, sean estos provocados o accidentales, que haya comprometido la seguridad informática institucional; de que herramientas y controles dispone en la aplicación de mecanismos de seguridad; si cuenta con apoyo externo, interno y financiero para el establecimiento de medidas de seguridad y la exploración sobre el grado de aceptación o rechazo que se obtendría al plantear una propuesta para el desarrollo de políticas de seguridad informática que colabore con los Gobiernos Municipales de El Salvador en el establecimiento de una infraestructura de red segura que cumpla

con un marco de trabajo establecido por las mejores prácticas en materia de seguridad informática.

Específicos

- Identificar y catalogar la magnitud de las alcaldías de acuerdo al número de edificaciones interconectadas, número de host con que cuenta y herramientas de seguridad utilizadas a fin de categorizar los gobiernos municipales en grupos comunes.
- Identificar si las alcaldías de El Salvador han mantenido su infraestructura de red operable y estable sin haber sido afectada en su integridad, disponibilidad, autenticidad y confidencialidad en la data que posee bajo su resguardo.
- Identificar si los departamentos de TI cuentan con apoyo externo calificado en lo que a seguridad informática y tecnológica respecta, y con apoyo interno de la alta gerencia de la comuna, de forma que la gestión de servicio TI este correctamente alineada con los procesos de mejora continua de la institución.
- Conocer el grado de aceptación y la disponibilidad de parte de los encargados TI de las alcaldías para implementar un manual que dicte el código de conducta a seguirá por medio de políticas, basadas en buenas prácticas, para la mejor administración y seguridad de su red informática.

4.1.2 Fuentes de Información

Primaria

La información se ha obtenido por medio de un cuestionario estructurado, el cual ha tenido como sujeto principal de investigación los encargados de TI de las alcaldías de El Salvador.

Secundaria

Como fuente secundaria de información se contó con el apoyo de material bibliográfico referido al tema tales como tesis, libros de texto, sitios Web, apuntes de clases, etc.

4.1.3 Ámbito o Alcance de la Investigación

En el proceso investigativo se consideró un porcentaje de Alcaldías que representan una muestra del universo de los potenciales beneficiarios al desarrollar el presente documento.

4.1.4 Universo de la Investigación

Se basa en el número total de Gobiernos Locales que componen la República de El Salvador, los cuales conforman un universo finito de 262 Municipios.

4.1.5 Muestra de la Investigación

Se basa en una distribución muestral por proporciones lo que implica considerar las siguientes variables.

P: probabilidad de beneficio al implementar políticas de seguridad.

Q: probabilidad de perjuicio al no implementar políticas de seguridad.

Asumiendo un porcentaje similar para ambas opciones se tiene:

P=50% Y Q=50%

Teniendo un universo de Gobiernos Municipales finito se aplica la siguiente formula:

$$n = \frac{Z^2 P\,(QN)}{E^2\,(n-1) + z^2\,(PQ)}$$

Dónde:

n = Tamaño de la muestra =?

N = Tamaño del universo = 262

Z = Grado de confianza = 75% (K=1.15)

P = Probabilidad de beneficio al implementar políticas = 0.5

Q = Probabilidad de perjuicio al no implementar políticas = 0.5

E = Máximo error permitido = 10%

n = 29 participantes

4.2 Diseño de la Herramienta de Investigación

4.2.1 Cuestionario Estructurado

En el proceso para la obtención de la información se utilizó la técnica de la encuesta, por medio de un cuestionario estructurado, el cual se conforma de la siguiente manera:

1. Petición de colaboración (encabezado: Generalidades, Objetivo, instrucciones y bienvenida): se le informa al encuestado sobre los fines para los cuales será utilizada la encuesta y al mismo tiempo se le solicita su aporte y colaboración en el llenado de la misma.
2. Datos de clasificación: Se solicita al encuestado determinar el número de edificaciones interconectadas en red LAN; cantidad de computadoras con que cuenta la comuna; sistema operativo mayormente instalado y nivel académico del responsable TI de la Alcaldía. Donde el número de edificaciones interconectadas es la categoría de clasificación utilizada para la tabulación de resultados**.**
3. Cuerpo del cuestionario: lo conforma el conjunto de 12 preguntas cerradas y 1 abierta**.**
4. Datos de identificación: Espacio reservado para identificar el nombre del encuestador/a, nombre de la Alcaldía; firma y sello del participante del cuestionario.

4.2.2 Prueba Piloto

Se efectuó una prueba piloto con una serie de preguntas realizadas a gerentes de informática de alcaldías pertenecientes al departamento de San Salvador, sobre los resultados obtenidos se realizó la redacción definitiva de la encuesta**.**

4.2.3 Administración de la Encuesta

Una vez alcanzada la cantidad de participantes requeridos para el proceso de la encuesta, y tras finalizado dicho proceso, la información obtenida de cada uno de los cuestionarios fue vaciado en un sistema que permitió realizar el cálculo de los resultados de la investigación generando la tabla de frecuencias y su respectivo gráfico.

CAPITULO V: RECOLECCIÓN DE DATOS

Los datos obtenidos en la investigación de campo se recopilaron considerando 29 Gobiernos Municipales seleccionados de entre varios departamentos de El Salvador. El número de municipios participantes de la encuesta se describen en la siguiente figura

Diagrama 8: Número de Municipios participantes de la encuesta según Departamentos de El Salvador. .

El listado de Municipios participantes de la muestra se detalla en la siguiente tabla

No	Departamento	Municipio	Edificaciones Interconectadas	Cantidad de computadoras	Población con DUI
1	Ahuachapán	Alcaldía Municipal de San Lorenzo	1	11 a 50	9194
2	Chalatenango	Alcaldía Municipal de La Palma	1	11 a 50	6454
3	Chalatenango	Alcaldía Municipal de Nueva Concepción	1	11 a 50	28625
4	Chalatenango	Alcaldía Municipal de San Ignacio	1	menos de 10	4556
5	Cuscatlán	Alcaldía Municipal de San Pedro Perulapán	1	11 a 50	23171
6	Cuscatlán	Alcaldía Municipal de San Bartolomé Perulapia	1	11 a 50	4158
7	Cuscatlán	Alcaldía Municipal de San Rafael Cedros	1	11 a 50	9062
8	La Libertad	Alcaldía Municipal de Ciudad Arce	1	51 a 200	60314
9	La Libertad	Alcaldía Municipal de San Matías	N/R	11 a 50	7314
10	La Libertad	Alcaldía Municipal de Antiguo Cuscatlán	más de 4	51 a 200	33698
11	La Libertad	Alcaldía Municipal de San Juan Opico	2	11 a 50	74280
12	La Libertad	Alcaldía Municipal de San Pablo Tacachico	1	11 a 50	20366
13	La Libertad	Alcaldía Municipal de Zaragoza	1	11 a 50	22525
14	La Paz	Alcaldía Municipal de San Juan Talpa	1	11 a 50	4067
15	La Paz	Alcaldía Municipal San Luis Talpa	1	11 a 50	11302
16	San Salvador	Alcaldía Municipal de San Marcos	4	51 a 200	63209
17	San Salvador	Alcaldía Municipal de Santo Tomas	1	11 a 50	25344
18	San Salvador	Alcaldía Municipal de Tonacatepeque	1	11 a 50	90896
19	San Salvador	Alcaldía Municipal de Aguilares	1	11 a 50	21267
20	San Salvador	Alcaldía Municipal de San Martin	2	51 a 200	72758

No	Departamento	Municipio	Edificaciones Interconectadas	Cantidad de computadoras	Población con DUI
21	San Salvador	Alcaldía Municipal de San Salvador	más de 4	más de 200	316090
22	San Salvador	Alcaldía Municipal de Soyapango	más de 4	más de 200	241403
23	San Vicente	Alcaldía Municipal de Tepetitán	1	11 a 50	N/R
24	San Vicente	Alcaldía Municipal de San Esteban Catarina	1	menos de 10	2932
25	Usulután	Alcaldía Municipal de San Dionisio	N/R	11 a 50	4945
26	Usulután	Alcaldía Municipal de Usulután	1	51 a 200	73064
27	Usulután	Alcaldía Municipal Ciudad Puerto El Triunfo	1	11 a 50	16584
28	Usulután	Alcaldía Municipal de El Triunfo	1	11 a 50	6924
29	Usulután	Alcaldía Municipal de Jiquilisco	1	11 a 50	47784

Tabla 5: Listado de Municipios participantes de la encuesta según Departamentos de El Salvador

Los resultados obtenidos mediante la captura de la información por medio del cuestionario estructurado se registraron de la siguiente manera:

5.1 Tabulación de los Datos de Clasificación

A. EDIFICACIONES INTERCONECTADAS

¿Con cuántas edificaciones interconectadas en red LAN cuenta la alcaldía?

- Un solo Distrito
- Dos Distritos
- Tres Distritos
- Cuatro Distritos
- Más de 4 Distritos
- N/R

a) Objetivo:

Identificar la cantidad de edificaciones con que cuenta cada alcaldía para catalogarla según tamaño.

b) Tabulación de datos:

Categoría de clasificación a utilizar.

B. CANTIDAD DE COMPUTADORAS

¿Con cuántas computadoras aproximadamente cuenta la municipalidad?

- Menor o igual a 10
- De 11 a 50
- De 51 a 200
- Más de 200
- N/R

a) Objetivo:

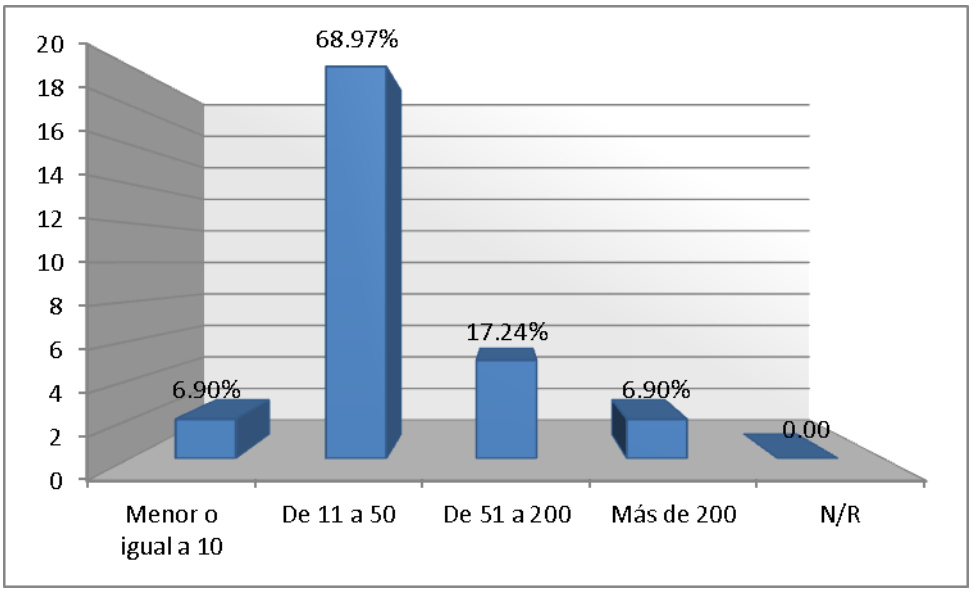
Conocer el promedio de dispositivos host que posee cada una de las municipalidades encuestadas.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Menor o igual a 10	2	9.52%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	2	6.90%
De 11 a 50	17	80.95%	1	50.00%	0	0.00%	0	0.00%	0	0.00%	2	100.00%	20	68.97%
De 51 a 200	2	9.52%	1	50.00%	0	0.00%	1	100.00%	1	33.33%	0	0.00%	5	17.24%
Más de 200	0	0.00%	0	0.00%	0	0.00%	0	0.00%	2	66.67%	0	0.00%	2	6.90%
N/R	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 6: Número de computadoras por alcaldía.

c) Representación Gráfica:



Gráfica 1: Número de computadoras por alcaldía.

C. SISTEMA OPERATIVO DE SERVIDORES

¿Qué sistema operativo utiliza la mayoría de los servidores institucionales?

- Linux
- Unix
- Mac OS
- Windows
- N/R

a) Objetivo:

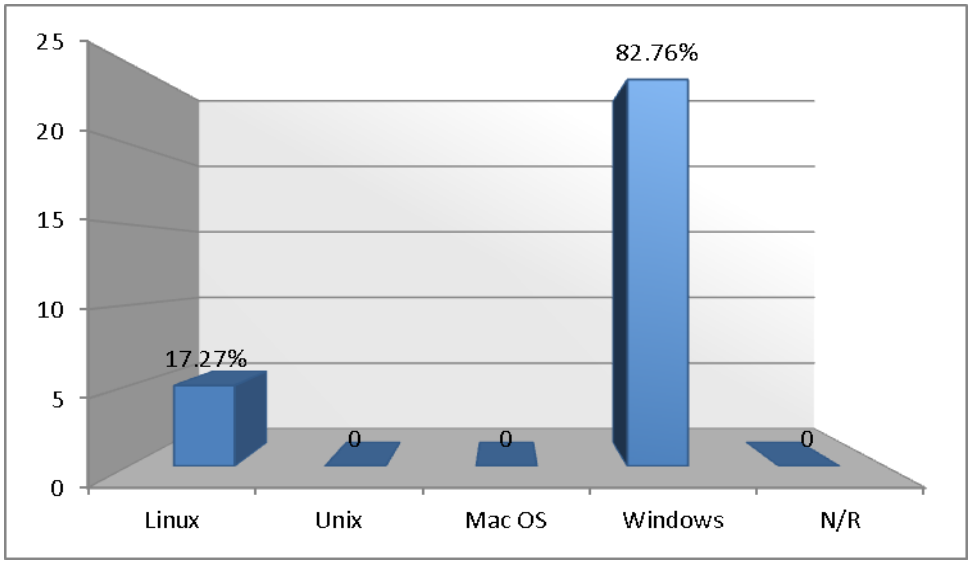
Conocer bajo que plataforma se encuentran operando los servidores institucionales para desarrollar propuestas a partir del más frecuente.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Linux	3	14.29%	1	50.00%	0	0.00%	0	0.00%	1	33.33%	0	0.00%	5	17.24%
Unix	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Mac OS	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Windows	18	85.71%	1	50.00%	0	0.00%	1	100.00%	2	66.67%	2	100.00%	24	82.76%
N/R	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 7: SO predomínate en los servidores.

c) Representación Gráfica:



Gráfica 2: SO predomínate en los servidores.

D. SISTEMA OPERATIVO DE LOS TERMINALES

¿Qué sistema operativo utiliza la mayoría de los terminales (computadoras) de la comuna?

- Linux
- Unix
- Mac OS
- Windows
- N/R

a) Objetivo:

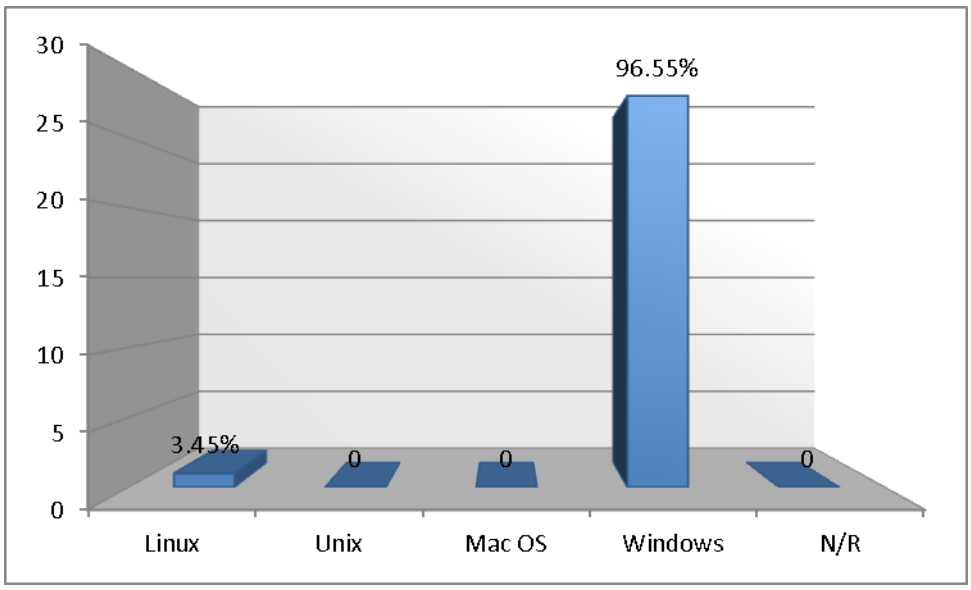
Conocer el SO bajo el cual operan los terminales del gobierno local.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Linux	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	33.33%	0	0.00%	1	3.45%
Unix	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Mac OS	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Windows	21	100.00%	2	100.00%	0	0.00%	1	100.00%	2	66.67%	2	100.00%	28	96.55%
N/R	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 8: SO predomínate en terminales.

c) Representación Gráfica:



Gráfica 3: SO predomínate en terminales.

E. GRADO ACADÉMICO

En el área informática. ¿Cuál es el último grado académico obtenido por el encargado de TI de la alcaldía?

- Estudiante
- Técnico
- Universitario
- Postgrado
- Maestría
- N/R

a) Objetivo:

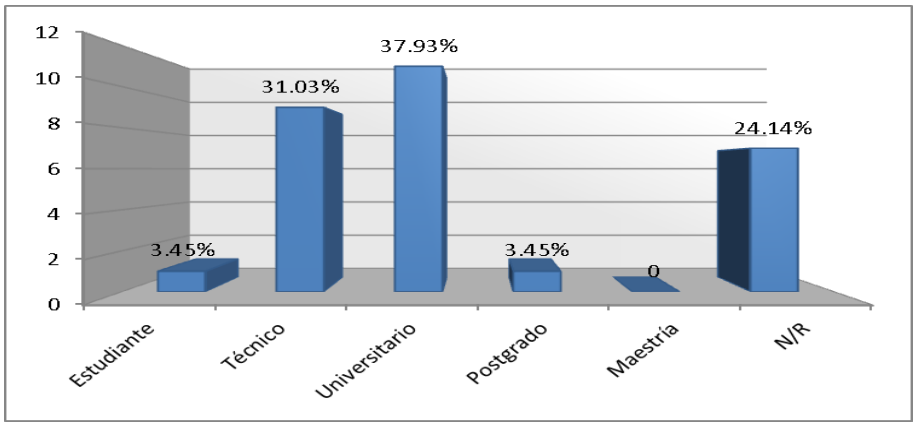
Conocer el Grado académico alcanzado por la persona que dirige la unidad TI del gobierno municipal.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Estudiante	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Técnico	8	38.10%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	50.00%	9	31.03%
Universitario	4	19.05%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	1	50.00%	11	37.93%
Postgrado	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Maestría	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
N/R	7	33.33%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	7	24.14%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 9: Grado académico de los encargados TI.

c) Representación Gráfica:



Gráfica 4: Grado académico de los encargados TI.

Análisis de resultados:

Se observa que 24.14% de los participantes de la muestra se abstuvieron de responder a la pregunta. Ante lo cual habría que dar un seguimiento a través de RRHH para analizar los atestados de la persona designada y verificar si cumple con los requisitos del puesto de trabajo exigido. De incumplir estos habría que evaluar la reasignación de dicho personal a áreas donde pueda aplicar de mejor manera sus competencias.

5.2 Tabulación del cuestionario

PREGUNTA 1.

¿En su experiencia laboral dentro de esta institución conoce de situaciones que hayan comprometido y puesto bajo riesgo la seguridad de la información que se encuentra almacenada y/o que es transmitida a través de la infraestructura de red LAN de la alcaldía?

- Si
- No
- N/R

a) Objetivo:

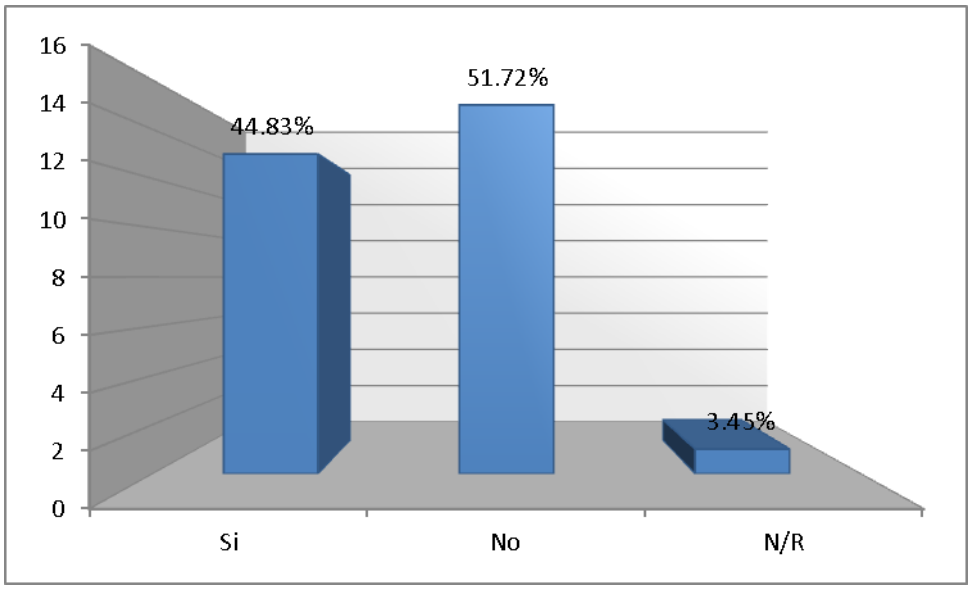
Verificar si el entrevistado conoce de situaciones impropias que haya permitido corromper, alterar y afectar la INTEGRIDAD de la información que dentro de la alcaldía se administra.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Si	8	38.10%	1	50.00%	0	0.00%	1	100.00%	2	66.67%	1	50.00%	13	44.83%
No	12	57.14%	1	50.00%	0	0.00%	0	0.00%	1	33.33%	1	50.00%	15	51.72%
N/R	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 10: Tabulación pregunta 1.

c) Representación Gráfica:



Gráfica 5: Representación gráfica de la pregunta 1.

d) Análisis de resultados:

Se observa que en general más de la mitad de los participantes de la encuesta (aproximadamente 52%) expresa desconocer que, dentro de la alcaldía para la cual laboran, la data almacenada y/o que es transmitida a través de la LAN de la institución se ha encontrado expuesta a eventos que afecten la buena operatividad de la misma. De lo anterior podrían inferirse dos situaciones: La primera; que la alcaldía haya sido objeto de situaciones que comprometieron la seguridad y que los encargados de TI no se hayan enterado y la segunda; que la integridad de la data trasferida a través de la infraestructura de red jamás haya sido objeto de algún acto comprometedor.

PREGUNTA 2.

¿Tiene usted conocimiento si la disponibilidad de la información digital que la alcaldía administra ha sufrido interrupciones, demoras o es inaccesible debido a actos vandálicos generados como denegación de servicio (DoS) que haya ocasionado paralizar operaciones?

