RESUMEN

El Instituto para el Ecodesarrollo Regional Amazónico (ECORAE) se encuentra impulsando el Proyecto Regional de Conectividad cuyo objetivo es dotar de enlaces satelitales directos a los Gobiernos Municipales Cantonales de la Región Amazónica para que tengan acceso al Internet y a través de estos se amplifique la señal satelital a otras instituciones locales y de esta manera promover la inclusión digital a través de sus instituciones

Además, promueve la creación de los Telecentros Comunitarios que tienen el propósito básico de buscar los mecanismos y los procesos más adecuados a cada medio para lograr la coordinación de todas las fuerzas locales que van desde el Gobierno Municipal hasta las Juntas Parroquiales incluyendo a instituciones educativas, centros de salud, instituciones públicas y privadas, y su convergencia en el foco del desarrollo integral y armónico de la vida del municipio.

El presente trabajo describe cómo se define un Plan de Seguridad Integral para el Proyecto Regional de Conectividad definiendo en un principio su estructura organizacional como son las funciones y los roles, para luego pasar a definir las políticas y concluir con un plan de implementación de las políticas definidas.

PRESENTACION

El Instituto para el Ecodesarrollo Regional Amazónico ECORAE, es una entidad de derecho público con autonomía administrativa, económica y financiera con jurisdicción en la Región Amazónica Ecuatoriana, con domicilio principal en la Ciudad de Quito, cuyos objetivos están encaminados al ecodesarrollo de la Región Amazónica Ecuatoriana. Fue creado el 21 de septiembre de 1992 mediante Ley 010 expedida por el Congreso Nacional. Es un Organismo que planifica y facilita el desarrollo humano sustentable de la Región Amazónica Ecuatoriana.

El Directorio del ECORAE está constituido por las siguientes autoridades gubernamentales:

Ministro del ambiente - Presidente del Directorio
Delegado del Ministro de Defensa Nacional
Representante de Consejos Provinciales Amazónicos
Representante de los Municipios Amazónicos
Delegado por los Centros Agrícolas de la RAE
Delegado por Organizaciones - Indígenas de la RAE.
Delegado del Presidente Ejecutivo de Petroecuador
Delegado del Ministro de Relaciones Exteriores
Delegado del Ministro de Agricultura y Ganadería

El 25 de septiembre de 2003, la Oficina de Servicio Civil y Desarrollo Institucional “OSCIDI”, con Resolución No. OSCIDI.2003-040 emite dictamen favorable a la Estructura y Estatuto Orgánico por Procesos del Instituto para el Ecodesarrollo Regional Amazónico, ECORAE, y es publicada en la Resolución 0017 del Registro Oficial 245 del 6 de

Enero de 2004 donde se resuelve expedir la siguiente Estructura y Estatuto Orgánico por Procesos del Instituto para el Ecodesarrollo Regional Amazónico –ECORAE:

1. PROCESOS GOBERNANTES:

1.1 Direccionamiento estratégico del ecodesarrollo regional amazónico. Responsable: Directorio

1.2 Gestión estratégica del ecodesarrollo regional amazónico. Responsable: Secretario Ejecutivo

2. PROCESOS HABILITANTES:

2.1 DE ASESORÍA, conformado por el proceso:

2.1.2 Asesoramiento Legal

2.2 DE APOYO, conformado por el proceso:

2.2.1 Desarrollo institucional, integrado por los siguientes subprocesos:

2.2.1.1 Gestión de recursos organizacionales

2.2.1.2 Gestión financiera

3. PROCESOS AGREGADORES DE VALOR:

3.1 PLANIFICACIÓN DEL DESARROLLO SUSTENTABLE, conformado por los siguientes subprocesos:

3.1.1. Sistema Integrado de Información

3.1.2. Gestión de Cooperación Técnica - Económica

3.2 EVALUACIÓN Y MONITOREO

4. PROCESOS DESCONCENTRADOS

El Instituto para el Ecodesarrollo Regional Amazónico -ECORAE-

tendrá en su ámbito de competencia las provincias de la región amazónica, en las cuales tendrá la siguiente estructura de procesos:

4.1 PROCESO GOBERNANTE

4.1.1 Direccionamiento Estratégico Provincial del Desarrollo Sustentable

4.2 PROCESO HABILITANTE

4.2.1 Gestión Administrativa Financiera

4.3 PROCESO AGREGADOR DE VALOR

4.3.1 Planificación y Evaluación del Desarrollo Sustentable Provincial

Por otra parte el Gobierno Municipal es un organismo fundamental en el Proyecto Regional de Conectividad ya que, en sitios donde el ECORAE no tiene sus Secretarías Técnicas Provinciales, la infraestructura comunicacional se instala en el sitio donde lo define el Gobierno Municipal.