- Si
- No
- N/R

a) Objetivo:

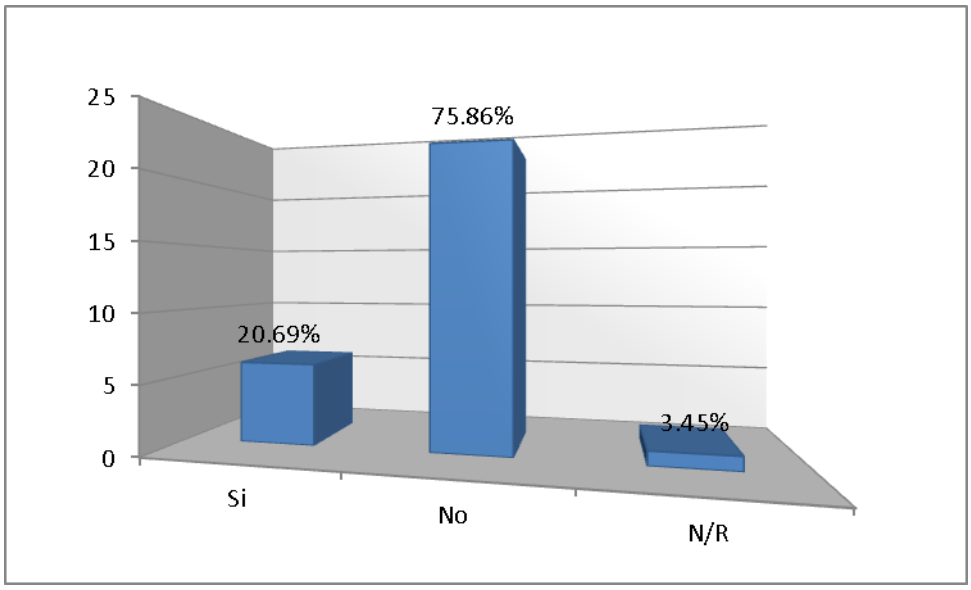
Indagara si la alcaldía ha sufrido actos generados por manipulaciones o ataques masivos indeseados de denegación de servicios (DoS) que hayan afectado la DISPONIBILIDAD de la data que es ofrecida a través de la RED de la institución.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Si	4	19.05%	1	50.00%	0	0.00%	0	0.00%	1	33.33%	0	0.00%	6	20.69%
No	17	80.95%	0	0.00%	0	0.00%	1	100.00%	2	66.67%	2	100.00%	22	75.86%
N/R	0	0.00%	1	50.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 11: Tabulación pregunta 2.

c) Representación Gráfica:



Gráfica 6: Representación gráfica de la pregunta 2.

d) Análisis de resultados:

Se observa que en general la gran mayoría de la población entrevistada (aproximadamente 76%) expresa que la disponibilidad de la información ofrecida a través de la red LAN de la comuna para la cual trabajan, jamás ha visto afectada sus operaciones debido a actos vandálicos informáticos.

PREGUNTA 3.

En el entendido que a la técnica de enmascaramiento de una Dirección MAC en un dispositivo de red se le conoce como suplantación de MAC (MAC spoofing) ¿Ha experimentado si en esta institución se ha comprobado actos de suplantación de identidad por parte de algún computador que intente interceptar, almacenar o transmitir información no autorizada través de la red LAN de la alcaldía?

- Si
- No
- N/R

a) Objetivo:

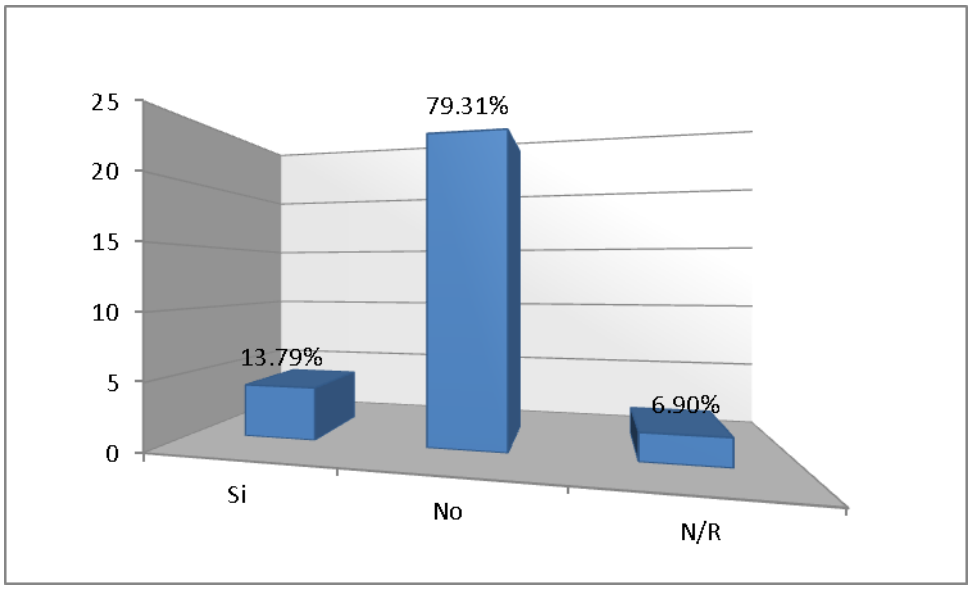
Investigar si el gobierno municipal ha sido objeto de alteraciones o cambios en la dirección de la interfaz de Control de Acceso al Medio (MAC) mediante la suplantación de algún dispositivo que permita poner en riesgo la AUTENTICIDAD de la información administrada.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Si	2	9.52%	1	50.00%	0	0.00%	0	0.00%	1	33.33%	0	0.00%	4	13.79%
No	17	80.95%	1	50.00%	0	0.00%	1	100.00%	2	66.67%	2	100.00%	23	79.31%
N/R	2	9.52%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	2	6.90%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 12: Tabulación pregunta 3.

c) Representación Gráfica:



Gráfica 7: Representación gráfica de la pregunta 3.

d) Análisis de resultados:

Se evidencia que la mayoría de las alcaldías (casi un 80%) expresan nunca haber comprobado si en algún momento los host institucionales han sido objeto de suplantación MAC.

PREGUNTA 4.

¿La información o data que la alcaldía administra es resguardada de manera segura y solo es accedida por el personal debidamente autorizado?

- Si
- No
- N/R

a) Objetivo:

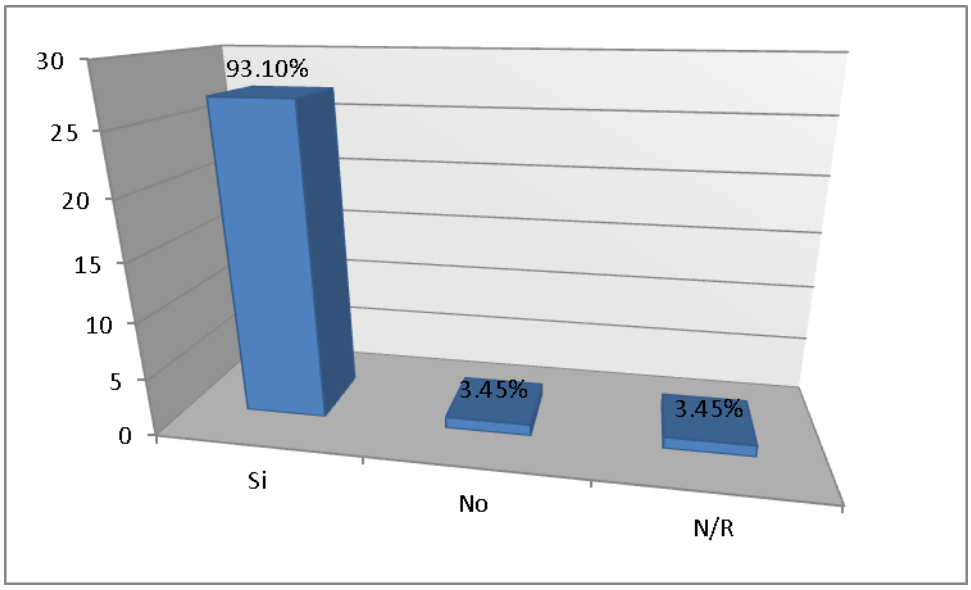
Indagar si la alcaldía posee controles para mantener la CONFIDENCIALIDAD de la información digital institucional.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Si	19	90.48%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	27	93.10%
No	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
N/R	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 13: Tabulación pregunta 4.

c) Representación Gráfica:



Gráfica 8: Representación gráfica de la pregunta 4. .

d) Análisis de resultados:

Más del 93 por ciento de los encargados TI entrevistados aseguran que la información digital administrada permanece confidencial y solo es accedida por la persona autorizada.

PREGUNTA 5. (Pregunta abierta)

¿Podrían mencionar algún malware (virus, gusano, troyano, rootkits, scareware, spyware, crimeware) o cualquier otro código malicioso que haya infectado o afectado las operaciones institucionales?

a) Objetivo:

Conocer los nombres de aquellos malware que tecnológicamente han afectado y/o interferido con las normales las actividades de los gobiernos municipales.

b) Tabulación de datos:

Las respuestas fueron catalogadas de acuerdo al número de veces que aparecieron en la encuesta.

Malware (***Xi***)	**Numero de apariciones** (**Frecuencia absoluta *fi***)	(**Porcentaje %**)
Virus Skype	1	3.45%
Virus no especificados	1	3.45%
Virus autorun.inf	1	3.45%
Troyano CryptoLocker /CTB-Locker	2	6.89%
Troyanos no especificados	3	10.34%
Spyware no especificado	1	3.45%
N/R	20	68.97%
Total	**29**	**100%**

Tabla 14: Tabulación pregunta 5.
Tabla de frecuencia sobre códigos maliciosos que han afectado las Alcaldías de El Salvador.

d) Análisis de resultados:

Solo el 31% de los participantes mencionaron haber sufrido los efectos nocivos ocasionados por algún malware (de ellos los troyanos parecen ser los de mayor impacto).

Es de hacer notar que casi el 69% de la población participante de la muestra se abstuvo de mencionar si en algún momento algún código malicioso haya infectado o afectado las operaciones de la alcaldía. Ante ello pueden inferirse múltiples posibilidades, entre las que se pueden enunciar:

1. Que nunca hayan sufrido alguna amenaza seria que los obligue a desinfectar los equipos afectados.
2. Que de haber sido afectados, los antivirus hicieron su trabajo y ante la ausencia de controles no se registró la afectación.
3. Que ante la ausencia de herramientas de monitoreo que rastreen intrusiones y generen la alerta, podrían haber sido infectados y la unidad TI jamás detecto la amenaza.
4. Que de haber sido afectados mantengan bajo reserva dicho evento.

PREGUNTA 6.

¿Su institución o alcaldía cuenta con el apoyo de un Equipo de Respuestas a Incidentes de Seguridad de Computadores o en Inglés Computer Security Incident Response Team (CSIRT). Que le colabore en la prevención y respuesta ante incidentes de seguridad informática?

- Si
- No
- N/R

a) Objetivo:

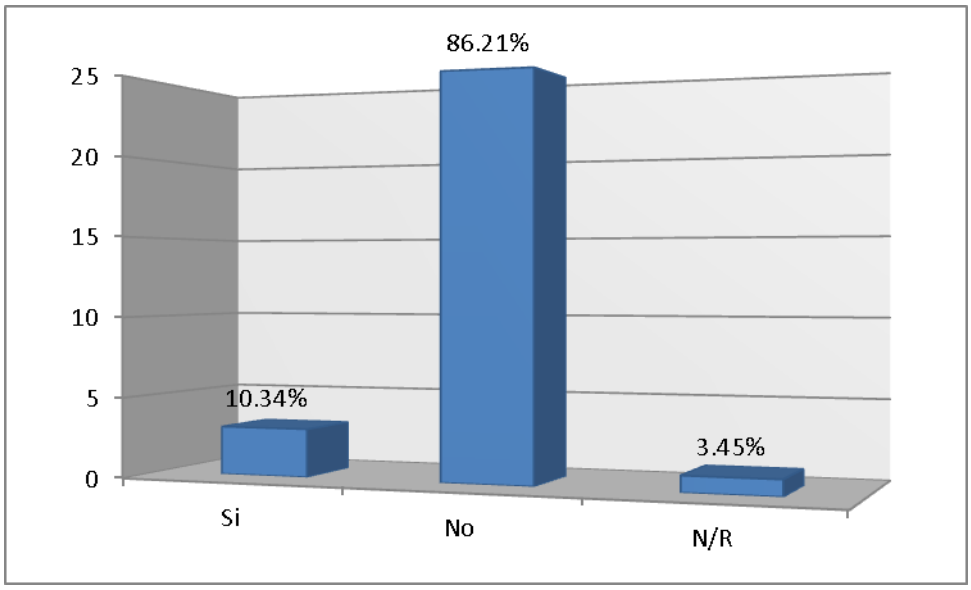
Conocer si la institución cuenta con el apoyo de un CSIRT al cual pueda acudir o sobre el cual pueda apoyarse para la ejecución y coordinación que le permita reaccionar ante incidentes o amenazas a la seguridad informática reportados.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Si	3	14.29%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	3	10.34%
No	17	80.95%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	25	86.21%
N/R	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 15: Tabulación pregunta 6.

c) Representación Gráfica:



Gráfica 9: Representación gráfica de la pregunta 6.

d) Análisis de resultados:

El 87% (la gran mayoría) de las instituciones participante de la encuesta expresan carecer de el apoyo de un equipo de respuesta a incidentes informáticos. Situación que evidencia una vulnerabilidad para reaccionar a solventar situaciones críticas una vez las catástrofes informáticas se hayan suscitado.

PREGUNTA 7.

¿Considera usted necesaria la creación de un Centro de Respuesta a Incidentes de Seguridad Informática a nivel nacional, el cual aglutine a múltiples instituciones públicas y municipales, que registre y recopile fallas reportadas por los asociados, para el establecimiento de soluciones comunes desde donde además se administre y generen directrices o parámetros de cómo deben las alcaldías reaccionar ante percances informáticos, al cual también puedan acudir para solicitar apoyo en caso de incidentes?

- Muy de acuerdo
- De acuerdo
- Me es indiferente
- En desacuerdo
- N/R

a) Objetivo:

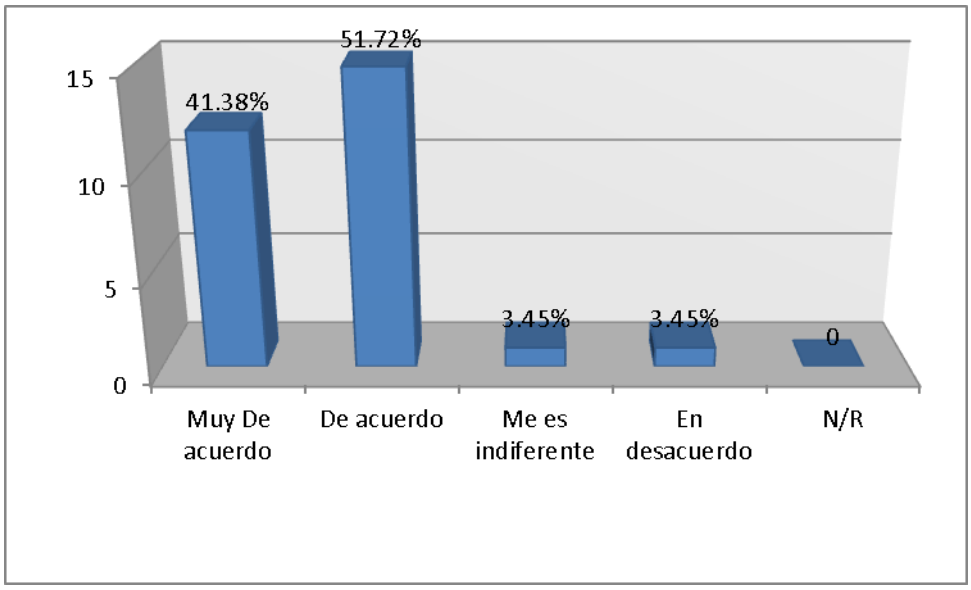
Verificar si los encargados de TI aceptarían la sugerencia de la creación de un Instituto de reacción y respuesta a incidentes de computadores ante desastres informáticos.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Muy De acuerdo	8	38.10%	1	50.00%	0	0.00%	0	0.00%	2	66.67%	1	50.00%	12	41.38%
De acuerdo	11	52.38%	1	50.00%	0	0.00%	1	100.00%	1	33.33%	1	50.00%	15	51.72%
Me es indiferente	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
En desacuerdo	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
N/R	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 16: Tabulación pregunta 7.

c) Representación Gráfica:



Gráfica 10: Representación gráfica de la pregunta 7. [10]

d) Análisis de resultados:

Más del 90% de los participantes de la encuesta (si se toman en cuenta las opciones combinadas de “Muy de acuerdo” junto a “De acuerdo”) aprueban la creación de un organismo que se encargue de proponer soluciones tecnológicas a percances informáticos surgidos en los gobiernos municipales.

PREGUNTA 8.

¿De las siguientes herramientas de seguridad informática con cuales cuenta la alcaldía?

- Sistema de detección de intrusos o IDS
- Sistema de prevención de intrusos o IPS
- Cortafuegos o Firewall lógico (software)
- Cortafuegos o Firewall físico (hardware)
- Zona Desmilitarizada o DMZ
- Antivirus por pc
- Firewall por pc
- N/R

a) Objetivo:

Identificar que herramientas utiliza la alcaldía para afrontar actos que intenten afectar la seguridad informática de la institución.

b) Tabulación de datos:

Las respuestas fueron catalogadas de acuerdo al número de veces que fueron seleccionadas por los participantes de la encuesta.

Herramienta/Aplicación de seguridad (*Xi*)	**Numero de apariciones (Frecuencia absoluta *fi*)**	**% Basado en 29 participantes**
Sistema de detección de intrusos o IDS	4	13.79%
Sistema de prevención de intrusos o IPS	4	13.79%
Cortafuegos o Firewall lógico (software)	10	34.48%
Cortafuegos o Firewall físico (hardware)	10	34.48%
Zona Desmilitarizada o DMZ	3	10.34%
Antivirus por pc	25	86.20%
Firewall por pc	12	41.37
N/R	3	10.34

Tabla 17: Tabulación pregunta 8.
Tabla de frecuencia sobre herramientas o aplicaciones de seguridad
Instaladas en los gobiernos Municipales de El Salvador.

d) Análisis de resultados:

Se evidencia que la mayoría de las Alcaldías de El Salvador enfilan todos sus esfuerzos en asegurar su infraestructura de red al decantarse por utilizar Firewall Físicos y/o lógicos (utilizados por aproximadamente el 35% de los encuestados). Declinando casi en su totalidad de utilizar herramientas que monitoricen el tráfico de los paquetes que circulan a través de la LAN (Utilizados por únicamente el 14%). Al mismo tiempo los equipos informáticos son protegidos mayormente por antivirus (87% de las comunas expresaron utilizarlo) y en menor escala por firewall personales (41%). También se evidencia que casi el 90% de las instituciones carecen de la utilización de propuestas de seguridad como son las DMZ.

PREGUNTA 9

¿La configuración de las anteriores herramienta está a cargo del personal del área de informática de la alcaldía o es contratada a un agente externo calificado. Mediante por ejemplo Acuerdos de Nivel de Servicio o similares?

- Las configuraciones son totalmente realizadas por personal TI de la alcaldía.
- Las configuraciones son parcialmente realizadas por personal TI de la alcaldía
- Las configuraciones son contratadas a personal externo calificado.
- N/R

a) Objetivo:

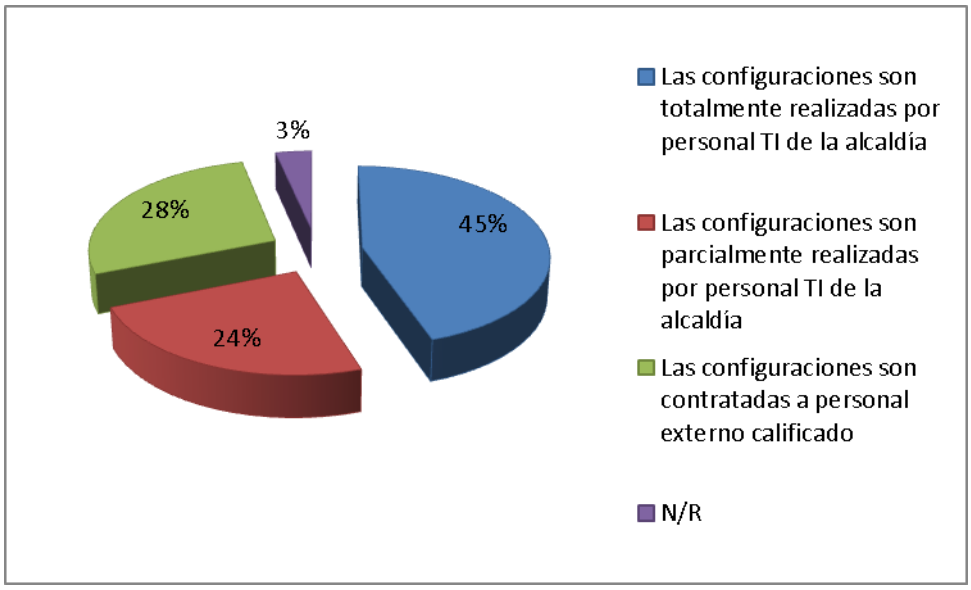
Verificar si la alcaldía cuenta con asistencia técnica externa calificada (outsorsing) que le colabore, apoye y asista en la configuración de dispositivos de seguridad de redes informáticas.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Las configuraciones son totalmente realizadas por personal TI de la alcaldía	11	52.38%	2	100.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	13	44.83%
Las configuraciones son parcialmente realizadas por personal TI de la alcaldía	2	9.52%	0	0.00%	0	0.00%	1	100.00%	3	100.00%	1	50.00%	7	24.14%
Las configuraciones son contratadas a personal externo calificado	7	33.33%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	50.00%	8	27.59%
N/R	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 18: Tabulación pregunta 9.

c) Representación Gráfica:



Gráfica 11: Representación gráfica de la pregunta 9..

d) Análisis de Resultados

De las opciones propuestas se puede comprobar que menos de la mitad de los Gobiernos Municipales (45 %) cuentan con su propia planta de personal TI a cargo de las configuraciones de los dispositivos y herramientas de seguridad lo que implica que más de la mitad (52%) de las Alcaldías sub-contratan los servicios a agentes externos calificados.

PREGUNTA 10

¿El Consejo Municipal participa de los planes de seguridad informática?

- Siempre
- Casi siempre
- En ocasiones
- Nunca
- N/R

a) Objetivo:

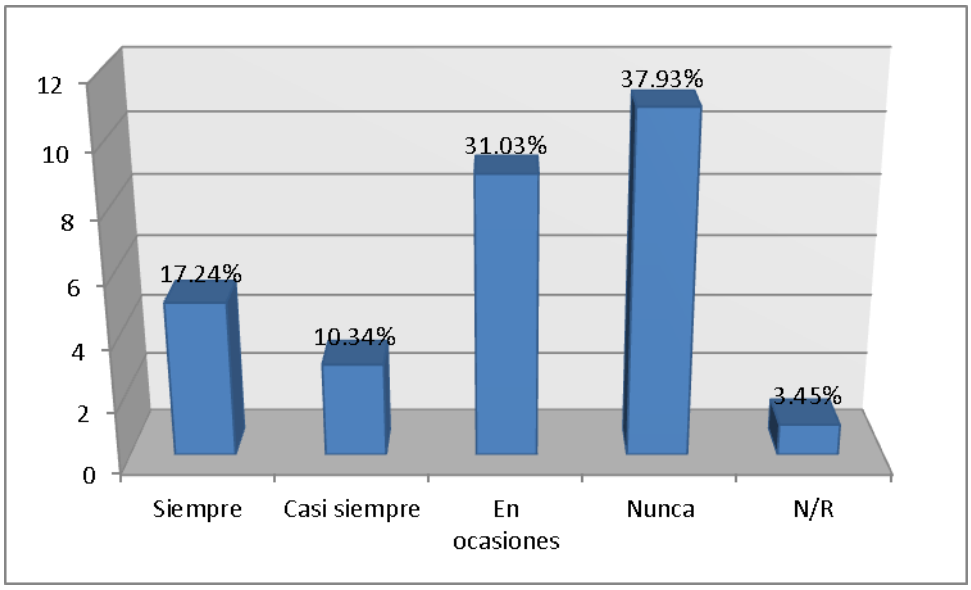
Establecer el nivel de participación que la alta gerencia de la alcaldía tiene sobre la creación de políticas de seguridad informática.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Siempre	4	19.05%	1	50.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	5	17.24%
Casi siempre	3	14.29%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	3	10.34%
En ocasiones	6	28.57%	1	50.00%	0	0.00%	1	100.00%	1	33.33%	0	0.00%	9	31.03%
Nunca	8	38.10%	0	0.00%	0	0.00%	0	0.00%	2	66.67%	1	50.00%	11	37.93%
N/R	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	50.00%	1	3.45%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 19: Tabulación pregunta 10. [19]

c) Representación Gráfica:



Gráfica 12: Representación gráfica de la pregunta 10.

d) Análisis de Resultados

Al evaluar los resultados se puede establecer que el 69% (si se toman en cuenta las opciones combinadas de “En ocasiones” junto a “Nunca”) de los Consejos Municipales muestra cierto desintereses o apatía en involucrarse en la planificación de los procesos necesarios para asegurar los activos informáticos.

PREGUNTA 11

¿Dispone el departamento TI o la unidad encargada de una partida de fondos destinada a la inversión en dispositivos o herramientas de seguridad informática?

- Siempre
- Casi siempre
- En ocasiones
- Nunca
- N/R

a) Objetivo:

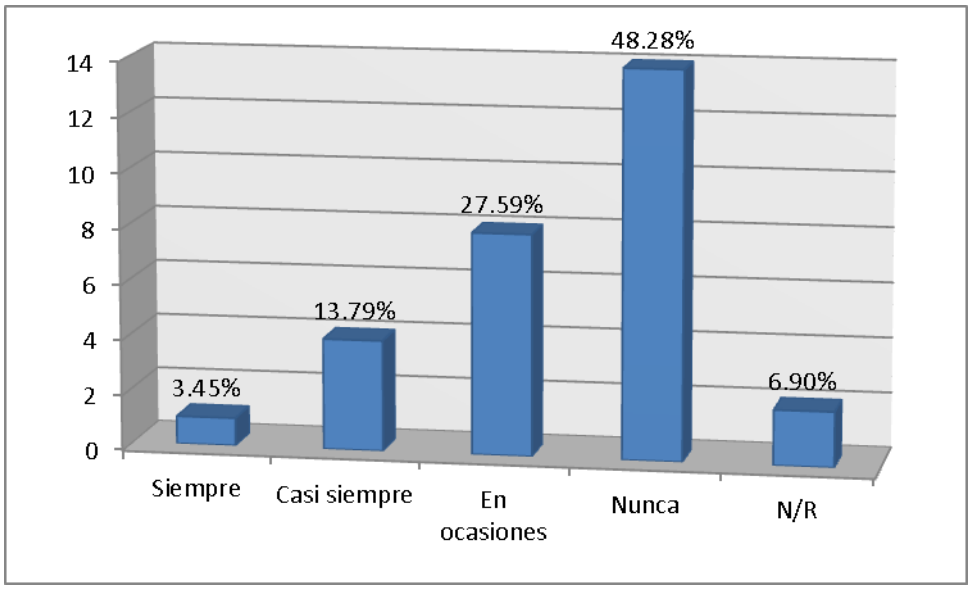
Conocer el grado de concientización que la alta gerencia tiene sobre la necesidad de inversión en dispositivos o herramientas de seguridad informática.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Siempre	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
Casi siempre	3	14.29%	0	0.00%	0	0.00%	1	100.00%	0	0.00%	0	0.00%	4	13.79%
En ocasiones	5	23.81%	1	50.00%	0	0.00%	0	0.00%	2	66.67%	0	0.00%	8	27.59%
Nunca	11	52.38%	1	50.00%	0	0.00%	0	0.00%	1	33.33%	1	50.00%	14	48.28%
N/R	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	50.00%	2	6.90%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 20: Tabulación pregunta 11.

c) Representación Gráfica:



Gráfica 13: Representación gráfica de la pregunta 11.

d) Análisis de Resultados

Según los resultados obtenidos; el aporte financiero recibido por parte de las Alcaldías para apoyar la seguridad informática es medianamente aceptable ya que según la percepción de la mayoría de los participantes de la encuesta escasamente cuentan con fondos para invertir en dispositivos o herramientas de seguridad informática.

PREGUNTA 12

¿Dispone el departamento o unidad TI de un manual de políticas de seguridad de la información que forme parte de la cultura organizacional de la alcaldía donde se plasmen la hoja de ruta o el plan de acción o los protocolos a seguir para minimizar amenazas a la red y proteger los activos informáticos institucionales?

- Ya se tiene el manual
- Se está desarrollando dicho manual.
- Se está planificando la elaboración de dicho manual.
- Se ha propuesto la elaboración del mencionado manual.
- N/R

a) Objetivo:

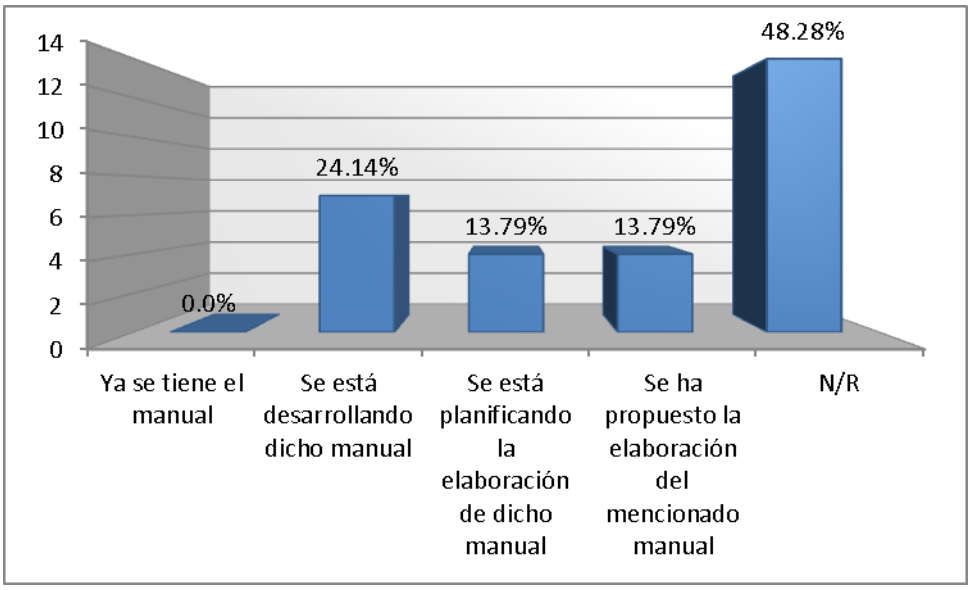
Verificar si la comuna posee un manual de políticas para la administración de los activos informáticos institucionales.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Ya se tiene el manual	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Se está desarrollando dicho manual	4	19.05%	1	50.00%	0	0.00%	1	100.00%	1	33.33%	0	0.00%	7	24.14%
Se está planificando la elaboración de dicho manual	3	14.29%	1	50.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	4	13.79%
Se ha propuesto la elaboración del mencionado manual	3	14.29%	0	0.00%	0	0.00%	0	0.00%	1	33.33%	0	0.00%	4	13.79%
N/R	11	52.38%	0	0.00%	0	0.00%	0	0.00%	1	33.33%	2	100.00%	14	48.28%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 21: Tabulación pregunta 12. [21]

c) Representación Gráfica:



Gráfica 14: Representación gráfica de la pregunta 12.

d) Análisis de Resultados

Se evidencia que la totalidad de las alcaldías de El Salvador carecen de un manual que establezca las políticas informáticas a aplicar para el apropiado resguardo de los activos informáticos y la protección en la transmisión de los mismos.

PREGUNTA 13

¿Si existiera una propuesta para el desarrollo de políticas de seguridad informática que colabore con los Gobiernos Municipales de El Salvador en el establecimiento de una infraestructura de red segura que cumpla con un marco de trabajo establecido por las mejores prácticas en materia de seguridad informática?

¿Usted lo implementaría?

- Si
- No
- N/R

a) Objetivo:

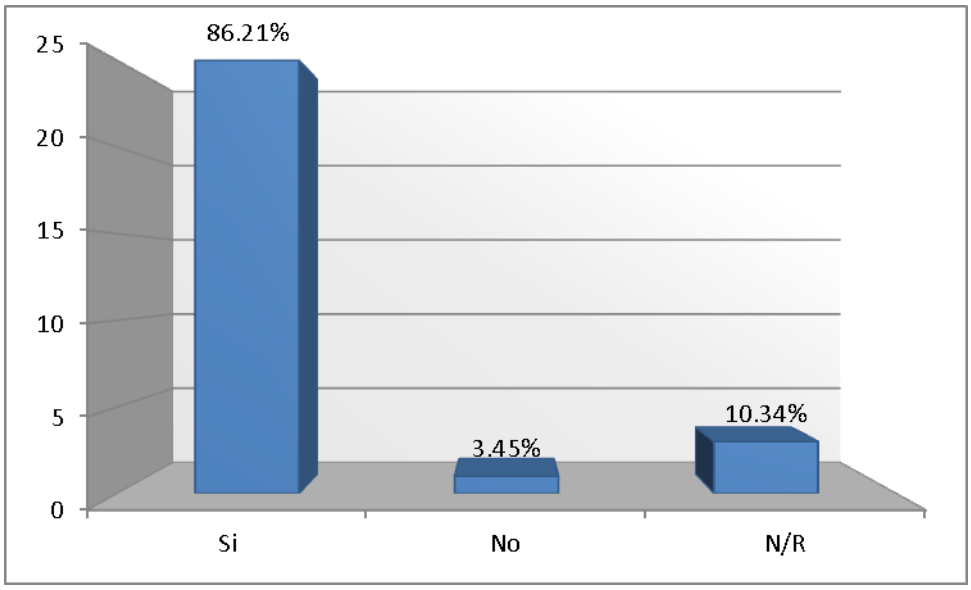
Conocer el porcentaje de alcaldías dispuestas implementar un manual de políticas para la administración de los activos informáticos institucionales.

b) Tabulación de datos:

	Un solo Distrito		Dos Distritos		Tres Distritos		Cuatro Distritos		Más de 4 Distritos		N/R		Total	
Respuestas	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**
Si	19	90.48%	1	50.00%	0	0.00%	1	100.00%	3	100.00%	1	50.00%	25	86.21%
No	1	4.76%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	1	3.45%
N/R	1	4.76%	1	50.00%	0	0.00%	0	0.00%	0	0.00%	1	50.00%	3	10.34%
Totales	21	100.00%	2	100.00%	0	0.00%	1	100.00%	3	100.00%	2	100.00%	29	100.00%

Tabla 22: Tabulación pregunta 13.

c) Representación Gráfica:



Gráfica 15: Representación gráfica de la pregunta 13.

d) Análisis de Resultados

Más del 85% por ciento de las encargados TI de los gobiernos municipales encuestados, confirma que implementarían un manual de políticas de seguridad en redes informáticas, aplicando las mejores prácticas.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Al hacer un análisis del número de edificaciones interconectadas que componen las alcaldías de El Salvador, se puede comprobar que la gran mayoría (72%) poseen un solo distrito, situación beneficiosa para el establecimiento de una infraestructura de red segura, debido a que los esfuerzos para el control de los dispositivos internos que acceden a la red local de la institución se focalizan en un área reducida (un solo edificio) lo que implica menor inversión. Aunque es de hacer notar que apenas el 19% de las comunas que poseen un solo distrito suelen invertir de manera frecuente en dispositivos y herramientas de seguridad.

- Se puede verificar que al menos el 44% de las alcaldías de El Salvador han sido objeto de incidentes que han expuesto y comprometido la seguridad de la información digital que administran. Lo cual evidencia una vulnerabilidad en la **integridad** de la data que se encuentra bajo su resguardo**.** En lo referente a la **disponibilidad** de la data que los gobiernos municipales ofrecen a través de la infraestructura de red institucional, puede afirmarse que en escasas ocasiones esta se ha visto afectada; lo que implica un aspecto positivo a considerar debido a que, al parecer, hasta el presente las operaciones no han sido interrumpidas por actos indebidos. Otros dos aspectos importantes a distinguir es que en la práctica, la mayoría de los participantes de la encuesta mencionan jamás haber experimentado actos de suplantación de identidad que manipulen la **autenticidad** de la información institucional. Al mismo tiempo, también declaran que la **confidencialidad** de la información digital de la comuna es resguardada de manera segura y sólo es accedida por el personal debidamente autorizado. Sin embargo ante la ausencia de controles y de dispositivos de monitoreo que rastreen intrusiones, resulta prematuro

afirmar que en la red informática nunca se han experimentado actos de suplantación de identidad, ni que la data solo sea accedida por personal autorizado.

- Se puede concluir que el involucramiento del Consejo Municipal de la mayoría de los gobiernos locales de El Salvador en el desarrollo de políticas, y el establecimiento de controles de seguridad informática es reducido, dicha situación puede afectar la puesta en marcha de cualquier plan de acción orientado a mitigar o reducir amenazas dentro de la red LAN institucional. Aunado a lo anterior, la participación financiera que es destinada a la inversión en dispositivos o herramientas de seguridad, y la ausencia de contactos con especialistas externos certificados en seguridad informática (que formen parte de un equipo CSIRT) que autentiquen procesos, apoyen y colaboren con los departamentos o unidades TI en la prevención y respuesta ante incidentes es limitado. El anterior escenario dificulta la posibilidad de mantener una infraestructura de red estable, segura y saludable; lo cual no garantiza el apropiado resguardo de los activos informáticos institucionales.

- Se pudo comprobar que gran parte de los administradores TI a cargo del área informática de los Gobiernos Municipales, comprenden la necesidad de disponer de un manual de políticas de seguridad de la información que forme parte de la cultura organizacional de las alcaldías, donde se establezcan las acciones a tomar para minimizar amenazas a la red y proteger los activos informáticos institucionales; y confirmaron que si existiere una propuesta para el desarrollo de políticas de seguridad informática que colabore con los Gobiernos Municipales de El Salvador en el establecimiento de una infraestructura de red segura, que cumpla con un marco de trabajo establecido por las mejores prácticas en materia de seguridad informática, harían uso de este y lo implementarían.

6.2 Recomendaciones

- Para el presente estudio se propone categorizar las alcaldías de El Salvador en 3 niveles considerando los parámetros de número de computadora y número de edificaciones interconectadas a la red LAN

  Por su Tamaño

  - Pequeñas: Las que tienen hasta 2 Distritos conectados a la red LAN y que poseen un número máximo de 50 computadoras.
  - Medianas: Las que cuentan con 3 ó 4 Distritos interconectados entre sí y cuentan con hasta 200 computadoras.
  - Grandes: Las que cuentan con más de 4 Distritos interconectados y poseen más de 200 computadores.

- Valorar y direccionar los esfuerzos para que los departamentos o unidades TI de las municipalidades implementen más herramientas de verificación y monitoreo en tiempo real, que permitan controlar el tráfico de paquetes que circulan a través de la red LAN, a fin de minimizar incidentes indeseados y evitar interrupciones en el servicio. Permitiendo de esta manera que la información sea accesible cuando se necesite y se preserve la confidencialidad e integridad de los datos junto a la privacidad de los usuarios. Lo anterior generaría un posible incremento en la percepción de los ciudadanos respecto a la calidad del servicio ofrecidos; permitiendo de esta manera alinear la tecnología con el negocio al poner especial énfasis en blindar la información digital que es almacenada, resguardada y trasmitida dentro de las áreas más sensibles de la mayoría de las comunas, como son: El Registro del Estado Familiar (REF) y la Unidad de Administración Tributaria Municipal (UATM).

- Es imperioso que la alta gerencia se involucre de manera constante y participe en todo lo referente a seguridad informática, permitiendo con ello que toda propuesta de seguridad que se desee implementar cuente con el aval del consejo municipal, además deberán definirse políticas de seguimiento y control que verifiquen el cumplimiento de las normas propuestas. De la misma manera habrá de realizarse los esfuerzos necesarios que permitan invertir y erogar los fondos necesario para la adquisición de dispositivos y herramientas de seguridad que incrementen la protección de los activos digitales de las municipalidades. Y finalmente se deberán de establecer contactos con especialistas en seguridad informática de otros gobiernos municipales, profesionales externos certificados, agrupaciones, asociaciones, comités, foros de alerta temprana y equipos CSIRT a fin de asesorarse y mantenerse actualizado sobre la forma óptima de confrontar amenazas informáticas.

- Como una forma de contribuir al empeño que los departamentos TI de las comunas ponen para proteger y mantener segura la infraestructura de red de los Gobiernos Municipales, es preciso complementar dichos esfuerzos a través del desarrollo de un manual de políticas de seguridad que definan la hoja de ruta y el plan de acción que se habrá de seguir para afrontar y mitigar riesgos de seguridad, generados por amenazas a la red y que además proponga controles para mejorar la protección y resguardo de los activos informáticos institucionales. Lo anterior podría lograrse mediante el desarrollo de la PROPUESTA PARA EL ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD EN REDES INFORMÁTICAS, APLICANDO LAS MEJORES PRÁCTICAS PARA IMPLEMENTARSE EN LAS ALCALDÍAS DE EL SALVADOR.

CAPITULO VII: PROPUESTA

7.1 Diseño de la solución

En la tabla que se muestra a continuación se realiza una comparación entre varias opciones de buenas prácticas en materia de seguridad informática de entre la que se seleccionara aquella que servirá de fundamento para el desarrollo del manual de Políticas de Seguridad de la Información que este destinado a facilitar la entrega de servicios de tecnologías de la información y que más se acople a los fines del presente estudio.

Propuesta	**Certificación**
ITIL	Certificable a través de la ISO/IEC 20000. Establece exigencias Mínimas a cumplir y su implementación requiere personal certificado.
COBIT	Certificable a través de la ISO/IEC 15504 e ISO/IEC 38500. Establece exigencias Mínimas a cumplir y su implementación requiere personal certificado.
ISO/IEC 27001	Certificable a través de la ISO/IEC 27000. Establece exigencias Mínimas a cumplir y su implementación requiere personal certificado.
ISO/IEC 27002	No Certificable, es una guía de buenas prácticas. Recomienda los Máximos a cumplir, su implementación no requiere personal certificado.

Tabla 22: Tabla comparativa de propuestas de seguridad informática

La opción ISO/IEC 27002

Es la intención del presente estudio proponer una serie de controles que permitan a los gobiernos municipales de El Salvador involucrar a cada una de las unidades o departamentos que lo componen en el logro de los siguientes aspectos:

- La conformación de un Comité de Seguridad de la Información comprometido con la seguridad dentro de la comuna.
- La asignación de obligaciones y responsabilidades en materia de seguridad informática de todos los miembros dentro de la organización.
- La correcta gestión y apropiado resguardo de los activos informáticos institucionales.
- Establecer el control de accesos a sistemas y aplicaciones.
- Proponer controles sobre la forma adecuada de proteger la integridad física de las instalaciones.
- Asegurar la gestión de la seguridad en las redes de telecomunicaciones y otros dispositivos.

A fin de plasmar las directrices sobre el establecimiento de medidas de seguridad a instaurar en la red informática de la institución. Y siendo que La Normativa ISO/IEC 27001 es un Estándar Certificable y la ISO/IEC 27002 es un apéndice del anterior que funge como una guía, un código de buenas prácticas acorde a uno de los objetivos de este documento se ha seleccionado para el desarrollo del presente documento la normativa ISO/IEC 27002:2013 (versión más reciente).

ISO/IEC 27002 como un anexo de la ISO/IEC 27001

La siguiente imagen muestra la estructura que compone la ISO 27001 y como al final de la misma en el Anexo ‘’A” se enlista una serie de objetivos de control que engloba 114 controles pertenecientes a 14 dominios los cuales mantienen la misma denominación que los encontrados en la ISO 27002.

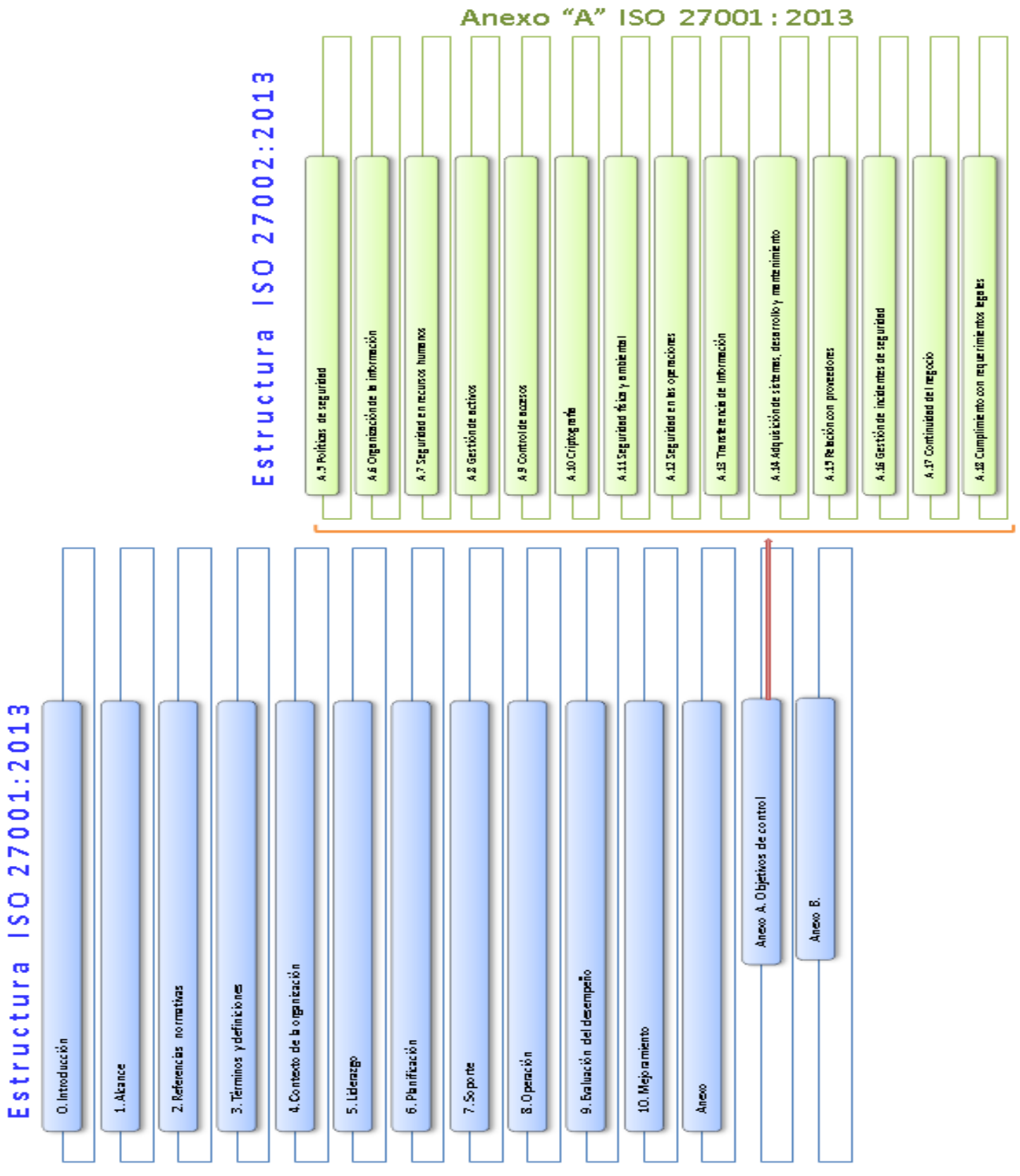


Diagrama 9: ISO/IEC 27002 como un anexo de la ISO/IEC 27001

7.2 Propuesta

Página dejada en blanco intencionalmente

POLÍTICAS DE SEGURIDAD

Normas de generales vigentes que deberán observarse en materia de seguridad de la información en la Alcaldía de *(nombre de la alcaldía)*

1. Sobre las políticas

1.1 Introducción

La disposición de una red informática debe estar orientada a soportar las irrupciones que pudieren generarse tanto desde el exterior como desde el interior de la misma; sean estos provocados o accidentales; para ello la información que es resguarda o es transmitida a través de la LAN perteneciente al gobierno municipal deberá cumplir con varios criterios, los cuales permitan que la data administrada logre la misión de mantener su integridad, disponibilidad, autenticidad y confidencialidad. En donde:

Integridad:

Es el proceso mediante el cual la información debe almacenarse y transmitirse a través de la red de forma incorrupta sin que esta haya sido objeto de alteraciones por parte de terceros, manteniendo sus dimensiones exactamente igual independientemente del tiempo y de la cantidad de veces que sea transmitida. Ejemplo: Bit Flipping es un ataque en el cual el atacante intercepta los mensajes transmitidos para realizar cambios en algunos bits del texto cifrado alterando así la data del criptograma

Disponibilidad:

Enuncia que la información debe estar disponible en el momento que sea requerida sin interrupción ni demora. Ejemplo: Denial of Services (DoS) en él; los dispositivos víctimas son inundados por una infinidad de mensajes, lo cual genera la negación de recursos y servicios a host legítimos

Autenticidad:

Determina que los objetos debe ser transmitidos, recibidos y almacenados sin que quepa la menor duda que son enviados y han sido administrados por quien debe ser.