Por estas circunstancias, el Proyecto Regional de Conectividad como un evento regional, esta generando y va a generar en un futuro muy cercano la necesidad de tener mayor seguridad humana, física y lógica. Las instituciones que se incluyen en el proyecto con el acceso a Internet van a encontrarse debilitadas al no tener ninguna clase de protección y pueden comenzar a reforzar las medidas de seguridad pero nunca podemos saber cuándo o cómo pueden ser expuestas. Ante esta nueva necesidad institucional se requiere de un plan integrado de seguridad que sea proactivo e indique como sobrevivir a los múltiples escenarios y preparar a las instituciones en el manejo de las amenazas inesperadas que podrían enfrentar en el futuro.

La mayoría de las instituciones locales que forman parte del proyecto han invertido tiempo y dinero para la infraestructura tecnológica de la información que las soporte. Esa infraestructura ante este nuevo evento, podría resultar ser una gran debilidad si esta comprometida ya que se encuentra desprotegida tanto en su componente físico como lógico. Para esas instituciones locales que se vayan integrando en la era de la intercomunicación, las políticas de información bien documentadas que se implementen en toda la institución, son herramientas esenciales para minimizar los riesgos de seguridad.

Hay que imaginar lo que sucedería si la información de éstas instituciones, fuera alterada, se perdiera, estuviera en peligro, fuera borrada o robada.

Ante esta amenaza, implementar una política de seguridad integral le da un valor intrínsico al proyecto que impulsa el ECORAE en todos los municipios amazónicos, mejorando la credibilidad del mismo y aumentará la confianza a que otras instituciones que manejan información relevante deseen integrarse.

¿Cómo desarrollar un Plan Integral de Seguridad?

Identificando y evaluando los activos que deben protegerse y como protegerlos para que permitan la prosperidad de las instituciones.

- Identificando cuáles son los potenciales problemas de seguridad, considerando la posibilidad de violaciones a la seguridad y el impacto que tendrían si es que llegan a ocurrir. Estas amenazas son externas e internas

- Amenazas informáticas externas: se originan fuera de la institución y pueden ser gusanos, Caballos de Troya, virus, ataques de hackers o resentimientos de ex empleados.
- Amenazas internas: son aquellas que provienen del interior de la institución y que pueden ser muy costosas por que el infractor tiene mayor acceso para saber donde reside la información más relevante. Entre este tipo de amenazas también se incluye el uso indebido de acceso a Internet por parte de los empleados y trabajadores.

- Evaluando los riesgos, calculando la probabilidad que ocurran ciertos sucesos, determinando cuáles pueden cuasar daño institucional, asignando valor a la perdida de los datos si llegaran a ocurrir y los costos asociados con las soluciones para las violaciones de la seguridad.
- Las responsabilidades tecnológicas de seguridad deben identificar y diferenciar dichas amenazas. Sería ideal contar con la participación del responsable informático institucional, el procurador síndico, un concejal en el caso de los gobiernos municipales y un representante del alcalde o director institucional.
- Estableciendo políticas de seguridad que direccionen a los documentos asociados; parámetros, procedimientos y normas. Estos documentos deben tener información específica relacionada con las plataformas informáticas, las plataformas tecnológicas, las responsabilidades del usuario y la estructura organizacional. Así, si se realizan cambios futuros, es mas fácil cambiar los documentos subyacentes que la política en si misma.
- Implementar una política en toda institución en donde se debe establecer claramente las responsabilidades en cuanto a la

seguridad y reconocer quién es el propietario de los sistemas y datos específicos. También se puede requerir que todos los funcionarios institucionales firmen una declaración; si la firman, debe comunicarse claramente. Éstas son las tres partes esenciales de cumplimiento que debe incluir la política:

- **Cumplimiento.** Indicando claramente un procedimiento para garantizar el cumplimiento y las consecuencias potenciales por incumplimiento.
- **Funcionarios de seguridad**. Asignando funcionarios que sean directamente responsables de la seguridad de la información.
- **Financiación**. Asegurando que cada departamento que maneje información se le asignen los fondos necesarios para cumplir adecuadamente con la política de seguridad implementada.