Confidencialidad:

Implica que la información debe mantenerse resguardada y debe ser transmitida de manera segura y solo debe ser accedida por las personas autorizadas. Ejemplo: ARP Poisoning: Ataque que consiste en el envenenamiento de la tabla ARP.

Según lo anterior y con el propósito de asegurar los activos informáticos de la Alcaldía de *(nombre de la alcaldía)* se ha adoptado el presente manual de políticas de seguridad de la información enmarcados en un conjunto de prácticas recomendables. Las cuales combinan principios, prácticas y métodos de administración de cambios, administración de calidad, y mejora de capacidades; con el fin de promover la mejora continua de los servicios, los procesos, las actividades y tecnologías relacionadas.

1.2 Objetivos

- Proteger los activos informáticos de la Alcaldía mediante acciones que permitan minimizar amenazas con el objetivo que la data administrada logre la misión de mantener su integridad, disponibilidad, autenticidad y confidencialidad.
- Mantener las presentes políticas actualizadas, mediante revisiones periódicas y programadas a fin de adaptarlas a los cambios venideros.
- Establecer una cultura organizacional sobre seguridad informática de modo que todo el personal de la comuna conozca, sea capacitado y concientizado sobre la reglamentación establecida y los beneficios esperados al respetar la misma.

1.3 Limitaciones

El presente documento únicamente contempla los lineamientos que se deben de seguir dentro del gobierno municipal para proteger adecuadamente, mediante la aplicación de buenas prácticas, los activos tecnológicos y de la información de la Alcaldía de *(nombre de la alcaldía).* Se comprende que la implantación de las mismas no garantiza ni implica la fiabilidad del 100% de la seguridad de la infraestructura de red municipal.

1.4 Generalidades

Con el fin de salvaguardar y proteger los activos informáticos institucionales, la Alcaldía de *(nombre de la alcaldía)* ha adoptado el siguiente manual de políticas de seguridad con el propósito de plasmar los lineamientos que sirvan como base para el mantenimiento, mediante la gestión de la seguridad, de la información digital que es transmitida, administrada y almacenada dentro de la infraestructura de red LAN de la comuna. Ello alineado y acorde a estándares internacionales de buenas prácticas aplicadas a la seguridad de la información. En línea con lo anterior las presentes políticas toman como guía el listado de dominios ofrecidos por el código de buenas prácticas de seguridad de la información estándar ISO/IEC 27002:2013; siendo a partir de esa estructura que se consideran las siguientes clausulas, dominios o secciones:

Dominio o Sección: POLÍTICAS DE SEGURIDAD

Dominio: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Dominio: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Dominio: GESTIÓN DE ACTIVOS

Dominio: CONTROL DE ACCESOS

Dominio: CIFRADO

Dominio: SEGURIDAD FÍSICA Y AMBIENTAL

Dominio: SEGURIDAD OPERATIVA

Dominio: SEGURIDAD EN LAS TELECOMUNICACIONES

Dominio: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Dominio: GESTIÓN DE INCIDENTES

2. Términos y Consideraciones

2.1 Términos

Acuerdo de Nivel de Servicio (ANS): Contrato escrito entre un proveedor de servicio y su cliente.

Clausula o Dominio: Disposición de un contrato o ley que establece ciertas condiciones.

Control: Instrumento para la administración de riesgos, incluye procesos, políticas, directrices, estructuras organizacionales, las cuales pueden ser de índole administrativa, técnica, de gerencial o legal.

Comité de Seguridad de la Información: Ente constituido por las máximas autoridades y jefaturas que conforman la estructura organizativa de la comuna y es conformado para apoyar todo lo concerniente a la seguridad informática. Podrá estar integrado por concejales, alcaldes, delegados municipales, gerentes, Jefe de unidades, etc.

CSIRT: Equipos de Respuesta a Incidentes de Seguridad en Computadores o Computer Security Incident Response Team.

ID: Identificador Único

ISO/IEC 27002: Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.[22]

LAIP: Ley de Acceso a la Información Publica

Propietario de la información y de los activos: Responsable o persona a cargo del activo.

Responsable de la Seguridad Informática: Persona certificada en seguridad informática que tiene por objeto garantizar el fiel cumplimiento de los planes y procedimientos en seguridad informática establecidos en las presentes políticas y asesorar sobre la materia.

Servicio de Directorio (**SD**): Es una aplicación o un conjunto de aplicaciones que

[22] http://es.wikipedia.org/wiki/ISO/IEC_27000-series

almacena y organiza la información sobre los usuarios de una red de ordenadores y sobre los recursos de red que permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. [23]

Terceros: Personal externo a la comuna que colabora o presta sus servicios a la misma (Estudiantes en servicios social, pasantes o practicantes, profesionales externos, proveedores de servicio, etc.)

2.2 Consideraciones

Salvo excepcionales casos, la numeración utilizada para etiquetar los Dominios, Objetivos de control y Controles coincide con el orden en que aparecen enlistados en la guía utilizada como base del código de buenas prácticas de seguridad de la información estándar ISO/IEC 27002:2013. Cuando algunos valores numéricos pareciera que faltaren es debido a que el contenido de esos tópicos no fueron considerados en la presente normativa.[24]

[23] http://es.wikipedia.org/wiki/Servicio_de_directorio

[24] Véase: ISO/IEC 27002:2013 en Apéndice

3. Estructura de las presentes Políticas de Seguridad

Las políticas adoptadas por la Alcaldía de *(nombre de la alcaldía)* cubren 49 Controles, 20 Objetivos de control embebidos dentro de 12 Dominios de seguridad; desglosados de la siguiente manera[25]:

1. Sobre las políticas
2. Términos y Consideraciones
3. Estructura de las Presentes Políticas de Seguridad
4. Evaluación de riesgos de la Alcaldía
5. Dominio: POLÍTICAS DE SEGURIDAD
    - 1 Objetivo de control
    - 2 controles
6. Dominio: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
    - 1 Objetivo de control
    - 2 Controles
7. Dominio: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
    - 2 Objetivos de control
    - 2 Controles
8. Dominio: GESTIÓN DE ACTIVOS
    - 3 Objetivos de control
    - 5 Controles
9. Dominio: CONTROL DE ACCESOS
    - 3 Objetivos de control
    - 6 Controles
10. Dominio: CIFRADO
    - 1 Objetivo de control
    - 1 Control

[25] Considérese Dominios desde el numeral 5 en adelante.

11. Dominio: SEGURIDAD FÍSICA Y AMBIENTAL
    - 2 Objetivos de control
    - 13 Controles
12. Dominio: SEGURIDAD OPERATIVA
    - 2 Objetivos de control
    - 2 Controles
13. Dominio: SEGURIDAD EN LAS TELECOMUNICACIONES
    - 1 Objetivo de control
    - 2 Controles
14. Dominio: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
    - 2 Objetivos de control
    - 7 Controles
16. Dominio: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
    - 1 Objetivo de control
    - 6 Controles
18. Dominio: CUMPLIMIENTO [26]
    - 1 Objetivo de control
    - 1 Control

[26] Salvo excepcionales casos, la numeración utilizada para etiquetar los Dominios, Objetivos de control y Controles coincide con el orden en que aparecen en la ISO/IEC 27002:2013. Cuando algunos valores numéricos pareciera que faltaren es debido a que el contenido de esos tópicos no fueron considerados en el presente documento.

4. Evaluación de riesgos de la Alcaldía

Todo riesgo debe ser medido, clasificado y cuantificado. Es por ello que la Alcaldía de *(nombre de la alcaldía)* realizó el análisis de los riesgos informáticos a los que podría verse expuesta, ello con la finalidad de estar preparados para mitigar los efectos contraproducentes que estos podrían generar en caso de que ocurriesen. Mediante lo anterior se planteó una serie de consideraciones a tomar en cuenta para determinar los controles a seleccionar, entre las que se tienen:

- Se deberán tener bien definido que activos se han de proteger. Para ello habría que clasificar, catalogar y valorar los activos según su grado de importancia estratégica, considerando entre otros: hardware, software, servicios informáticos, información almacenada, manuales, contratos con proveedores, recurso humano, etc. de los cuales habría que identificar también los riesgos a los que se encuentren expuestos. (Para cubrir este criterio se seleccionó el Dominio 8 que versa sobre la Gestión de Activos)
- Se deben considerar, estimar y tratar de predecir todas (o al menos la mayoría) de las posibilidades de ocurrencia de un hecho que afecte la infraestructura informática de la comuna. A través de ello se podrá determinar en cuales habrá de enfocarse los esfuerzos (mediante el plan de acción apropiado) para la protección de los activos etiquetados y valorados como estratégicos. (Para cubrir este criterio se seleccionó el Dominio 8 que versa sobre la Gestión de Activos y el Dominio 16 sobre Gestión de Incidentes)
- Se debe realizar un estudio que permita estimar el costo económico que pudiese derivarse tras un hecho que atente contra la infraestructura informática de la comuna. Con ello se podrá determinar que es más oneroso: si el incrementar el nivel de protección a los activos informáticos o el costo de rescatar la información afectada (reproducirla nuevamente).

Luego de identificados los riesgos; los activos a proteger y el impacto que estos pueden ocasionar en la Alcaldía, se clasifico cada una de las amenazas y vulnerabilidades que pueden afectar las operaciones de la comuna. Estas se

categorizaron según el entorno al cual pueden afectar, a saber:

- Amenazas humanas (Personal interno y externo).
- Amenazas al sistema (Seguridad Lógica).
- Amenazas físicas externas y ambientales (Seguridad física y ambiental).
- Amenazas en la red (Seguridad en las telecomunicaciones).

Para afrontar todas las anteriores, las presentes políticas adoptan una serie controles que en su mayoría han sido seleccionados para reducir o minimizar los riesgos de las amenazas actuales. Empero existen otros controles no considerados que pudiesen también ser incorporados, adaptados y acondicionados a futuros requerimientos de la Alcaldía surgidos de necesidades posteriores.

Observación:

La aplicación de controles se establece para reducir riesgos, debido a que (de momento) la seguridad informática infalible no existe.

5. Dominio: POLÍTICAS DE SEGURIDAD

5.1 Objetivo de control: Directrices de la Dirección en seguridad de la información

Establecer el conjunto de políticas a aplicar, mediante la descripción de los Dominios, Secciones o Clausulas a considerar, que contribuyan a generar el plan de acción a seguir en la gestión de seguridad informática con el objeto de contribuir en minimizar amenazas y proteger los activos informáticos de la comuna.

5.1.1 Control: Conjunto de políticas para la seguridad de la información.

5.1.1.1 El presente manual de políticas ha sido avalado por el Comité de Seguridad de la Información y aprobado por el Consejo Municipal de la Alcaldía de *(nombre de la alcaldía)* según Decreto Numero *(número del decreto)* establecido en el Acuerdo *(número o código del acuerdo)* *sesión (ordinaria o extraordinaria)* de fecha (*fecha de sesión*) a partir del cual se ordena la entrada en vigencia del mismo, en línea con lo anterior se dictamina se sigan los procedimientos establecidos a fin que las mismas se hagan del conocimiento a todo el personal de la institución y a los proveedores de servicios tecnológicos de la comuna.
Las clausulas, secciones o dominios a considerar se enuncian a continuación:

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.
Tiene como finalidad establecer responsabilidades para la seguridad de la información y el contacto con los grupos de interés especial.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
Determinar las obligaciones contraídas, en materia de seguridad informática, por todo el personal que se incorpora o que labora en la institución.

GESTIÓN DE ACTIVOS
Controla el uso aceptable y correcto resguardo de los activos institucionales.

CONTROL DE ACCESOS

Administra los accesos lógicos de los usuarios a sistemas y aplicaciones.

CIFRADO

Propone técnicas criptográficas basadas en estándares para proteger la confidencialidad, autenticidad o integridad de la información.

SEGURIDAD FÍSICA Y AMBIENTAL.

Su finalidad es la de proteger la integridad física de las instalaciones y de los equipos contra amenazas externas y ambientales.

SEGURIDAD OPERATIVA.

Establece las responsabilidades y procedimientos de operación, junto a la gestión de vulnerabilidades técnicas.

SEGURIDAD EN LAS TELECOMUNICACIONES

Orientado a asegurar la perfecta gestión de la seguridad en las redes de telecomunicaciones y el intercambio de información con partes externas.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

Proteger la información y los sistemas de aplicaciones desarrollados por la alcaldía, proveedores o asignados a terceros.

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Establecer las operaciones a realizar para incrementar la capacidad de prevención y respuesta a incidentes, si los hubiere, que afecten la infraestructura de red de la municipalidad.

CUMPLIMIENTO

Establece la regulación a implementar para garantizar el cumplimiento de las

políticas y normas de seguridad de la información.

5.1.2 Control: Revisión de las políticas para la seguridad de la información.

5.1.2.1 Las presentes políticas deberán ser objeto de control y habrán de ser sometidas a evaluaciones periódicas a fin de que se documente, mejore y actualice oportunamente situaciones imprevistas detectadas. Al mismo tiempo se deberán realizar los ajustes oportunos a las mejoras propuestas que surjan tras las revisiones programadas.

La responsabilidad sobre los controles, propuestas de mejora y divulgación de los cambios aplicados recaerá sobre el Comité de Seguridad de la Información quien deberá contar con el aval del Consejo Municipal para validar los cambios a aplicar.

6. Dominio: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Objetivo de control: Organización interna

Generar el andamiaje estructural y organizacional que será el responsable de garantizar el cumplimiento de los planes y procedimientos en seguridad informática establecidos en las presentes políticas.

6.1.1 Control: Asignación de responsabilidades para la seguridad de la información.

6.1.1.1 El Consejo Municipal deberá conformar el Comité de Seguridad de la Información al cual se le asignaran roles, obligaciones y responsabilidades que incluyen: la regulación, adaptación y propuestas de revisión a las presentes políticas en respuesta a los cambio venideros; coordinación en la implementación de los controles; auditar los procesos; monitorizar el cumplimiento de lo establecido y adoptar las medidas correctivas tras el incumplimiento de estas. Además deberá establecer los medios para que todo el personal de la comuna conozca, sea capacitado y concientizado sobre la reglamentación establecida y los beneficios esperados al respetar la misma.

Edicto:

El Consejo Municipal de la Alcaldía (nombre de la alcaldía) en apoyo a las presentes políticas establece la siguiente estructura organizativa denominada Comité de Seguridad de la Información, como entidad responsable de coordinar la seguridad de la información a nivel institucional basándose en buenas practicas informáticas, que tendrá por objeto la responsabilidad de planificar, implementar, supervisar, evaluar y proponer mejoras al sistema de seguridad de la información a través de la propuesta del establecimiento de estrategias y controles adecuados que aseguren apropiadamente los activos informáticos de la comuna. En línea con lo anterior se acuerda proponer como integrantes del mencionado comité a las siguientes

personas:

(Ejemplo de listado de integrantes, acomodar según necesidades)

- *Subgerente de Servicios Municipales o un delegado especializado,*
- *Subgerente de Planificación y Desarrollo urbano o un delegado especializado,*
- *Jefe de UACI o un delegado especializado,*
- *Jefe de la Unidad Jurídica o un delegado especializado,*
- *Jefe de REF o un delegado especializado,*
- *Jefe de RR HH o un delegado especializado,*
- *Jefe de Informática o un delegado especializado,*

Los anteriores serán los garantes que se cumplan los planes y procedimientos establecidos; determinara las sanciones ante las faltas cometidas sobre la base legal de las presentes. Deberán proponer mejoras aplicables a las presentes políticas y revisar periódicamente los nivele de seguridad adecuándolos a las nuevas tecnologías. Además deberán proveer los medios para promover los procesos de concientización entre todo el personal de la alcaldía.

Recomendación:

En el entendido que el Comité de Seguridad de la Información carece de las experiencias técnicas en materia de seguridad informática. Este podrá peticionar la colaboración de peritos en la materia sean internos o externos a quienes solicitara asesoría para la aclaración, explicación o ampliación de respuestas o dudas surgidas en la disciplina de la seguridad informática.

6.1.1.2 Sera el Consejo Municipal el encargado de designar al Responsable de la Seguridad Informática de la comuna quien deberá ser elegido atendiendo a su idoneidad para ocupar el cargo según sus competencias y perfil. La persona seleccionada tendrá como responsabilidades: garantizar el fiel cumplimiento de los planes y procedimientos en seguridad informática establecidos; verificar y controlar que se cumplan los estándares de seguridad acordados aplicables a los proveedores de servicios de tecnología contratados mediante ANS; mantener un canal de

comunicación para notificar al Comité de Seguridad de la Información sobre la detección de vulnerabilidades y/o fallos identificados; capacitar al personal de la comuna sobre procedimientos de seguridad, ingreso, acceso y manipulación de la información digital almacenada en los sistemas informáticos institucionales; Pre-veer riesgos y amenazas para preparar los planes de contingencia y las estrategias de reacción a implementar ante eventos informáticos.

Debido a su rol, a la personal seleccionada se le exigirá que tenga formación técnica en seguridad informática y deberá responsabilizarse de los siguientes aspectos.

Seguridad ligada a los Recursos Humanos.

Seguridad en la Gestión de Activos.

Seguridad sobre el Control de Accesos.

Seguridad relacionada al Cifrado.

Seguridad del entorno Físico y Ambiental.

Seguridad de las Operaciones.

Seguridad de las Telecomunicaciones.

Seguridad relacionada al desarrollo y mantenimiento de sistemas informáticos

Seguridad relacionada en el manejo de incidentes informáticos.

Edicto:

El Consejo Municipal de la Alcaldía (nombre de la Alcaldía) acuerda nombrar a (nombre del elegido) como persona responsable de dirigir la seguridad de la información a nivel institucional basándose en buenas practicas informáticas, quien tendrá por objeto, entre otros: garantizar el fiel cumplimiento de los planes y procedimientos en seguridad informática establecidos; Colaborar en la elaboración de los ANS y verificara el fiel cumplimiento de los requisitos de seguridad establecidos en los mismos; Dará informes regularmente sobre el estado de la seguridad al Comité de Seguridad de la Información; promover y concientizar dentro del personal de la comuna sobre procedimientos de seguridad y los propósitos de aplicar las presentes políticas; Coordinar las operaciones en la prevención, afronta y resolución de incidentes, si los hubiere, que afecten la infraestructura de red de la municipalidad.

6.1.1.3 Se designara a los Jefes encargados de cada unidad organizacional de la comuna, como el Propietario de la información y de los activos**,** bajo cuya responsabilidad recaen las siguientes obligaciones: deberá clasificar, documentar y mantener actualizada la base de los activos asignados según literal 8.2.1 de la presente políticas; además deberán especificar cuáles usuarios subalternos tendrá permisos y privilegios sobre la información bajo su responsabilidad

6.1.1.4 El encargado de la Unidad de Recursos Humanos será el/la responsable de comunicar e instruir al nuevo personal sobre la normativa establecida en las presentes políticas. Adema deberá notificar, de manera oportuna, a todo el personal sobre cambios, modificaciones o ajustes que surgieren tras la revisión de las mismas.

6.1.1.5 El encargado de la Unidad Jurídica validara y revisara los aspectos legales y todo lo referente al marco jurídico aplicable a las presentes políticas. Al mismo tiempo podrá proponer cambios sobre las mismas a fin de alinearlas con las leyes vigentes de la república.

6.1.4 Control: Contacto con grupos de interés especial.

6.1.4.1 El Responsable de la Seguridad Informática será el vínculo, que fungirá como enlace, para canalizar todos los conocimiento adquiridos por las diferentes unidades institucionales, a efectos de establecer las estrategias proactivas y reactivas a aplicar para afrontar incidentes informáticos. Al mismo tiempo podrá mantener contacto con especialistas en seguridad informática de otros gobiernos municipales, profesionales externos certificados, agrupaciones, asociaciones, comités, foros de alerta temprana y equipos de respuesta a incidentes de seguridad en computadores o Computer Security Incident Response Team (CSIRT) a fin de asesorarse y mantenerse actualizado sobre la forma óptima de confrontar amenazas informáticas.

7. Dominio: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Objetivo de control: Sobre las contrataciones

Establecer el procedimiento a seguir durante los procesos de contratación de personal. Lo que incluye la comprensión y concientización sobre las obligaciones y funciones contraídas por los empleados y/o terceros en materia de seguridad informática. Además define los responsables que se encargaran garantizar la difusión de las presentes políticas.

7.1.2 Control: Términos y condiciones de contratación

7.1.2.1 El manual de contrataciones, desarrollado por la Unidad de Recursos Humanos deberá incluir las obligaciones y funciones contraídas por los empleados en materia de seguridad informática. Las anteriores habrán de ser revisadas y ajustadas a modo de adecuarlas a los cambios surgidos tras las revisiones programadas de las presentes políticas.

7.1.2.2 Es responsabilidad del Comité de Seguridad de la Información establecer las obligaciones y funciones de seguridad informática a ser incluido al perfil de cada uno de los puestos de trabajo de la comuna.

7.1.2.3 Es responsabilidad de la Unidad Jurídica apoyar las presentes políticas mediante la elaboración de acuerdo de confidencialidad a ser utilizado para la contratación o subcontratación de personal y/o terceros.

7.1.2.4 Es responsabilidad de la Unidad de Recursos Humanos cumplir las siguientes obligaciones:

- Informar a todo el personal en entrenamiento, pasantía, servicio social e inducción laboral sobre las obligaciones y responsabilidades adquiridas al hacer uso de los servicios tecnológicos institucionales.

- Atestiguar que todos los empleados de la comuna firmen el Acuerdo de confidencialidad sobre la información administrada por la alcaldía.
- Coordinar junto con el responsable de la seguridad informática la difusión, comprensión, concientización y aceptación de las presentes políticas por parte de todo el personal de la comuna que hace uso de los servicios informáticos institucionales.
- Cooperar con el responsable de la seguridad informática para establecer los canales que permitan capacitar y comunicar de manera oportuna a todo el personal que haga uso de los servicios tecnológicos de la comuna para notificarles sobre amenazas o percances que puedan afectar la seguridad de la alcaldía y como hacerle frente a situaciones o incidentes informáticos surgidos.

7.3 Objetivo de control: Cese o cambio de puesto de trabajo.

Garantizar un proceso metódico cuando finaliza la relación laboral entablada entre empleados y/o terceros con la Municipalidad.

7.3.1 Control: Cese o cambio de puesto de trabajo.

7.3.1.1 Tras el cese de actividades laborales o cambio del puesto de trabajo el empleado deberá de entregar todos los activos informáticos que le hayan sido asignados lo cual incluye dispositivos tecnológicos, software, códigos en desarrollo, licencias, claves y tarjetas de acceso, documentos institucionales, etc. Como control de lo anterior será responsabilidad de la Unidad Jurídica el levantamiento del acta de recepción de los mismos.

7.3.1.2 Es obligación de la Unidad de Recursos Humanos informar con anticipación al Responsable de la Seguridad Informática sobre el cese de labores u operaciones del usuario que se retira o es promovido a otras áreas.

7.3.1.3 Es responsabilidad del jefe encargado/a (que haya sido designado como Propietario de la información y de los activos) de la unidad donde labora la persona que se retira o es promovida a otras áreas controlar que esta mantenga documentada todas las operaciones y proyectos en los cuales ha participado.

7.3.1.4 Es obligación del Responsable de la Seguridad Informática evaluar factores de riesgo de la persona que es removida o promovida a otras áreas a fin de:

- Se valore la necesidad o no de deshabilitársele los accesos y privilegios.
- Se considere permitir acceso físico y lógico a áreas donde se almacena información sensible.
- Se le restrinja el uso de cualquier medio de soporte extraíble a través del cual la persona pueda apropiarse de información sensible. Al mismo tiempo deberá considerarse tomar las medidas necesarias para controlar y monitorear las transferencias electrónicas para evitar el envió de información municipal a través de la infraestructura de red institucional.
- Todo monitoreo (de ser estrictamente necesario) sobre las actividades informáticas institucionales de la persona que cesa operaciones en la comuna, deberá realizarse respetando las normas de ética. Evitando vulnerar la privacidad de la misma.

8. Dominio: GESTIÓN DE ACTIVOS.

8.1 Objetivo de control: Responsabilidad sobre los activos

Establecer las directrices para el inventariado de los activos informáticos y los responsables del resguardo de los mismos.

8.1.1 Control: Inventario de activos

8.1.1.1 Los jefes encargados de cada unidad que han sido designados como Propietarios de la información y de los activos trabajaran en coordinación con la Unidad Informática a fin de llevar a cabo y mantener actualizado un inventario de los activos informáticos asignados en custodia. La clasificación habrá de considerar los siguientes ítems: (identificación del activo, Tipo de activo, Descripción del activo, propietario del activo y localización del activo). La revisión del inventario habrá de llevarse a cabo, de manera rigurosa, al menos una vez por año.

Recomendación:

Dentro de los activos informáticos a considerar se encuentran: aplicaciones Apps, software, herramientas de desarrollo, bases de datos, archivos de datos, dispositivos informáticos (Firewall físicos, routers, cableado, servidores, computadores, impresores, aparatos de comunicación y otros), servicios informáticos, manuales técnicos y de usuarios, contratos con proveedores y ANS.

Herramientas recomendadas

- Genos Open Sourc
- GLPI
- SpiceWorks

8.1.1.2 Los jefes encargados de cada unidad que han sido designados como Propietarios de la información y de los activos trabajaran en coordinación con el

Responsable de la Seguridad Informática a fin de clasificar la información de acuerdo al nivel de sensibilidad establecida en las directrices de clasificación del literal 8.2.1.1 de las presentes políticas. En dado caso exista la necesidad de reclasificar cierta parte o toda la información el encargado de la unidad habrá de notificar inmediatamente al Responsable de la Seguridad Informática para que tome las acciones pertinentes.

8.1.1.3 Es responsabilidad del Responsable de la Seguridad Informática y del Encargado de la Unidad Informática blindar la información conforme al grado de sensibilidad asignado a la misma.

8.2 Objetivo de control: Clasificación de la información.

Garantizar que la información digitalmente almacenada sea clasificada según su grado de sensibilidad.

Observación:

De acuerdo al Capítulo II de la Ley de transparencia municipal, emitido por la Asamblea Legislativa de la República de El Salvador existen puntos importantes que ha de considerarse al momento de establecer directrices para clasificar la información que es solicitada a la comuna, debido a que según se establece en el Art. 9. “Se reconoce a todas las personas naturales y jurídicas, el derecho a solicitar información a los Concejos Municipales y de recibir ésta de manera oportuna, clara y de fácil entendimiento” y la obligación de las municipalidades a proporcionar dicha información según el literal a) del Art. 10 que dice: Las Municipalidades tienen la obligación de “Proporcionar la información requerida por el ciudadano cuando sea procedente de acuerdo a esta Ley”. Empero en el Art. 12 del apartado denominado *De las Excepciones* se enuncia: “Cada Municipalidad establecerá, en una Ordenanza la reglamentación sobre el acceso público a la información municipal, las informaciones que son calificadas como confidenciales, las cuales no podrán ser divulgadas”. Lo anterior permite a las municipalidades emitir una reglamentación que establezca criterios de clasificación para controlar la seguridad de la misma.

Debe considerarse también que existe la Ley de Acceso a la información Pública (LAIP). La cual en el Art. 6 literales 'd', 'e' y 'f' detalla las definiciones de clasificación de la información. Siendo estas: Oficiosa, Reservada y Confidencial.

8.2.1 Control: Directrices de clasificación.

8.2.1.1 Toda información digitalmente almacenada deberá ser etiquetada, manipulada, y valorada de acuerdo a su nivel de sensibilidad conforme la siguiente clasificación:

- Nivel de seguridad 0
  Color: azul; Nivel de daño: ninguno; Acceso: sin clasificar, de libre acceso público; LAIP: OFICIOSA
- Nivel de seguridad 1
  Color: verde; Nivel de daño: moderado; Acceso: restringido, solo personal o entidades autorizadas; LAIP: RESERVADA
- Nivel de seguridad 2
  Color: amarillo; Nivel de daño: significativo; Acceso confidencial, accesible solo para reducido grupo de miembros del personal; LAIP: CONFIDENCIAL.
- Nivel de seguridad 3
  Color: rojo; Nivel de daño: severo; Acceso: secreto, accesible solo para la alta gerencia, alcalde y concejales; LAIP: CONFIDENCIAL.

8.3 Objetivo de control: Manejo de los soportes de almacenamiento.

Reglamentar los procedimientos a aplicar para la administración, traslado y eliminación de los soportes de almacenamiento.

8.3.1 Control: Gestión de soportes extraíbles.

8.3.1.1 La Unidad Informática de la alcaldía mantendrá el control sobre los

dispositivos de almacenamiento externo autorizados para manipular información dentro de la comuna. Ello incluye: Discos USB externos, Memorias USB, chip card, ID cards, quemadores de discos Cds, DVDs, Blue Ray o similares y además cualquier otro dispositivo que permita extraer y/o almacenar información. Entre ellos: Video/audio tapes, diskettes, cassetes, film u otros.

8.3.1.2 Queda restringida la utilización de unidades USB extraíbles, de índole personal, ajenas a la comuna, en aquellos dispositivos que contengan información categorizada dentro de los niveles 1, 2, o 3 de seguridad, tipificada en las directrices de clasificación del literal 8.2.1.1 de este manual. Incluyese las unidades REF y Despacho. Si por algún motivo hubiere necesidad de realizar copia de la información almacenada en dichos dispositivos, los jefes encargados de cada unidad que han sido designados como Propietarios de la información y de los activos del área, deberán realizar una solicitud junto con la respectiva justificación, al Responsable de la Seguridad Informática quien a su vez podrá ser asistido por personal de la Unidad Informática para apoyar sobre la mejor forma de realizar el proceso.

8.3.1.3 El Encargado de la Unidad Informática velará porque la comuna cuente con las herramientas necesarias que permitan administrar la instalación de dispositivos de almacenamiento externo, para reducir los riesgos asociados en la copia de información sensible. De no ser posible será el responsable de cerrar los puertos USB que permitan bloquear la conexión de dispositivos extraíbles.

Recomendación de seguridad:

SO: Windows

- Alteración de los valores de registro del sistema que permiten la conexión de dispositivos USB.
- Deshabilitan de los puertos USB desde el administrador de dispositivos.
- Desinstalación de los controladores de los dispositivos de almacenamiento masivo USB.

SO: linux

- Quitar al usuario del grupo plugdev y crear una blacklist

8.3.1.4 Todo el personal que esté autorizado a manipular dispositivos de almacenamiento externo tales como los descritos en el numeral 8.3.1.1 que accedan a computadoras o servidores que contengan información sensible, habrá de estar plenamente capacitado en la gestión segura y manejo de información confidencial.

8.3.2 Control: Eliminación de soportes.

8.3.2.1 Para la destrucción, eliminación o borrado de manera segura de información confidencial; que no sea más requerida y que la ley de la república permita, serán los jefes encargados de cada unidad que han sido designados como los Propietarios de la información y de los activos quienes realicen la petición y su respectiva justificación al Responsable de la Seguridad Informática quien a su vez podrá solicitara ser asistido por personal de la Unidad Informática designado por el Encargado de la Unidad Informática para asesorar sobre la mejor forma de realizar el proceso.

Recomendaciones:

Para el borrado seguro, siguiendo las buenas prácticas, puede recurriese a la norma *EN 15713:2010: "Destrucción segura del material confidencial. Código de buenas prácticas."*

Herramientas recomendadas

SO. Windows

- Heidi (Eraser)
- Hardwipe

8.3.3 Control: Soportes físicos en tránsito

8.3.3.1 Todo dispositivo informático que contenga información sensible, categorizada dentro de los niveles 2 o 3 de seguridad, tipificada en las directrices de clasificación del literal 8.2.1.1 de estas políticas, deberá ser transportado guardando las medidas de seguridad pertinentes. La información contenida dentro de dispositivos extraíbles deberá ser cifrada para evitar comprometer su contenido en caso de extravió.

Herramientas Recomendadas:

- Rohos Mini Drive

9. Dominio: CONTROL DE ACCESOS

9.1 Objetivo de control: Requisitos de negocio para el control de accesos.

Establecer las políticas de seguridad que dicten el procedimiento a seguir para impedir accesos no autorizados.

9.1.1 Control: Política de control de accesos.

9.1.1.1 Se adoptaran políticas de control de acceso, que permitan establecer, implementar supervisar, mejorar, controlar y administrar de manera eficiente el registro de usuarios y sus respectivas contraseñas, privilegios, derechos de accesos, y responsabilidades. La revisión de dichas políticas deberá establecerse en intervalos de plazo máximo de 6 meses.

Recomendación

Véase **Carta de asignación de control de acceso** en el apartado Apéndice de las presentes políticas.

9.1.2 Control: Control de acceso a las redes y servicios asociados.

9.1.2.1 Se establecerá políticas de control de acceso, que permita adoptar, implementar, supervisar y mejorar, controlar, y administra de manera eficiente el acceso a los servicios de red y de conexiones remotas con un periodo no mayor a 6 meses.

Herramientas recomendadas

- OpenNAC
- Packetfence

9.2 Objetivo de control: Gestión de acceso de usuario.

Ofrecer una visión sobre el ciclo de vida del acceso de usuarios. Desde su creación o alta hasta su cancelación o baja.

9.2.1 Control: Gestión de altas/bajas en el registro de usuarios.

9.2.1.1 Cada empleado de la comuna que por sus funciones laborales deba hacer uso de los servicios tecnológicos ofrecidos por la comuna deberá contar con un identificador único ID (login) para el acceso a infraestructura de red que conforman los distintos dispositivos informáticos de la alcaldía el cual será asignado de acuerdos al nivel privilegio en el cual sea catalogado.

9.2.1.2 Toda persona que reciba un ID para acceder a la infraestructura de red de la comuna deberá aceptar los términos y condiciones establecidas en la **Carta de asignación de control de acceso.**

9.2.1.3 El Identificador Único es de uso exclusivo de la persona a quien le sea asignado. Por lo tanto es responsable de mantener en total reserva dicho identificador. En caso de sospecha que dicho ID han sido apropiado o está siendo manipulado por personas distintas a la asignada, el usuario propietario deberá notificar a la brevedad al Encargado de la Unidad a la que pertenece para que este a su vez informe al Responsable de la Seguridad Informática quien iniciara las investigaciones y determinara los procedimientos a ejecutar.

9.2.1.4 Es responsabilidad del Encargado de la Unidad Informática de la comuna adoptar e implementar las herramientas necesarias para el establecimiento de los controles de acceso.

Herramientas recomendadas

- UserLock

9.2.1.5 Es responsabilidad del Encargado de la Unidad Informática controlar, supervisar, revisar y auditar que cada uno de los usuarios autorizados a ingresar a los servicios informáticos provistos por la comuna traten de evadir los controles de seguridad establecidos para escalar privilegios.

Herramientas recomendadas

- Pangolin

9.2.1.6 Los identificadores asignados a usuarios podrán ser dados de baja en cualquier momento si se sospecha que está siendo utilizado de manera impropia para obtener accesos no autorizados; divulgación o manipulación indebida de información privilegiada; intentos de utilizar la infraestructura de red de la comuna para realizar actos informáticos vandálicos, sean locales o hacia el exterior; Intentos de conexiones remotas no autorizados; Instalación de software y/o aplicaciones no autorizadas y todo aquello que sea considerado nocivo o que afecte la correcta operatividad del sistema de gestión de la seguridad de la información.

9.2.1.7 La base de datos de los identificadores ID deberá ser objeto de frecuentes revisiones a fin de dar de baja a aquellos que se encuentren en desuso o que la persona a quien le fue asignado haya dejado de prestar sus servicios a la comuna o hayan cambiado su rol dentro de la alcaldía a uno que posea privilegios de acceso distinto al cargo anteriormente desempeñado.

9.2.2 Control: Gestión de los derechos de acceso asignados a usuarios y revisión de los derechos de acceso de los usuarios.

9.2.2.1 Toda política de privilegios de acceso deberá ser objeto de revisión de manera programada para identificar los niveles de acceso otorgados a los usuarios, el cual deberá contar con las siguientes características:

- Ser finito es decir que deberá contar con un periodo de caducidad (La revisión

de privilegios deberá establecerse en intervalos de plazo máximo de 6 meses.)

- Estar definido: detallara las condiciones bajo las cuales puede ser instaurado para establecer los privilegios a asignar/revocar (obligación competente a responsable de la seguridad informática)
- Ser controlado: deberá poseer un protocolo estricto para su asignación y definición del personal autorizado para hacer uso de los privilegios (obligación concerniente a la unidad informática).
- Estar categorizado: a que aplicación se puede acceder y bajo cuales condiciones.(similar al procedimiento seguido en el literal 8.1.1.2 de las presentes políticas)

Herramientas Recomendadas:

- Aveksa: de paga

9.2.3 Control: Gestión de los derechos de acceso con privilegios especiales.

9.2.3.1 Los usuario que por razones laborales requieran acceso con privilegios diferentes a los asignados originalmente, deberán realizar la solicitud al jefe encargado (designado como Propietario de la información y de los activos) de la unidad en la cual laboran para que este realice las gestiones pertinentes ante el Responsable de la Seguridad Informática.

9.4 Objetivo de control: Control de acceso a sistemas y aplicaciones.

Establecer los controles que garanticen la creación de contraseñas seguras que restrinjan el acceso a los servicios ofrecidos por la comuna.

9.4.3 Control: Gestión de contraseñas de usuario.

9.4.3.1 El identificador único ID asignado, según se dicta en el literal 9.2.1.1 de la

presente Sección, deberá contar con una contraseña segura. La cual deberá ser modifica de manera frecuente, acorde al nivel de seguridad de la información que esta almacenada en aquellos dispositivos que contengan información categorizada según lo establecido en las directrices de clasificación del literal 8.2.1.1 de las presentes políticas. Ante lo cual se propone:

- Nivel de seguridad 0: CADA 360 DIAS
- Nivel de seguridad 1: CADA 270 DIAS
- Nivel de seguridad 2: CADA 180 DIAS
- Nivel de seguridad 3: CADA 90 DIAS

Herramientas Recomendadas:

- Password Safe
- Randow Password Generator

9.4.3.2 Para establecer el primer acceso a través del ID asignado se facilitara una contraseña provisional segura. La cual se proporcionara de manera directa entregada en forma impresa a través de la **Carta de asignación de control de acceso**. Dicha contraseña deberá ser modificada por el usuario, para ello deberá contarse con herramientas que validen que las claves iniciales tengan un periodo de caducidad muy corto (máximo 3 días) antes de quedar invalidada. De darse el caso de finalizado el plazo. El usuario deberá solicitar otra contraseña teniendo que apegarse a los protocolos establecidos.

9.4.3.3 Toda contraseña deberá tener un mínimo de 8 caracteres para lo cual los sistemas deberán estar parametrizados para que validen dicho requerimiento.

Herramientas Recomendadas:

- KeePASS

9.4.3.4 Deberá existir un control sobre los cambios de contraseñas las cuales no deberá repetirse ni aceptar que haya sido utilizadas en los últimos 6 cambios.

9.4.3.5 La contraseña deberá tener un control de conteo de intentos de autenticación, los cuales dependerá de las directrices de clasificación del literal 8.2.1.1 de las presentes políticas. Una vez superados los mismos la contraseña podría ser deshabilitada por un tiempo determinado. Ante lo anterior se propone:

- Nivel de seguridad 0: Infinita cantidad de intentos
- Nivel de seguridad 1: 15 intentos
- Nivel de seguridad 2: 10 intentos
- Nivel de seguridad 3: 5 intentos

10 Dominio: CIFRADO.

10.1 Objetivo de control: Controles criptográficos.

Proponer las políticas para el establecimiento de los controles criptográficos

10.1.1 Control: Política de uso de los controles criptográficos.

10.1.1.1 El Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática determinaran, establecerán y aplicaran todos los procesos y técnicas de criptografía necesarias para salvaguardar y proteger la información digital de la comuna. Para ello se deben realizar la evaluación de riesgos respectivos que permita aplicar protección de la información en tránsito, de los datos, de los servicios provistos y de las claves de acceso. Los procesos de la evaluación de las políticas de criptografía habrán de realizarse al menos una vez por año.

Herramientas Recomendadas:

Cifrado de información en tránsito

- BoxCryptor: Cifrado de archivos en Dropbox y otras nubes.
- PGP: Cifrado de correos electrónicos (o GnuPG).
- TigerChat, TigerText: Mensajería segura.
- HTTPS Everywhere: Encryptacion web

Cifrado de información local y móvil

- FreeOTFE: Crea unidades cifradas virtuales.
- Microsoft BitLocker, AxCrypt: Suite de cifrado Windows.
- SSE: Suite de cifrado Android.

11 Dominio: SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Objetivo de control: Áreas seguras.

Ofrecer las directrices que permitan establecer un perímetro de seguridad en las áreas destinadas para alojar dispositivos informáticos, que contengan información sensible, en conjunto a las estrategias a implementar para reducir el acceso físico a las mismas.

11.1.1 Control: Perímetro de seguridad física.

11.1.1.1 Toda área seleccionada para el alojamiento y resguardo de los dispositivos informáticos que ofrecen servicios y/o que alojan información sensible. Deberá contar con un perímetro de seguridad físico adecuado. Ello implica limitar el fácil acceso a la misma por medio de elementos que restrinja el paso actuando como barreras (divisiones, biombos, escritorios con recepcionista, paredes, etc.). Además deberá estar lo más distante posible de las zonas de circulación de los ciudadanos que ingresen a realizar trámites a la comuna.

11.1.2 Control: Controles físicos de entrada.

11.1.2.1 El Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática determinaran quienes tendrán acceso físico (y serán acreditados para ello) a las áreas protegidas que posean dispositivos que almacenen información sensible. Ellos podrán ser catalogados de la siguiente manera:

- Personal TI con privilegios: (que podrán manipular Hardware y realizar todo tipo de trabajo relacionado al mantenimiento correctivo: destapar CPU`s, cambiar disco duro, Memoria RAM, MotherBoard. Realizar BackUps, etc.)
- Personal TI con acceso físico controlado (podrán hacer mantenimiento preventivo, limpieza, actualizaciones, instalaciones de cableado, etc.)

- Personal de mantenimiento interno o externo (personal asignado para la limpieza del área -auxiliar de servicio-; personal de mantenimiento de aires acondicionados o instalaciones eléctricas y cualquier personal outsorsing que ingrese al lugar a instalar o dar mantenimiento a dispositivos provistos por proveedores -como los ISP-).
- Visitas/invitados (toda persona que accede al lugar y no pertenezca a ninguna de las tres anteriores).

11.1.2.2 Las persona categorizadas como Personal de mantenimiento interno o externo y las categorizadas como Visitas/invitados según lo establecido en el literal 11.1.2.1 de esta misma clausula; que acedan al área protegida, deberán en todo momento contar con la presencia y supervisión del personal TI de la comuna o de cualquier persona designada por el Encargado de la Unidad Informática. La escolta de los anteriores se deberá realizar desde el ingreso al área restringida hasta que finalice las operaciones para las cuales se le autorizo el ingreso.

11.1.2.3 Se deberá adoptar controles de acceso físico al interior del área protegida (restringido a través de custodio o de acceso electrónico controlado: como sistemas biométricos, tarjeta magnética u otra medida de seguridad que impida el libre acceso al área.)

11.1.2.4 Se deberá establecer un libro visitas donde se detalle: nombre de la persona que acceda al área; unidad o departamento a la que pertenece (si fuese interno: de la misma comuna); institución a la que pertenece (si fuesen terceros externos); motivo de la visita; hora de entrada y salida.

11.1.3 Control: Seguridad de oficinas, despachos y recursos.

11.1.3.1 Se deberá ubicar y seleccionar la mejor área para el alojamiento y resguardo de los dispositivos informáticos que ofrecen servicios y/o que alojan información

sensible. El sitio escogido habrá de contar con las siguientes condiciones:

- Estar climatizado; es decir debe mantener clima controlado.
- Deberá contar con sistema eléctrico de respaldo.
- Estar acondicionado para soportar siniestros naturales y/o incendios.
- Deberá contar con un perímetro de seguridad físico adecuado. Según lo establecido en el literal 11.1.1.1 de la presente clausula.

Recomendaciones:

Para el control de las condiciones en áreas protegidas y mejoras en el grado de disponibilidad de la información, se pueden considerarse los esquemas de certificación publicados por la Uptime Institute sobre los centros de proceso de datos, basado en 4 niveles (Data Center Tier IV).

11.1.3.2 Toda data (Backups) que sea copia de información sensible, deberá resguardarse en un área distinta y distante (de donde se encuentre alojada la fuente primaria). De preferencia fuera del edificio mismo de la Alcaldía. A manera de reducir la pérdida total de la misma si un desastre afectase toda la edificación. El traslado, resguardo y cifrado de los backups a de guiarse por las directrices establecidas en las presentes políticas (Ver literal 8.3.3.1, literal 10.1.1.1 y literal 12.3.1.1)

11.1.3.3 Tras la finalización de las labores diarias y para garantizar que el área restringida queda protegida y que ninguna tarea critica sea olvidada; se deberá establecer un *checklist* (lista de comprobación), donde se indique el procedimiento a seguir por la última persona acreditada que abandone el sitio. (Se deberán considerar acciones como: Desconexión y apagado de dispositivos no indispensable, cerrado de puertas y ventanas, activación de alarmas -si las hubiere-, etc.)

11.1.3.4 Queda restringida la colocación de información de índole sensible en lugares de acceso público (aplican: listados telefónicos internos; listados de proveedores; listado de compras y/o adquisiciones; memos, notas, post-its o recordatorios, etc.).

11.1.4 Control: Protección contra las amenazas externas y ambientales.

11.1.4.1 Se debe planificar y diseñar establecer procedimientos para la protección de dispositivos informáticos ubicados en áreas seguras evitando con ellos daños que puedan generarse por incendios o efectos de humo, corrosión, altas temperaturas, humedad, inundaciones, etc. Lo anterior incluye mantener elementos inflamables (como los utilizados en las jornadas de fumigación) o explosivos (como los utilizados para las celebraciones patronales) alejados del área asegurada y contar con dispositivos contra incendios accesibles (estratégicamente ubicados).

Recomendaciones:

Para la protección de equipos informáticos y de telecomunicaciones de amenazas o desastres pueden considerarse los estándares NFPA 75 y NFPA 76 de la National Fire Protection.

11.1.5 Control: El trabajo en áreas seguras.

11.1.5.1 Toda área segura deberá mantenerse bajo reserva, sin identificar su ubicación ni las actividades que en ella se realizan. Solo habrá de darse a conocer a aquellos empleados de la comuna que por sus funciones laborales deban conocer la existencia del mismo.

11.1.5.2 Toda área segura deberá ser monitoreada cuando se encuentre cerrada para evitar el acceso de intrusos.

11.1.5.3 Deberá restringirse la captura de fotografías y/o tomas de vídeo del interior de las áreas protegidas.

11.2 Objetivo de control: Seguridad de los equipos.

Proteger la infraestructura tecnológica de la comuna.

11.2.1 Control: Emplazamiento y protección de equipos.

11.2.1.1 Todo equipo que almacene información sensible habrá de ser ubicado en las áreas protegidas y deberá controlarse el uso (manipulación física) sobre el mismo.

11.2.1.2 Todo dispositivo informático debe ser ubicado a manera de no interrumpir el libre tránsito de los usuarios que ingresan a la alcaldía. Tampoco deberá quedar accesible para que intenten manipularlo y su monitor ha de estar instalado a modo de no permitir la visualización de lo que estos proyectan.

11.2.1.3 Los equipos informáticos son exclusivamente para el desarrollo de las actividades labores asignadas.

11.2.1.4 Todo personal que haga uso de los equipos informáticos provistos por la comuna es responsable sobre del buen cuido, uso y manejo del mismo. Ante cualquier falla detectada sobre la operatividad de estos deberá notificar al encargado de la unidad en la cual labora para que este realice las gestiones pertinentes ante el Encargado de la Unidad Informática.

11.2.1.5 No está permitido el ingreso de alimento y bebidas en las áreas protegidas. En el resto de la comuna la manipulación de alimentos cerca de dispositivos informáticos debe ser controlada.

11.2.1.6 Sobre el traslado o movilización de dispositivos informáticos se trabajara sobre los siguientes criterios:

- Ningún dispositivo informático deberá ser removido del lugar asignado sin la autorización del Encargado de la Unidad Informática. (Si existiese necesidad de reubicación, el encargado de la unidad interesada deberá realizar la petición a la Unidad Informática)
- Ningún dispositivo informático deberá ser removido del lugar asignado (ni

siquiera por parte del personal de la Unidad Informática) sin la notificación y justificación (presentada por parte del Encargado de la Unidad Informática) ante el encargado de la unidad de donde se pretende retirar.

11.2.2 Control: Instalaciones de suministro.

11.2.2.1 Los equipos informáticos deben contar con Sistema de alimentación ininterrumpida (UPS: uninterruptible power supply) los cuales habrán de ser revisados y probados de manera periódica

11.2.2.2 Se deberán adoptar medidas para proteger toda la instalación eléctrica de la comuna contra fallos y/o cortes generados por eventos naturales.

11.2.2.3 Se debe planificar la instalación de tomacorrientes según la demanda de dispositivos electrónicos a conectar en cada área.

11.2.3 Control: Seguridad del cableado.

11.2.3.1 Toda instalación cableada debe ser planificada y su tendido debe regirse cumpliendo los siguientes puntos.

- Su recorrido debe estar alejado de cualquier acceso público para evitar conexiones fraudulentas. (Úsese tubería, canaletas o ductos porta cables)
- Su selección debe considerar la ruta del recorrido, que incluye: tiraje vertical, tiraje horizontal aéreo o de piso a piso (pudiéndose aplicar la normativa NEC NFPA -70 1999 articulo 800).
- Debido a la interferencia generada (inducción de campo magnético por cableado eléctrico) los cables eléctricos y los de transporte de datos o telecomunicaciones debe estar separados según norma (pudiendo aplicarse la normativa española UNE-EN 50174-2).
- Para el apropiado mantenimiento y reducir errores todos los cables deben

estar plenamente identificados y documentado.

Recomendaciones:

Para implementar y establecer una infraestructura de red bajo norma también puede considerarse el estándar TIA/EIA-568B que brinda las directrices sobre el cableado a utilizar, los requisitos de instalación, test de prueba del cableado instalado, tipo de conectores y terminaciones, distancias y arquitectura. Igualmente es aplicable la normativa ISO/IEC 11801.

11.2.4 Control: Mantenimiento de los equipos.

11.2.4.1 Solo el personal acreditado según lo establecido en el literal 11.1.2.1 de la presente clausula podrá realizar mantenimiento preventivo y correctivo en los dispositivos informáticos de la comuna.

11.2.4.2 El Encargado de la Unidad Informática será el responsable de establecer los controles y la calendarización para realizar las revisiones periódicas que permitan efectuar el mantenimiento preventivo oportuno en todos los dispositivos informáticos de la comuna. Para ello se guiara por las recomendaciones provistas por los fabricantes.

11.2.4.3 Todo dispositivo informático debe contar con un archivo o historial donde se registre cada una de las operaciones que sobre el mismo se han realizado. Ello incluye mantenimientos, reportes de fallas y cambio de piezas o componentes.

11.2.4.4 Sobre el mantenimiento, traslado o movilización de dispositivos informáticos se trabajara sobre los siguientes criterios:

- Por mantenimiento preventivo (in situ): se realizaran copias de seguridad según el procedimiento establecido en el Control 12.3.1 de las presentes políticas.

- Por mantenimiento preventivo (fuera de la unidad a la cual ha sido asignado): se realizaran copias de seguridad según el procedimiento establecido en el Control 12.3.1 de las presentes políticas. Además se deberá borra la información sensible que el equipo contenga siguiendo procesos similares a los establecidos en el literal 8.3.2.1 de las presentes políticas.
- Por retiro del equipo para traslado a otras unidades: el mismo procedimiento seguido en el caso anterior.
- Por mantenimiento correctivo (si el equipo ya no está encendiendo o las opciones para recuperar información no están operando): El propietario de la información y de los activos deberá indicar e identificar qué información ha sido actualizada o modificada desde la fecha en que se realizó el ultimo respaldo programado (según lo establecido en el Control 12.3.1 de las presentes políticas) hasta la fecha de falla del equipo. Posterior a ello El Encargado de la Unidad Informática realizaran los procedimientos necesarios para intentar recuperar la información requerida.

11.2.5 Control: Salida de activos fuera de las dependencias de la empresa.

11.2.5.1 El retiro de cualquier dispositivo informático y/o software bien sea perteneciente a la comuna o que pertenezca a terceros (proveedores de servicios informáticos), debe contar con la autorización del Propietario de la información y de los activos y del Encargado de la Unidad Informática. Además debe establecerse y quedar registrado la fecha de retorno del mismo. En dado caso el equipo y/o software pertenezca a un proveedor de servicio y el dispositivo es retirado por finalización de contrato, deberá quedar establecido en un formulario de control que el servicio ha sido dado de baja y que por ello se realiza el retiro definitivo del dispositivo.

11.2.6 Control: Seguridad de los equipos y activos fuera de las instalaciones.

11.2.6.1 El manejo y manipulación de todo dispositivo informático que se encuentre

autorizado a salir de la comuna que cumpla con lo establecido en el literal 11.2.5.1 de la presente clausula, debe regirse por las mismas políticas de seguridad que son aplicables al interior de la alcaldía (entre ellas se incluye lo establecido en el literal 8.3.3.1 de las presentes políticas), estableciendo medidas adicionales tales como: custodia permanente, traslado sigiloso, etiquetado e identificado del equipo de forma disimulada a manera que no evidenciar su contenido y utilización del mismo evitando la ostentosidad.

11.2.7 Control: Reutilización o retirada segura de dispositivos de almacenamiento.

11.2.7.1 Todo dispositivo que contenga data que haya cumplido su vida útil, este en desuso o que haya de ser sustituido deberá ser objeto de una revisión minuciosa a manera de evitar que al ser desechado mantenga información concerniere a la comuna. Para ello habrá de identificarse que componentes habrán de ser destruidos físicamente, y en caso de reutilización de los mismos deberá verificarse que se haya efectuado el borrado seguro por sobre-escritura. (Aplica lo establecido en el literal 8.3.2.1 de las presentes políticas)

Herramientas Recomendadas:

SO. Windows

- CCleaner (Drive Wiper)
- Darik´s Boot and Nuke (DBAN)

11.2.8 Control: Equipo informático de usuario desatendido.

11.2.8.1 Todo usuario que por cualquier motivo deba alejarse físicamente del dispositivo informático asignado debe verificar que su equipo cuente con la protección adecuada, dejándolo inaccesible contra acceso indebidos en su ausencia (mientras el computador aun siga encendido). Para ello está en la obligación de

cerrar cualquier sesión que mantenga abierta o activar el protector de pantalla el cual debe estar protegido con contraseña al reanudar. De no poder configurar estas opciones el usuario está en la obligación de informar al Propietario de la información y de los activos para que este solicite al El encargado de la Unidad de Recursos Humanos o al Responsable de la Seguridad Informática para que realice las gestiones y se capacite al personal sobre el proceso para implementar y automatizar dichas configuraciones (véase los literales 9.2.1.3 y 9.2.1.4 de las presentes políticas).

Recomendaciones:

En la mayoría de SO existe la función de Control de Energía u Opciones de Energía la cual, a parte de colaborar con el ahorro energético, es una excelente herramienta a considerar a la hora de proteger los computadores que se encuentran desatendidos puesto que en ella se puede seleccionar varias acciones: por ejemplo puede configurarse Apagar el Monitor de modo automático tras cierto tiempo de inactividad (con la opción de activar la petición de contraseña al reanudar), de igual forma puede indicársele al equipo en qué momento se desean se apaguen los Discos Duros, pasar a Inactividad y en la mayoría de los casos hasta poner en modo Hibernación. Aunque ha de tenerse en cuenta que los dispositivos generan cierta dificultad de acceso remoto cuando se encuentra en modo suspensión e hibernación.

12 Dominio: SEGURIDAD OPERATIVA.

12.2 Objetivo de control: Protección contra código malicioso

Proteger la información digital contenida en los dispositivos institucionales y el software en ellos instalados.

12.2.1 Control: Controles contra el código malicioso.

12.2.1.1 Es responsabilidad del Encargado de la Unidad Informática velar porque la comuna cuente con herramientas apropiadas contra códigos maliciosos, para la adecuada protección de la información y del software instalado en cada uno de los dispositivos informáticos. Para ello y con la finalidad de evitar interrupciones del servicio causadas por infecciones, infracciones de seguridad u otro tipo de ataques informáticos deberá:

- Instalar programas Antivirus y Antispyware confiables.
- Activar los Firewall de los sistemas operativos.
- Establecer los procedimientos para mantener actualizado (de ser posible de manera automática) todo software instalado.
- Aplicar la normativa establecida en las presentes políticas.

12.2.1.2 Es responsabilidad del Encargado de la Unidad Informática realizar análisis periódicos de vulnerabilidades en configuraciones; en aplicaciones instaladas y en sistemas, con el fin de identificar puntos débiles que puedan ser explotados.

Recomendaciones:

Se deben establecer y planificar un conjunto de acciones a realizar para la identificación de agujeros de seguridad, lo cual permitirá realizar los ajustes necesarios según los resultados obtenidos. Para ello se recomienda realizar ataques simulados en sistemas de prueba o laboratorio, que habrán de ser preparados para ese fin, evitando con ello afectar entornos reales. El primer paso habrá de iniciarse

mediante un escaneo de redes; para encontrar equipos activos y los servicios que estos ofrecen (ver literal 13.1.1.2 de las presentes políticas); posteriormente se deberán de identificar vulnerabilidades (Nessus es la herramienta apropiada, también puede probarse Kaspersky: análisis de vulnerabilidades); tras descubrir vulnerabilidades habrá de procurarse realizar pruebas para explotar las mismas (Metasploit Framework puede ser usado para este fin); finalmente de acuerdo a los resultados obtenidos se deberán hacer los cambios necesarios y proponer mejoras al sistema de seguridad de la información.

Para limitar vulnerabilidades se aconseja:

En los dispositivos:

- Evitar la ejecución automática desde discos duros.
- Deshabilitar ejecución automática desde unidades de red.
- Deshabilitar ejecución automática desde CD/DVD.
- Deshabilitar ejecución automática de medios extraíbles.

En los navegadores:

- Utilizar versiones actualizadas.
- Configurar la ejecución automática para borrar el historial de direcciones URL visitadas.
- Eliminar cookies al cerrar el navegador.
- habilitar la limpieza automática de la memoria cache al cerrar el navegador.
- Restablecer página de inicio al cerrar el navegador.
- Activar Filtros antiphishing.
- Instalar extensiones o aplicaciones que evitan la ventana emergente (anti pop-up)

Herramientas Recomendadas

- Wireshark
- netstat
- nmap

- Nessus
- Metasploit Framework

12.2.1.3 Todo software que sea instalado en cualquier dispositivo que se conecte a la infraestructura de red de la comuna deberá ser avalado por el Encargado de la Unidad Informática.

12.2.1.4 Es responsabilidad de la Unidad Informática revisar, auditar y documentar de manera periódica el software instalado (Software de Sistema, Software de Programación y Software de Aplicación) junto con el registro de las respectivas licencias de todos y cada uno de los dispositivos informáticos pertenecientes a la comuna.

12.2.1.5 Todo usuario que haga uso de cualquier dispositivo que se conecte a la infraestructura de red de la comuna es responsable de verificar que los archivos a los que acceda se encuentren libre de códigos maliciosos. Para ello deberá estar capacitado en la gestión segura de manejo de antivirus y (de ser posible) firewall personales. De no poder manejar estas herramientas el usuario está en la obligación de informar al Propietario de la información y de los activos para que este solicite al Encargado de la Unidad de Recursos Humanos o al Responsable de la Seguridad Informática que realice las gestiones y se capacite al personal sobre el manejo de las mismas. Además deberá evitar realizar las siguientes acciones:
Antes de la infección

- Abrir archivos de procedencia desconocida.
- Abrir archivos adjuntos, o acceder a enlaces en aquellos correos de procedencia dudosa.
- Brindar información comprometedora a petición de correos no solicitados o de redes sociales.
- Hacer clic en ventanas emergentes que inviten a descargar aplicaciones desconocidas.

- Acceder a sitios impropios.
- Instalar software no autorizado.
- Aceptar certificados de servidor de páginas Web cuando el navegador indica que no lo reconoce.
- Desactivar o alterar las configuraciones de seguridad instaladas en los dispositivos.

Después de la infección

- Desinfectar sin asistencia de la Unidad Informática el dispositivo afectado.
- Conectar dispositivos externos como USB, Discos Externos, etc.
- Enviar correos, visitar sitios web, o accesar a los servicio ofrecidos por la comuna hasta que la Unidad Informática de el aval que el equipo esta desinfectado.

12.2.1.6 Todo usuario que haga uso de cualquier dispositivo que se conecte a la infraestructura de red de la comuna que identifique situaciones anómalas en el comportamiento habitual del mismo o que se entere o tenga sospechas de algún incidente que pueda afectar o comprometer los activos informáticos de la comuna deberá notificar a la brevedad al Encargado de la Unidad a la que pertenece para que este a su vez informe al Responsable de la Seguridad Informática quien iniciara las investigaciones y determinara los procedimientos a ejecutar.

12.3 Objetivo de control: Copias de seguridad.

Implementar una estrategia de respaldo de la información institucional para recuperación de la misma en caso de desastre.

12.3.1 Control: Copias de seguridad de la información.

12.3.1.1 Es obligación del Responsable de la Seguridad Informática establecer los procedimientos a implementar para el adecuado respaldo de la información basándose en las directrices de clasificación del literal 8.2.1.1 de las presentes

políticas. Dicho procedimiento debe cubrir los siguientes criterios:

- Selección del medio adecuado para el almacenamiento de la información
- Realizar copias de la información de manera programada y frecuente (preferentemente de manera automática), para ello se debe considerar la velocidad con la cual se genera, actualiza e inyecta nueva data a los servidores de la comuna.
- Verificar la integridad de todos los respaldos, para identificar fallas del duplicado, con un periodo no mayor a 3 meses.
- Realizar pruebas de recuperación de la información para establecer el tiempo requerido para rescatar la data en caso de incidentes.
- Almacenar un juego de las copias de la información respaldada en un dispositivo distinto y distante de donde se encuentre alojada la fuente primaria (véase literal 11.1.3.2). Además considérese almacenar una copia virtual en una ubicación remota en la nube.
- Se establecerá un procedimiento para el rotulado, archivado y el documentado de los respaldos a fin de identificarlos oportunamente en caso de algún incidente.
- Ante el cifrado de los respaldos, aplíquese lo establecido en el literal 10.1.1.1 de las presentes políticas.
- Ante el traslado de los respaldos, aplíquese lo establecido en el literal 8.3.3.1 de las presentes políticas.
- Ante la eliminación de los respaldos, aplíquese lo establecido en el literal 8.3.2.1 de las presentes políticas.

12.3.1.2 Es responsabilidad del Encargado de la Unidad Informática de la comuna aplicar las directrices establecidas en el literal anterior (12.3.1.1) e implementara las herramientas necesarias para el adecuado respaldo de la información digital de la comuna. Las herramientas seleccionadas deberán contar con las siguieres características:

- Deberá permitir elegir la periodicidad con la cual se respalde la información.

- Deberá permitir comprimir los archivos respaldados.
- Deberá permitir cifrar la información respaldada.
- Deberá permitir elegir la información a respaldar.
- Deberá permitir seleccionar el método de respaldo a realizar (Completo, Incremental o Diferencial)

Herramientas Recomendadas:

Almacenamiento en la nube

- Amazon Glacier

Sincronización

- Rsync: Sincronización de ficheros

Respaldos

- Mondo Rescue
- Bacula: Backups de varios niveles. (completo, incremental o diferencial)
- fwbackups: Backups de varios niveles.

Base de datos

- SQL Server Management Studio para SQL Server
- mysqldump para MySQL
- pg_dump para PostgreSQL
- Oracle Data Pump y Recovery Manager (RMAN) para Oracle

Protección continúa de datos

- InMage DR-Scout
- RecoverPoint
- AIMstor

13 Dominio: SEGURIDAD EN LAS TELECOMUNICACIONES

13.1 Objetivo de control: Gestión de la seguridad en las redes

Proteger la red informática de la comuna mediante la administración de los accesos a las redes por parte de los objetos del Servicio de Directorio autorizado a ingresar.

13.1.1 Control: Controles de red.

13.1.1.1 El Encargado de la Unidad Informática velara porque la comuna cuente con las herramientas necesarias que permitan controlar, verificar y auditar que la información que es transmitida a través de la infraestructura de red de la alcaldía mantenga su Integridad (se transmita de forma incorrupta), Disponibilidad (la información deberá estar disponible en todo momento), Autenticidad (la data es transmitida/recibida sin que quepa la menor duda quien la envió/recibió) y Confidencialidad (la información es transmitida de manera segura y solo es accedida por las personas autorizadas).

Herramientas Recomendadas:

- IDS: Snort

13.1.1.2 El Encargado de la Unidad Informática implementara una política de dispositivos de red de Cero Puertos Abiertos, la apertura de los mismo habrá de ser evaluada, justificada y documentada, según las necesidades generadas para los servicios informáticos estrictamente necesarios que requieran ser habilitados.

Herramientas Recomendadas:

- nmap

13.1.1.3 El Encargado de la Unidad Informática será el responsable de deshabilitara la opción de obtención automática DNS de todos los host clientes que no requieran, o no estén autorizados a establecer conexiones web.

13.1.1.4 Deberá estructurarse la asignación de IP´s a todos los host clientes que sean incorporados a la red de la comuna a manera de mantener el orden entre los dispositivos.

Recomendaciones:

A manera de ejemplo ante la existencia de una sola red podría utilizarse un pool de valores IP como los mostrados en la siguiente tabla:

Dispositivo	**Pool de IP´s**
Impresores	xx.xx.xx.10 a la xx.xx.xx.20
PC´s	xx.xx.xx.40 a la xx.xx.xx.150
Laptops	xx.xx.xx.160 a la xx.xx.xx.200
Móviles	xx.xx.xx.210 a la xx.xx.xx.240
Otros, etc.	xx.xx.xx.245 a la xx.xx.xx.250

Tabla 7-1: Ejemplo de Propuesta de asignación de IPs según dispositivo

13.1.1.5 Ante el ofrecimiento de acceso a las redes de la comuna sea desde el interior de la misma o de manera remota es obligación del Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática determinar que Objetos (usuarios, grupos, dispositivos, etc.) del Servicios de Directorio (SD) tendrán acceso a que redes y a cuales servicios. Para ello se considerara las directrices de clasificación establecidas en el literal 8.2.1.1 de las presentes políticas. (Deberá responderse a la pregunta: ¿a qué quieren acceder y a través de que dispositivos?).

Herramientas Recomendadas:

SO: Linux (Gratuita):

- Zentyal Server
- CentOS Directory Server

Otros (Gratuita)

- ApacheDS
- OpenDS
- OpenLDAP

SO Windows: (de paga)

- Active Directory

SO: Mac OS X

- Open Directory

13.1.1.6 Es responsabilidad del Encargado de la Unidad Informática validar que los dispositivos y usuarios autorizados a establecer conexiones a las redes de la comuna, sea desde el interior de la misma o de manera remota, que solo acecen a los servicios a los cuales se les haya autorizado. De detectar conexiones sin autorización o movimientos sospechosos informara al Responsable de la Seguridad Informática para que en conjunto definan las acciones a seguir.

13.1.1.7 Es obligación del Responsable de la Seguridad Informática analizar y estudiar la necesidad de autorizar/revocar las solicitudes de conexiones remotas junto con el impacto de validar o no el ofrecimiento de este servicio (Deberá responderse a la pregunta: ¿quiénes y por qué requieren acceso remoto?).

13.1.1.8 El Encargado de la Unidad Informática será el responsable de instaurar las herramientas y/o dispositivos necesarias que permitan el establecimiento de conexiones remotas de manera segura. Ello con el fin de reducir los riesgos asociados en la copia y/o alteración de información sensible.

Herramientas Recomendadas:

- OpenVPN
- *VPN IPSec*
- FileZilla Server/Client
- HotSpot Shield

13.1.1.9 Los permisos de acceso para el establecimiento de conexiones remotas deberá limitarse (habilitarse/bloquearse) a ciertos intervalos de tiempo a lo largo de la semana.

13.1.1.10 El Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática podrán autorizar suspender parcialmente o totalmente la transferencia y/o manipulación de la información y/o servicios informáticos brindados, si detectan o son alertados sobre deficiencias o anomalías severas que comprometan y pongan bajo riesgo la seguridad de la información que se encuentra almacenada y/o que es transmitida a través de la infraestructura de red LAN de la alcaldía. Para ello deberán contar con un plan de contingencia para reactivar a la brevedad los servicios suspendidos. Siendo entonces obligación del Responsable de la Seguridad Informática, brindar informes sobre las razones de la suspensión/reactivación de los servicios al Comité de Seguridad de la Información.

13.1.1.11 El Responsable de la Seguridad Informática podrán proponer al Comité de Seguridad de la Información la necesidad de auditar la red informática de la comuna (mediante por ejemplo un test de penetración) para realizar una evaluación de las medidas de seguridad informática adoptadas y encontrar vulnerabilidades no detectadas.

13.1.2 Control: Mecanismos de seguridad asociados a servicios en red.

13.1.2.1 Es responsabilidad del Encargado de la Unidad Informática asegurarse que

todo dispositivo informático (ROUTER) que se incorpore a la infraestructura de red de la comuna sea configurado considerando todas las medidas de seguridad aplicables. Ello incluye (entre otras):

- Modificar las credenciales de acceso establecidas por defecto.
- Asignar contraseña segura.
- Desactiva la difusión del identificador de red SSID (Service Set Identifier)
- Configurar el tipo de cifrado de red.
- Limitar el número de conexiones.
- Evaluar desactivar el DHCP
- Configurar el router para que únicamente sea administrable via LAN y no WiFi.
- Desactiva el protocolo TR-069 o CWMP

13.1.2.2 Las claves para conexión a redes inalámbricas deberá verificarse y modificarse al menos una vez cada seis meses, y es obligación del Encargado de la Unidad Informática controlar que solo dispositivos autorizados hagan uso de este servicio.

13.1.2.3 El Encargado de la Unidad Informática en coordinación con el Responsable de la Seguridad Informática serán los responsables de definir los distintos tipos de tráficos que circula a través de la infraestructura de red de la comuna, a modo de identificar aquellos de mayor importancia (categorizándolos por Clase de tráfico). Posterior a la clasificación se establecerán las reglas a instituir que permitan administrar los anchos de banda máximos y mínimos (a través de la Gestión de Ancho de Banda) que serán aplicados al control de tráfico (QoS: Quality of Service). La revisión de las reglas y categorización de clases habrá de llevarse a cabo, de manera rigurosa, al menos una vez por año.

13.1.3 Control: Segregación de redes.

13.1.3.1 El Encargado de la Unidad Informática en coordinación con el Responsable

de la Seguridad Informática serán los responsables de determinar la mejor forma de organizar la arquitectura de red de la comuna; para ello será necesario distinguir y establecer fronteras entre: redes locales; redes privadas de otras organizaciones (por ejemplo las establecidas entre la comuna y el ministerio de hacienda); redes dedicadas en la nube y redes externas o publicas cuyos accesos habrán de ser controlados.

13.1.3.2 La subdivisión de redes deberá hacerse en torno al valor de la información ofrecida de acuerdo a su nivel de sensibilidad conforme la clasificación establecida en el literal 8.2.1.1 de las presentes políticas.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Objetivo de control: Requisitos de seguridad de los sistemas de información.

Garantizar la inclusión de la seguridad en los sistemas informáticos desarrollados por la alcaldía, proveedores o asignados a terceros.

14.1.1 Control: Análisis, diseño y especificaciones de los requisitos de seguridad.

14.1.1.1 Ante el desarrollo y/o adquisición de software solicitado por cualquier unidad organizacional de la comuna será el Responsable de la Seguridad Informática en coordinación con el Propietario de la información y de los activos a cargo de dicha unidad quienes definirán las especificaciones requeridas y los niveles de protección requeridos acorde al nivel de sensibilidad de la información a administrar según se establece en las directrices de clasificación del literal 8.2.1.1 de las presentes políticas.

14.1.1.2 Para todo proyecto de desarrollo y/o adquisición de software informático es responsabilidad del Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática considerar lo siguiente:

- Incorporación de las especificaciones requeridas (según lo definido en el literal 14.1.1.1)
- Definir los controles de seguridad a aplicar desde la fase de análisis y diseño del sistema (tomando en cuenta que la mayoría de los errores de seguridad surgen en la etapa de diseño). Además se definirán la arquitectura a utilizar, el modo de autenticación, privilegios, derechos de acceso, etc. (véase literal 9.2 sobre Gestión de Acceso de usuarios).
- El establecimiento de los controles de validación de datos de entrada,

procesamiento y salida.

- Determinar las técnicas de encriptación a utilizar (tales como: cifrado simétrico, asimétrico, funciones de dispersión y firmas digitales).

Observación

Si el sistema es adquirido o desarrollado por tercero habrá que efectuarles pruebas de seguridad a fin de verificar si cumple con los requerimientos solicitados.

14.2 Objetivo de control: Seguridad en los procesos de desarrollo y soporte.

Proteger la información y los sistemas de aplicaciones adquiridos o desarrollados por la comuna.

14.2.2 Control: Procedimientos de control de cambios

14.2.2.1 De ser necesario la modificación, mejora o actualización de algún sistema informático será el jefe encargado de la unidad interesada (que ha sido designado como Propietarios de la información y de los activos) quien deberán realizar la solicitud junto con la respectiva justificación al Responsable de la Seguridad Informática. Este a su vez deberá requerir al Encargado de la Unidad Informática, a fin de:

- Evaluar el impacto de las modificaciones solicitadas.
- Realizar un análisis de riesgo de los cambios solicitados.
- Establecer los nuevos requisitos de seguridad.

De ser factibles las modificaciones el Responsable de la Seguridad Informática propondrá las modificaciones al Comité de Seguridad de la Información para su aprobación formal.

14.2.2.2 Ante la necesidad de realizar modificaciones o mejoras a los sistemas informáticos se deberán establecer controles durante la implementación de cambios de los mismos a fin de garantizar que las modificaciones a realizar no comprometan

la seguridad ni los controles existentes para ello se deberá tener presente lo siguiente:

- El Propietario de la información y de los activos a cargo de la unidad del área donde se realizaran las modificaciones deberá de avalar el proceso, si dichos cambios afectasen los sistemas de procesamiento de la información que está bajo su custodia.
- Las pruebas a realizar para efectuar las modificaciones habrán de efectuarse en un entorno de desarrollo o ambiente de desarrollo y pruebas (separado del sistema instalado).
- Sobres las gestiones de cambios a realizar en los sistemas se deberá mantener un control de versiones de todas las modificaciones efectuadas.
- Se deberá mantener un registro de todos los cambios realizados.
- Se deberá actualizar toda la documentación referente al sistema (manual de usuario, manual técnico, manual de instalación solo si los efectos del cambio afectaron dicho proceso, etc.)
- Procurar que el proceso de mejoras afecte lo mínimo las operaciones normales de la comuna.

14.2.3 Control: Revisión técnica de las aplicaciones tras efectuar cambios al sistema operativo.

14.2.3.1 De existir necesidad de actualizar o modificar el sistema operativo (mediante por ejemplo: parches u otras actualizaciones críticas) en aquellos dispositivos que contengan sistemas de aplicaciones, desarrollados por la alcaldía o contratados a terceros. Será responsabilidad del Encargado de la Unidad Informática el verificar y comprobar lo siguiente:

- Que los sistemas de aplicaciones instalados en los dispositivos donde se efectuó el cambio operen con toda normalidad y mantengan su integridad.
- Que los controles de seguridad de los sistemas o aplicaciones no se hayan visto afectados.

- Que el proceso de actualización y pruebas interfiera lo mínimo posible las operaciones normales de la comuna.

14.2.4 Control: Restricciones en los cambios a los paquetes de software.

De existir la estricta necesidad de modificar un software adquirido a proveedores o desarrollado por terceros Será responsabilidad del Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática el verificar lo siguiente:

- Que el contrato de licencia del sistema informático autorice efectuar las modificaciones.
- Que de poder realizarse la modificación sin afectar el contrato de licenciamiento habrá que evaluar la factibilidad de quien será el responsable de realizar las modificaciones (si será la alcaldía, si se solicitar asistencia del proveedor o se asignaran las modificaciones a terceros.)
- Que de efectuarse las modificaciones, la alcaldía deberá efectuar los cambios sobre una copia del sistema original documentado los cambios efectuados según lo establecido en el literal 14.2.2.2 de la presente cláusula.

14.2.7 Control: Desarrollo externo de software.

14.2.7.1 De autorizar a terceros la elaboración de cualquier sistema informático es responsabilidad del Responsable de la Seguridad Informática en coordinación con Encargado de la Unidad Informática y el apoyo del encargado de la Unidad Jurídica el tener en cuenta las siguientes consideraciones (aplica lo establecido en el literal 14.1.1.2 de la presente clausula):

- Establecer un acuerdo que garantice el compromiso de las partes donde se estipulen los requerimientos a implantar del sistema.
- Convenir los derechos de licencia sobre el sistema (permisos de uso, modificación, actualización, distribución, etc.)

- Garantía de aplicación de los controles de seguridad solicitados.
- Garantía de calidad del producto terminado.
- Acuerdo de custodia del código fuente del sistema.
- Establecer las obligaciones de encontrarse anormalidades (falla, vulnerabilidades, inconsistencias, etc.)

14.2.8 Control: Pruebas de funcionalidad durante el desarrollo de los sistemas.

14.2.8.1 Es responsabilidad del Encargado de la Unidad Informática en coordinación con Responsable de la Seguridad Informática verificar que, ante todo sistema informático desarrollo por la alcaldía, se realicen las pruebas de funcionalidad para verificar que la aplicación ejecute las tareas definidas según las especificaciones requeridas. Pudiendo efectuarse variedad de pruebas, tales como:

- Pruebas de compatibilidad (verificando su funcionalidad dentro de la variedad de navegadores existentes, comportamiento en la red LAN, comportamiento ante el hardware, etc.)
- Pruebas de regresión para controlar que ante cualquier corrección efectuada no se altere el correcto funcionamiento de lo que ya se comprobó que opera satisfactoriamente.
- Pruebas de integración para verificar como interactúa la aplicación entre los componentes de un mismo sistema, con otras aplicaciones, etc.

14.2.9 Control: Aprobación del sistema.

14.2.9.1 Es responsabilidad del Encargado de la Unidad Informática en coordinación con Responsable de la Seguridad Informática determinaran los criterios para la aprobación de nuevos sistemas informáticos, actualización o mejoras, sean estos desarrollados por la alcaldía, proveedores o asignados a terceros. Ante ello habrán de considerar lo siguiente:

- Si se cumple con los requisitos mínimos del hardware necesario.

- Verificar los procedimientos de recuperación de errores y reinicio del sistema.
- Realizar pruebas de los procedimientos operativos de rutina (a fin de verificar que los mismos valores de entrada generen los mismos valores de salida).
- Verificar que la interfaz del sistema sea intuitivo, de fácil comprensión y evite confusiones que puedan generar errores humanos.
- Determinar el impacto que el nuevo sistema tendrá en el entorno de seguridad informática establecido.
- Garantizar que la instalación del nuevo sistema no interfiera con otros sistemas informáticos ya existentes.
- Verifica que la instalación del nuevo sistema afecte lo mínimo posible las operaciones normales de la alcaldía.
- Aplicar lo establecido en el literal 14.1.1.2 de la presente clausula.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

16.1 Objetivo de control: Gestión de incidentes de seguridad de la información y mejoras.

Establecer las operaciones a realizar para la prevención, afronta y resolución de incidentes, si los hubiere, que afecten la infraestructura de red de la municipalidad.

16.1.1 Control: Responsabilidades.

16.1.1.1 El Encargado de la Unidad Informática en coordinación con el Responsable de la Seguridad Informática serán los responsables de proponer las estrategias que permitan prever riesgos y amenazas que intenten afectar la infraestructura de red de la municipalidad y deberán además establecer las tácticas de contingencia y de reacción a implementar ante eventos informáticos (Véase: 6.1.4.1).

16.1.2 Control: Notificación de los eventos de seguridad de la información.

16.1.2.1 Es responsabilidad del Responsable de la Seguridad Informática establecer el procedimiento y los mecanismos a seguir para canalizar de manera oportuna todo incidente identificado por cualquier usuario que haga uso de los servicios tecnológicos institucionales. Para ello se habrá tener en cuenta lo siguiente:

- Deberá existir un punto de contacto donde se notifique del incidente.
- Deberá existir el canal para la notificación del incidente al cual acuda la persona que informa del incidente.
- El punto de contacto deberá ser conocido por todos los usuarios que cuenten con un ID (login) otorgado por la comuna (según lo establecido en el literal 9.2.1.1 de las presentes políticas).

16.1.3 Control: Notificación de puntos débiles de la seguridad

16.1.3.1 Todo usuario que haga uso de los servicios tecnológicos de la comuna deberá seguir el procedimiento establecido en las presentes políticas para reportar de manera inmediata cualquier actividad o situación inusual que sea detectada. De presentarse alguna anormalidad se deberán seguir las siguientes acciones:

- Registrar las alertas y mensajes que aparecen en pantalla o el comportamiento anormal del equipo (Deberá estar capacitado según lo establece el literal 12.2.1.5).
- Informar de la anomalía detectada al Encargado de la Unidad a la que pertenece para que este informe al Responsable de la Seguridad Informática (véase además los literales 12.2.1.6 y 18.2.2.3).
- Abstenerse de realizar más operaciones en el dispositivo implicado en el incidente y esperar la asistencia técnica.

16.1.4 Control: Valoración de eventos de seguridad de la información y toma de decisiones.

16.1.4.1 Es Responsabilidad del Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática el valorar y categorizar los eventos que pudiesen generar incidentes que afectasen la infraestructura informática de la comuna, entre los que se habrán de considerar:

- Efectos generados por códigos maliciosos (véase controles contra código malicioso 12.2.1).
- Efectos o Actos vandálicos generados por ataques masivos de denegación de servicios.
- Efectos generados por la interrupción prolongada en los servicios de red.
- Efectos generados por un inadecuado procedimiento en la generación de respaldos (Respaldos corrompidos o desactualizados) (Véase literales 12.3.1.1 y 12.3.1.2 sobre copias de seguridad).

- Efectos ocasionados por actos indebidos intencionales o no en la manipulación de los activos informáticos.
- Efectos generados por siniestros naturales.

16.1.4.2 Es Responsabilidad del Responsable de la Seguridad Informática en coordinación con el Encargado de la Unidad Informática el procurar anticiparse a los incidentes mediante el establecimiento de una estrategia proactiva a fin de:

- Prever el incidente.
- Establecer el posible daño al activo informático de generarse el incidente.
- Establecer previamente el plan de contención a implementar en dado caso se presente el incidente.

16.1.5 Control: Respuesta a los incidentes de seguridad.

16.1.5.1 Ante cualquier incidente generado es responsabilidad del Encargado de la Unidad Informática en coordinación con el Responsable de la Seguridad Informática establecer el plan de contingencia y las medidas de corrección a aplicar considerando los siguientes aspectos:

Ante el incidente:

- Determinar las acciones iniciales a efectuar.
- Investigar y establecer el origen del incidente.
- Contener el incidente.
- Establecer las medidas correctivas a aplicar para prevenir eventos similares en el futuro.
- Establecer comunicación con el usuario afectado por el incidente.
- Notificar al Comité de Seguridad.

Durante el incidente:

- Verificar que únicamente personal con privilegios categorizados según lo establecido en el literal 11.1.2.1 de estas políticas y de ser necesario el apoyo de personal externo certificado especialista en incidentes (vease18.2.2.3)

puedan acceder a los datos vivos del sistema.

- Documentar todas las operaciones realizadas para la resolución del incidente.
- Informar de las acciones emprendidas al Comité de Seguridad de la Información.
- Verificar la integridad de los sistemas y la continuidad de las operaciones en el menor tiempo posible.

16.1.7 Control: Recopilación de evidencias

16.1.7.1 Es responsabilidad del Encargado de la Unidad Informática recolectar todas las evidencias para determinar responsabilidades de las causales del incidente:

- Para búsqueda de fallas internas.
- Para verificar si se ha violentado alguna de las presentes políticas u otra obligación contractual por parte del personal que ha hecho uso impropio de los servicios institucionales.
- Para solicitar compensación a los proveedores de servicios tecnológicos (ello si se determina que el incidente fue causado por fallas en algún dispositivo o servicio tecnológico que se encuentre bajo contrato. Entre ellos se deben incluir: Incidentes generados por fallas ocasionadas por aires acondicionados, malas Instalaciones eléctricas y/o redes, fallas en elementos periféricos informáticos, fallas en dispositivos de red, fugas de cualquier tipo, prolongadas interrupciones en servicios de telecomunicaciones, etc.).

Recomendaciones:

Para la preparación de un plan de contingencia ante incidentes informáticas puede recurrirse a la norma NIST SP 800-34 Rev. 1 (Contingency Planning Guide for Federal Information).

18. CUMPLIMIENTO

18.2 Objetivo de control: Revisiones de la seguridad de la información.

18.2.2 Control: Cumplimiento de las políticas y normas de seguridad.

18.2.2.1 Los miembros del Consejo Municipal son los responsables de brindar con el ejemplo el fiel cumplimiento de la presente normativa al cual también se someten.

18.2.2.2 Todo el personal que forme parte de la estructura organizacional es responsable de acatar lo establecido en las presentes políticas y de contribuir en la salvaguarda de los activos informáticos institucionales de la comuna.

18.2.2.3 Todo el personal que forme parte de la estructura organizacional de la comuna y haga uso de los servicios informáticos de la misma está en la obligación de notificar al jefe encargado/a de la unidad que haya sido designado como Propietario de la información y de los activos, sobre irregularidades, situaciones impropias o cualquier actividad sospechosa que a su criterio pueda afectar las operaciones informáticas institucionales. A su vez el Propietario de la información y de los activos deberá reportar inmediatamente (si la situación así lo amerita) sobre el incidente al Responsable de la Seguridad Informática quien habrá de tomar las acciones pertinentes. Quien de ser necesario solicitara apoyo al Comité de Seguridad de la Información para que en caso extremo; solicite asesoría a consultores certificados especialistas en Respuesta a Incidentes de Seguridad en Computadores (CSIRT).

POLÍTICAS DE SEGURIDAD

Apéndice

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
- 5.1.1 Conjunto de políticas para la seguridad de la información.
- 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.
- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
- 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.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.
- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los 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.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
- 12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
- 12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
- 12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

Carta de asignación de control de acceso de la
Alcaldía de *(nombre de la alcaldía)*

Yo _____en mi carácter de usuario/a designado/a para el cargo de_____ de la unidad o departamento de_____ , este día se me hace entrega de la cuenta de acceso y contraseña provisional para ser utilizada en la Alcaldía *(nombre de la alcaldía)* el cual entiendo me acreditan permisos para hacer uso de los servicios tecnológicos ofrecidos por la comuna para desempeñar mis labores profesionales; que hoy acepto, junto a las obligaciones generadas por el uso de la Cuenta de usuario de acuerdo a los permisos que se otorgan acorde al perfil del puesto al que he sido asignado/a, así como a las penalidades en que pudiera incurrir en materia de responsabilidad del Control de Accesos por el uso de la información, incluso aquella considerada como confidencial, de conformidad con lo establecido en las leyes y normativa vigente aplicable para tal efecto.

- La cuenta de acceso es personal, única e intransferible.
- La contraseña provisional asignada habrá de ser modificada en los próximos 3 días acorde a las políticas de seguridad.
- La contraseña provisional y las subsecuentes contraseñas deberán ser de índole personal (individual), secreta, segura pero de fácil recordación (mínimo 8 caracteres de tipo alfanuméricos) y deberá ser resguardada de manera apropiada (evitando que sea descubierta).
- En caso de sospecha que la contraseña provisional y las subsecuentes contraseñas han sido apropiada o está siendo manipulada por personas distintas a la asignada; el usuario propietario deberá modificarla inmediatamente. Si la situación se vuelve recurrente el usuario propietario deberá de informar sobre la anomalía al Propietario de la información y los activos para que este notifique al Responsable de la Seguridad Informática, quien deberá realizar las acciones correspondientes.
- Queda estrictamente prohibido compartir la cuenta de acceso y contraseña con otras personas.
- En caso de que el usuario cambie su rol a uno que posea privilegios de acceso distinto al cargo anteriormente desempeñado o se reubique en otra unidad o departamento dentro de la comuna, deberá notificarlo al Propietario de la información y los activos quien a su vez notificara al Responsable de la Seguridad Informática para realizar las acciones correspondientes.
- La información almacenada y ofrecida través de los servicios tecnológicos de la comuna es propiedad de la Alcaldía y solo será utilizada para realizar las tares laborales asignadas.
- Es obligación del usuario garantizar la confidencialidad de la información a la cual se tenga accesos, en caso contrario se procederá jurídicamente según sea el caso.
- De incumplir alguno de los ítems antes descritos el usuario será sancionado según lo establecido.

Quedando de enterado de los estatutos mencionados firmo de conformidad a lo establecido por El Comité de Seguridad de la Información de la alcaldía.

_____
Firma de Aceptación

Cuenta de usuario (ID/login):_____ Password (provisional):_____

Autorizada por: _____

Guía para la conformación de las Políticas de Seguridad

Para ser adoptadas por la Alcaldía de (nombre de la alcaldía)

Objetivo

Brindar un recomendable sobre la estructura que pudiesen tener las Políticas de Seguridad a ser adoptadas dentro de la Alcaldía de (nombre de la alcaldía). Al mismo tiempo se sugieren clausulas, dominios o secciones que deberían ser considerados para la puesta en marcha del documento.

1	**Sobre las políticas**	Recomendable incluir
	Puede contener Información general sobre las políticas y su aplicación dentro de la comuna; sobre seguridad informática u otros aspectos relevantes a aplicar en el documento. Pudiendo contener:	
	Introducción	
	Objetivos	
	Limitaciones	
	Generalidades	
	Beneficios	
2	**Términos y Consideraciones**	Recomendable incluir
	Puede incluir un glosario sobre los términos que se usan en las políticas desarrolladas.	
3	**Estructura de las presentes Políticas de Seguridad**	Recomendable incluir
	Puede proyectarse la forma en que se conforman las políticas, debiendo incluir el listado de todos los dominios seleccionados.	
4	**Evaluación de riesgos de la Alcaldía**	Recomendable incluir
	Puede incluir un estudio de evaluación de riesgos a los cuales puede verse expuesta la comuna.	
5	**Dominio: POLÍTICAS DE SEGURIDAD**	Obligatorio
	Objetivo de control 5.1 Directrices de la Dirección en seguridad de la información	Obligatorio
	Control 5.1.1: Conjunto de políticas para la seguridad de la información	Obligatorio
	Control 5.1.2: Revisión de las políticas para la seguridad de la información	Obligatorio
6	**Dominio: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**	Obligatorio
	Objetivo de control 6.1: Organización interna	Obligatorio
	Control 6.1.1: Asignación de responsabilidades para la seguridad de la información	Obligatorio
	Control 6.1.x	Elegir según necesidad
7	**Dominio: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**	Elegir según necesidad
	Objetivo de control 7.x:	Elegir según necesidad
	Control 7.x.x:	Elegir según necesidad
8	**Dominio: GESTIÓN DE ACTIVOS**	Elegir según necesidad

	Objetivo de control 8.x:	Elegir según necesidad
	Control 8.x.x:	Elegir según necesidad
9	**Dominio: CONTROL DE ACCESOS**	Elegir según necesidad
	Objetivo de control 9.x:	Elegir según necesidad
	Control 9.x.x:	Elegir según necesidad
10	**Dominio: CIFRADO**	Elegir según necesidad
	Objetivo de control 10.x:	Elegir según necesidad
	Control 10.x.x:	Elegir según necesidad
11	**Dominio: SEGURIDAD FÍSICA Y AMBIENTAL**	Elegir según necesidad
	Objetivo de control 11.x:	Elegir según necesidad
	Control 11.x.x:	Elegir según necesidad
12	**Dominio: SEGURIDAD OPERATIVA**	Elegir según necesidad
	Objetivo de control 12.x: Elegir según necesidad	Elegir según necesidad
	Control 12.x.x:	Elegir según necesidad
13	**Dominio: SEGURIDAD EN LAS TELECOMUNICACIONES**	Elegir según necesidad
	Objetivo de control 13.x:	Elegir según necesidad
	Control 13.x.x:	Elegir según necesidad
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**	Elegir según necesidad
	Objetivo de control 14.x:	Elegir según necesidad
	Control 14.x.x:	Elegir según necesidad
15	**RELACIONES CON SUMINISTRADORES**	Elegir según necesidad
	Objetivo de control 15.x:	Elegir según necesidad
	Control 15.x.x:	Elegir según necesidad
16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**	Elegir según necesidad
	Objetivo de control 16.x:	Elegir según necesidad
	Control 16.x.x:	Elegir según necesidad
17	**CONTINUIDAD DEL NEGOCIO**	Elegir según necesidad
	Objetivo de control 17.x:	Elegir según necesidad
	Control 17.x.x:	Elegir según necesidad
18	**CUMPLIMIENTO**	Elegir según necesidad
	Objetivo de control 18.x:	Elegir según necesidad
	Control 18.x.x:	Elegir según necesidad

Recomendable incluir	Es necesario para mantener un orden numérico más no obligatorio.	
Obligatorio	Para que cualquier Política de Seguridad cuente con el apoyo y la participación de las máximas autoridades es obligatorio que estas incluyan los Objetivos de control 5.1 y 6.1	
Elegir según necesidad	Dominios, Objetivos de control y Controles que pueden ser seleccionados según requerimientos de cada institución.	

Guía para la selección de controles de las Políticas de Seguridad Para ser adoptadas por la Alcaldía de (nombre de la alcaldía)

Objetivo

Proponer un bosquejo sobre cada uno de los controles propuestos en las presentes Políticas de Seguridad para que la Alcaldía de (nombre de la alcaldía) seleccione los que mejor se acomoden a sus necesidades.

5. Dominio: POLÍTICAS DE SEGURIDAD

Objetivo				
Establecer el conjunto de políticas a aplicar, mediante la descripción de los Dominios, Secciones o Clausulas a considerar, que contribuyan a generar el plan de acción a seguir en la gestión de seguridad informática con el objeto de contribuir en minimizar amenazas y proteger los activos informáticos de la comuna				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
5.1	Directrices de la Dirección en seguridad de la información	5.1.1	Conjunto de políticas para la seguridad de la información	Ordena la creación de políticas y los dominios que se han de considerar.
		5.1.2	Revisión de las políticas para la seguridad de la información	Insta a la revisión constante de las políticas para adecuarla a los cambios futuros.

6. Dominio: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo				
Tiene como finalidad establecer responsabilidades para la seguridad de la información y el contacto con los grupos de interés especial				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
6.1	Organización interna	6.1.1	Asignación de responsabilidades para la seguridad de la información.	Propone: • Conformar el Comité de Seguridad. • Selección del Responsable de la Seguridad Informática • Asignar responsabilidades al resto de las unidades organizacionales
		6.1.4	Contacto con grupos de interés especial	Autoriza al Responsable de la Seguridad Informática solicitar asesoría de especialistas externos expertos en seguridad informática

7. Dominio: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Objetivo				
Determinar las obligaciones contraídas, en materia de seguridad informática, por todo el personal que se incorpora o que labora en la institución.				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
7.1	Sobre las contrataciones	7.1.2	Términos y condiciones de contratación.	Establece indicaciones para la gestión de contratación de personal. **Responsables** • RRHH • El Comité de Seguridad • El Responsable de la Seguridad Informática.
7.3	Cese o cambio de puesto de trabajo.	7.3.1	Cese o cambio de puesto de trabajo.	Establece indicaciones sobre la promoción o remoción de personal. **Responsables** • RRHH • El Responsable de la Seguridad Informática • Los Propietario de la información y los activos.

8. Dominio: GESTIÓN DE ACTIVOS

Objetivo				
Controla el uso aceptable y correcto resguardo de los activos institucionales				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
8.1	Responsabilidad sobre los activos	8.1.1	Inventario de activos	Propone inventariar y mantener actualizado los activos informáticos asignados en custodia por cada unidad organizacional de la comuna. **Responsables** • Los Propietario de la información y los activos. • La Unidad Informática. Propone clasificar la información conforme al grado de sensibilidad de la misma **Responsables** • Los Propietario de la información y los activos. • El Responsable de la Seguridad Informática
8.2	Clasificación de la información.	8.2.1	Directrices de clasificación	Plantea una tabla de clasificación de la información de acuerdo a su nivel de sensibilidad (Acoplada a Ley de acceso a la información Pública LAIP)
8.3	Manejo de los soportes de almacenamiento.	8.3.1	Gestión de soportes extraíbles	Propone controlar los dispositivos de almacenamiento externo. Además a instaurar herramientas que permitan administrar la instalación de los mismos, para reducir los riesgos asociados en la copia de información sensible.

				Responsables • La Unidad Informática Insta a capacitar a todo usuario autorizado a manipular dispositivos con información sensible en la gestión segura y manejo de información confidencial.
		8.3.2	Eliminación de soportes	Establece responsabilidades para el procedimiento del borrado seguro de la información.
		8.3.3	Soportes físicos en tránsito	Directriz para el manejo de dispositivos informáticos en tránsito.

9. Dominio: CONTROL DE ACCESOS

<table>
<tr><th colspan="5">Objetivo</th></tr>
<tr><td colspan="5">Administra los accesos lógicos de los usuarios a sistemas y aplicaciones.</td></tr>
<tr><th>Numeral</th><th>Objetivo de control</th><th colspan="2">Controles</th><th>Descripción</th></tr>
<tr><td rowspan="2">9.1</td><td rowspan="2">Requisitos de negocio para el control de accesos.</td><td>9.1.1</td><td>Política de control de accesos.</td><td>Ordena la creación de políticas de control de control de acceso a dispositivos informáticos.</td></tr>
<tr><td>9.1.2</td><td>Control de acceso a las redes y servicios asociados</td><td>Ordena la creación de políticas de control de acceso a servicios de red y conexiones remotas.</td></tr>
<tr><td rowspan="2">9.2</td><td rowspan="2">Gestión de acceso de usuario.</td><td>9.2.1</td><td>Gestión de altas/bajas en el registro de usuarios</td><td>Establece el proceso y las obligaciones para la asignación y/o retiro de un identificador ID a toda persona que haga uso de los servicios informáticos ofrecidos por la comuna.
Responsables
• Cada empleado que reciba un identificado ID.
• Los Propietario de la información y los activos.
• El Responsable de la Seguridad Informática.
• La Unidad Informática
Propone la adopción e implementación de herramientas para monitorear y restringir accesos no autorizados.
Responsables
• La Unidad Informática</td></tr>
<tr><td>9.2.2</td><td>Gestión de los derechos de acceso asignados a usuarios y revisión</td><td>Insta a la revisión periódica de los derechos de acceso asignados a usuarios.</td></tr>
</table>

			de los derechos de acceso de los usuarios.	
		9.2.3	Gestión de los derechos de acceso con privilegios especiales	Directriz para la solicitud de modificación de privilegios a otro diferentes a los originalmente asignados.
9.4	Control de acceso a sistemas y aplicaciones.	9.4.3	Gestión de contraseñas de usuario	Establece controles para la validación de contraseñas seguras.

10. Dominio: CIFRADO

Objetivo				
Propone técnicas criptográficas basadas en estándares para proteger la confidencialidad, autenticidad o integridad de la información.				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
10.1	Controles criptográficos.	10.1.1	Política de uso de los controles criptográficos.	Directriz para Implementar procesos y técnicas de criptografía para salvaguardar y proteger la información digital de la comuna. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática

11. Dominio: SEGURIDAD FÍSICA Y AMBIENTAL

Objetivo				
Su finalidad es la de proteger la integridad física de las instalaciones y de los equipos contra amenazas externas y ambientales.				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
11.1	Áreas seguras	11.1.1	Perímetro de seguridad física	Insta a establecer un perímetro de seguridad física en áreas que alojen dispositivos informáticos que contengan información sensible.
		11.1.2	Controles físicos de entrada	Propone acreditar y catalogar al personal autorizado a ingresar a áreas que alojen equipo informático con información sensible. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática Insta a Implementar controles físicos de entrada en áreas a resguardar.
		11.1.3	Seguridad de oficinas, despachos y recursos	Proporciona indicaciones para acondicionar y asegurar áreas que alojen dispositivo informáticos. Propone el resguardo de backups en ubicaciones distantes entre sí.
		11.1.4	Protección contra las amenazas externas y ambientales.	Propone evaluar y analizar los riesgos a los que se exponen las instalaciones para afrontar amenazas externas y ambientales.
		11.1.5	El trabajo en áreas seguras	Proporciona indicaciones para encubrir las áreas seguras.
11.2	Seguridad de los equipos.	11.2.1	Emplazamiento y protección de equipos	Proporciona indicaciones sobre del buen cuido, uso y manejo del equipo informático.

				Responsables • Cada empleado que haga uso de equipo informático. Proporciona indicaciones sobre el traslado o movilización de dispositivos informáticos. **Responsables** • Los Propietario de la información y los activos. • La Unidad Informática
		11.2.2	Instalaciones de suministro	Insta a la protección de equipos informáticos con contra fallos y/o cortes energéticos.
		11.2.3	Seguridad del cableado	Insta a la planificación del cableado apropiado en tendidos eléctricos y de telecomunicaciones.
		11.2.4	Mantenimiento de los equipos	Establece directrices para el mantenimiento preventivo y correctivo de los dispositivos informáticos **Responsables** • Los Propietario de la información y los activos. • La Unidad Informática
		11.2.5	Salida de activos fuera de las dependencias de la empresa	Insta a implementar controles que garanticen la salida, el traslado y retorno seguro de los activos informáticos. **Responsables** • Los Propietario de la información y los activos. • La Unidad Informática
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Directriz para la custodia y traslado seguro de los activos informáticos fuera de la comuna.

		11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	Directriz para desechar equipo en desuso.
		11.2.8	Equipo informático de usuario desatendido	Indicación sobre protección de equipo informático cuando el usuario se ausenta.

12. Dominio: SEGURIDAD OPERATIVA

Objetivo				
Establece las responsabilidades y procedimientos de operación, junto a la gestión de vulnerabilidades técnicas.				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
12.2	Protección contra código malicioso.	12.2.1	Controles contra el código malicioso	Proteger la información digital contenida en los dispositivos institucionales y el software en ellos instalados contra códigos maliciosos y vulnerabilidades. **Responsables** • La Unidad Informática. Directriz que indica a los usuarios sobre la utilización segura de software en dispositivos informáticos. **Responsables** • Cada empleado que haga uso de equipo informático
12.3	Copias de seguridad.	12.3.1	Copias de seguridad de la información	Insta a implementar estrategias de respaldo de la información institucional para recuperación de la misma en caso de desastre. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática

13. Dominio: SEGURIDAD EN LAS TELECOMUNICACIONES

Objetivo				
Orientado a asegurar la perfecta gestión de la seguridad en las redes de telecomunicaciones y el intercambio de información con partes externas				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
13.1	Gestión de la seguridad en las redes	13.1.1	Controles de red	Insta a la organizar todo dispositivo informático que integra la red de la comuna. Insta a la protección de dispositivos informáticos contra intrusiones mediante el cierre de puertos. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática Insta a valorar la autorización de conexiones remotas, de autorizarse dicho proceso habrá de realizarse de manera segura. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática
		13.1.2	Mecanismos de seguridad asociados a servicios en red	Insta a cerciorarse que todo dispositivo informático que se incorpore a la infraestructura de red de la comuna sea configurado considerando todas las medidas de seguridad aplicables. **Responsables** • La Unidad Informática

		13.1.3	Segregación de redes	Insta a la planificación de la arquitectura de red, estableciendo fronteras entre: redes locales; redes privadas de otras organizaciones y redes externas. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática

14. Dominio: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivo				
Proteger la información y los sistemas de aplicaciones desarrollados por la alcaldía, proveedores o asignados a terceros.				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
14.1	Requisitos de seguridad de los sistemas de información.	14.1.1	Análisis, diseño y especificaciones de los requisitos de seguridad.	Insta a definir las especificaciones e identificar los requisitos funcionales y los niveles de protección adecuados acordes al nivel de sensibilidad de la información a gestionar. **Responsables** • Los Propietario de la información y los activos. • El Responsable de la Seguridad Informática. • La Unidad Informática
14.2	Seguridad en los procesos de desarrollo y soporte	14.2.2	Procedimientos de control de cambios	Establecer el procedimiento a seguir ante cambios, mejoras o actualizaciones a efectuarse sobre las aplicaciones desarrolladas por la comuna proveedores o terceros. **Responsables** • Los Propietario de la información y los activos. • El Responsable de la Seguridad Informática. • La Unidad Informática
		14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios al sistema operativo	Directriz de verificación a aplicar ante modificaciones a los sistemas operativos que contengan aplicaciones adquiridas, desarrolladas por la

				alcaldía o contratados a terceros. **Responsables** • La Unidad Informática
		14.2.4	Restricciones en los cambios a los paquetes de software	Directriz de verificación a aplicar ante modificaciones a las aplicaciones desarrolladas por la alcaldía, adquiridas a proveedores o contratados a terceros. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática
		14.2.7	Desarrollo externo de software	Establece el procedimiento a seguir ante la autorización de terceros para el desarrollo de software a la medida. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática • La Unidad Jurídica
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Insta a realizar variados tipos de pruebas de funcionalidad a los sistemas en desarrollo para verificar que la aplicación hace lo que se definió. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática
		14.2.9	Aprobación del sistema	Insta a establecer una serie de criterios a considerar para la revisión, aceptación y aprobación de nuevos sistemas informáticos, actualizaciones o mejoras, sean

				estos desarrollados por la alcaldía, proveedores o asignados a terceros. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática

16. Dominio: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Objetivo				
Establecer las operaciones a realizar para incrementar la capacidad de prevención y respuesta a incidentes, si los hubiere, que afecten la infraestructura de red de la municipalidad.				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
16.1	Gestión de incidentes de seguridad de la información y mejoras	16.1.1	Responsabilidades	Establece los responsables de proponer estrategias que permitan prever riesgos y amenazas. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática
		16.1.2	Notificación de los eventos de seguridad de la información	Insta a crear un canal para la notificación de incidentes. **Responsables** • El Responsable de la Seguridad Informática.
		16.1.3	Notificación de puntos débiles de la seguridad	Insta a proponer al personal que haga uso de los servicios o dispositivos informáticos provistos por la comuna a reportar cualquier anormalidad o actividad inusual detectada. **Responsables** Cada empleado que haga uso de equipo informático.
		16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Insta a categorizar los eventos que pueden generar incidentes y la afronta ante los mismos. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática

		16.1.5	Respuesta a los incidentes de seguridad	Insta a establecer un plan de contingencia a aplicar ante el surgimiento de incidentes. **Responsables** • El Responsable de la Seguridad Informática. • La Unidad Informática
		16.1.7	Recopilación de evidencias	Insta a recopilar evidencias para establecer responsabilidades y/o penalidades ante las causales del incidente. **Responsables** • La Unidad Informática

18. Dominio: CUMPLIMIENTO

Objetivo				
Establece la regulación a implementar para garantizar el cumplimiento de las políticas y normas de seguridad de la información.				
Numeral	**Objetivo de control**	**Controles**		**Descripción**
18.2	Revisiones de la seguridad de la información	18.2.2	Cumplimiento de las políticas y normas de seguridad	Insta a promover el cumplimiento de las presentes políticas y normas de seguridad. **Responsables** Todo el personal (sin excepción) que forme parte de la estructura organizacional de la comuna.

GLOSARIO

Alcaldías de El Salvador: Unidad política administrativa primaria dentro de la organización estatal de El Salvador.

Acuerdo de Nivel de Servicio (ANS): Contrato escrito entre un proveedor de servicio y su cliente.

CSIRT: Equipos de Respuesta a Incidentes de Seguridad en Computadores o Computer Security Incident Response Team.

Control: Instrumento para la administración de riesgos, incluye procesos, políticas, directrices, estructuras organizacionales, las cuales pueden ser de índole administrativa, técnica, de gerencial o legal.

Ciclo de Demming: Es una estrategia de mejora continua basada en 4 pasos que son: planifica, hacer, verificar y actuar (del inglés Plan, Do, Check, Act).

Dirección MAC: (del inglés, media access control) identificador de dirección física única para cada dispositivo de red o tarjeta.

Dominio o Clausula: Disposición de un contrato o ley que establece ciertas condiciones.

DMZ: (del inglés, demilitarized zone) Zona segura que se debe establecer entre la red LAN y la red externa de las instituciones.

DoS: (del inglés, Denial of Service) Acto que genera que los servicios o recursos informáticos sufran de interrupciones, demoras o sean inaccesibles.

DUI: Documento Único de Identidad

Estándar: Técnica o protocolo para realizar labores especificas

EIA: (del inglés, Electronics Industries Association) La Alianza de Industrias Electrónicas es un conglomerado de compañías electrónicas y de alta tecnología orientadas a promover la competitividad de la rama tecnológica.

Host: Dispositivos informáticos (computadoras, servidores, móviles, tablet, etc.) conectados a una red que ofrecen o hace uso de servicios ofrecidos a través de la misma.

SGSI: Sistema de Gestión de la Seguridad de la Información

IDS: (del inglés: intrusion detection system) Software cuya finalidad es detectar

accesos no autorizados a un host o red informática.

IPS: (del inglés: Intrusion Prevention System) Software cuya finalidad es proteger, mediante el control de accesos, los intentos fraudulentos de autenticación a un host o red informática.

IEC: (del inglés, International Electrotechnical Commission) La Comisión Electrotécnica Internacional es un ente normalizador en la rama eléctrica y otras relacionadas.

Dirección IP: Valor que identifica a cada dispositivo dentro de una red con protocolo IP.

ISO: (del inglés, International Organization for Standarization) La Organización Internacional de Normalización es la mayor entidad desarrolladora de normas y estándares a nivel mundial cuya finalidad es facilitar el comercio mundial mediante el uso de estándares comunes.

ISP: (del inglés, Internet Service Provider) Los Proveedor de Servicios de Internet son empresas que ofrecen servicios de conexión a internet.

ISO/IEC 27001: (Information technology - Security techniques - Information security management systems - Requirements) Es un estándar que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

ISO/IEC 27002: (Code of practice for information security management). Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007 [27]

LAN: (del inglés, Local Area Network) es una red de corto alcance conformada por la conexión de dispositivos informáticos y es denominada Red de Área Local.

Ley Especial Reguladora de la emisión del Documento Único de Identidad cuyo principal objetivo según el Artículo 1 es el de *"…establecer las disposiciones regulatorias generales y especiales del sistema de registro y emisión del Documento Único de Identidad, así como las características del proceso de registro de emisión*

[27] http://es.wikipedia.org/wiki/ISO/IEC_27000-series

para su obtención

Malware: Software intrusivo u hostil desarrollado con el fin de ocasionar daños informáticos.

Normativas: Conjunto de normas aplicables a una materia especifica.

Outsorsing: Subcontratación de servicios realizada a agentes externos a la empresa.

Políticas de Seguridad Informática: Conjunto de directrices que orientan sobre el uso adecuado de las TI.

REF: Registro del Estado Familiar

RNPN: Registro Nacional de las Personas Naturales

TIA: (del inglés, Telecommunications Industries Association) Asociación de la Industria de Telecomunicaciones.

TI: Tecnologías de la información

UATM: Unidad de Administración Tributaria Municipal

BIBLIOGRAFIA

Bdat
Seguridad en redes inalámbricas, [En línea] 2013.
Fecha de consulta 28/12/2013
http://www.bdat.net/seguridad_en_redes_inalambricas/x187.html

BSI Group
ISO/IEC 27001, [En línea] 2015.
Fecha de consulta 4/2/2015
http://www.bsigroup.com/es-MX/

CCN-CERT.cni.es
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [En línea] 2013.
Fecha de consulta 28/12/2013
https://www.ccn-cert.cni.es/elearning/file.php/12/analisisv3/data/downloads/magerit_metodo.pdf

Código Municipal y sus reformas. 10a. Edición, El Salvador,
Editorial Jurídica Salvadoreña, 2003.

CNPNC
Respuesta a Incidentes en Infraestructuras Críticas, [En línea] 2013.
Fecha de consulta 28/12/2013
http://www.cnpic-es.es/Ciberseguridad/1_Respuesta_a_incidentes/index.html

CNR
Ley Especial Reguladora De La Emisión Del Documento Único De Identidad, [En línea] 2015.
Fecha de consulta 10/2/2015
http://www.cnr.gob.sv/administrator/components/com_docestandar/upload/documentos/88A00.PDF

Feedback Network
Experiencia: Calcular la muestra correcta, [En línea] 2015.
Fecha de consulta 15/01/2015
http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.html

ISO
ISO/IEC Information security management, [En línea] 2015.
Fecha de consulta 4/02/2015
http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO 27000.ES
El portal de ISO 27001 en español, [En línea] 2015.
Fecha de consulta 14/03/2015
http://iso27000.es/

incibe
CERT de Seguridad e Industria, [En línea] 2014.
Fecha de consulta 15/12/2014
https://www.incibe.es/CERT/guias_estudios/guias/

ITIL®Foundation
Formación ITIL, [En línea] 2014.
Fecha de consulta 07/07/2014
http://itilv3.osiatis.es/

ISACA
COBIT 5, [En línea] 2014.
Fecha de consulta 20/08/2014
https://www.isaca.org/

Ley de Acceso a la Información Pública, El Salvador,
Imprenta y Offset Ricaldone, 2013.

Repositorio Institucional UFG
Diseño de un sistema de registro de estado familiar para mejorar la administración de datos en las alcaldías municipales del departamento de San Salvador,
[En línea] 2014.
Fecha de consulta 19/01/2014
http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/005.74-C112d/005.74-C112d-Capitulo%20I.pdf

Repositorio Institucional UPM
Diseño de infraestructura de red y soporte informático para un centro público de educación infantil y primaria, [En línea] 2016.
Fecha de consulta 18/05/2016
http://oa.upm.es/4976/3/PFC_JUAN_MARUGAN_MERINEROx.pdf

S. Northcutt, D. McLachlan y J. Novak
Network Intrusion Detection: An Analyst's handbook
New Riders Publishing, Septiembre 2000.

Stallings, William
Comunicaciones y Redes de Computadores. 7a. Edición, Madrid,
Pearson Educación, 2004.
ISBN: 978-84-205-4110-5

.Seguridad
Revista de seguridad y defensa digital - UNAM, [En línea] 2015.
Fecha de consulta 15/05/2015
http://revista.seguridad.unam.mx/

welivesecurity
Plataforma Educativa ESET, [En línea] 2015.
Fecha de consulta 15/05/2015
http://www.welivesecurity.com/la-es/2013/06/26/nuevo-curso-gestion-respuesta-incidentes-plataforma-educativa-eset/

ANEXOS

Caso de estudio