- Administrar el programa de seguridad estableciendo los procedimientos internos para implementar estos requerimientos y hacer obligatorio su cumplimiento.

Consideraciones importantes

A través del proceso de elaboración de una política de seguridad, es importante asegurarse que ésta tenga las siguientes características:

- Se pueda implementar y cumplir
- Sea concisa y fácil de entender
- Compense la protección con la productividad institucional
- Se debe valorar constantemente (procesos de auditoria)

Una vez que la política sea aprobada totalmente, todos los funcionarios deben tener acceso ya que ellos son los responsables de

su éxito y deben ser actualizadas periódicamente para reflejar los cambios en la institución.

Por la amplitud del proyecto, no deben existir dos políticas de seguridad iguales ya que cada institución es diferente y sus políticas dependen exclusivamente de cada una. Sin embargo, el ECORAE pretende comenzar con este sistema general de políticas y luego personalizarlo de acuerdo a los requerimientos específicos, limitaciones de financiación e infraestructura existente.

Una política integrada de seguridad es un recurso valioso que amerita la dedicación de tiempo y esfuerzo. La política que adopten las instituciones son la base para respaldar el Plan Integral de Seguridad para el Proyecto Regional de Conectividad que impulsa el ECORAE en la Región Amazónica Ecuatoriana.

CAPITULO 1. OBJETIVOS Y ALCANCES

El objetivo del presente trabajo es realizar un diagnóstico de la situación actual en cuanto a la seguridad de las redes institucionales que forman parte del Proyecto Regional de Conectividad y diseñar un Plan de Seguridad Integral para el Proyecto Regional de Conectividad que el Instituto para el Ecodesarrollo Regional Amazónico lo viene ejecutando desde el año 2004, que permita desarrollar operaciones seguras basadas en políticas y estándares bien definidos y conocidos por los integrantes del proyecto. Adicionalmente se definirá la estrategia que se debe llevar a cabo para implementar el plan.

ALCANCE

El ECORAE ha asumido como su responsabilidad lograr que la Región Amazónica Ecuatoriana entre en la sociedad del conocimiento a través de la masificación del uso de las Tecnologías de la Información y Comunicación y con ello modernizar sus instituciones públicas y socializar el acceso a la información.
A través del Proyecto Regional de Conectividad, el ECORAE ha previsto dotar de enlaces satelitales a los 41 gobiernos municipales que tienen las seis provincias amazónicas y en sus SecretaríasTécnicas Provinciales que están ubicadas en las capitales provinciales.

Donde se instale un enlace satelital, también se ha previsto dotar de enlaces a esa señal a cuatro instituciones relevantes dentro de la vida del cantón, que pueden ser instituciones educativas, instituciones de salud, instituciones privadas, organizaciones gubernamentales y organizaciones no gubernamentales.

El alcance de este proyecto es obtener un documento administrativo para que esas instituciones lo acepten como requisito para la inclusión y sea modelo base para crear su propio plan de seguridad que será implementado con el aval de la máxima autoridad institucional.

DEFINICION DE LOS OBJETIVOS DE SEGURIDAD

“El mundo globalizado y digital practica la exclusión de diversas formas y con

extrema eficiencia. Individuos, comunidades, naciones y continentes están excluidos de este juego y la exclusión digital es apenas una de las fases de todo este proceso. Un mundo que todavía no venció la barrera del hambre o de la paz debe tener cautela a la hora de discutir sobre computadores."[1]

"Según datos del último censo nacional (INEC –2001), en Sucumbíos el 89.42% de las viviendas particulares ocupadas por personas presentes no cuenta con el servicio telefónico. En Orellana no cuentan con el servicio el 90.64%, en Napo el 82.40%, en Pastaza el 76.09%, en Morona el 80.38% y en Zamora el 83.32%. A nivel regional existen solo 17.751 viviendas particulares ocupadas por personas presentes que tienen acceso al servicio telefónico de un total de 112.744, quedando así excluidas del servicio telefónico el 84.33% de viviendas."[2]

Por esta razón, el INSTITUTO PARA EL ECODESARROLLO DE LA REGION AMAZONICA ECUATORIANA – ECORAE ha asumido como su responsabilidad lograr que la Región Amazónica Ecuatoriana entre en la sociedad del conocimiento a través de la masificación del uso de las Tecnologías de la Información y Comunicación y con ello aumentar la competitividad del sector productivo, modernizar sus instituciones públicas y socializar el acceso a la información.

Pero solo la dotación de enlaces satelitales a INTERNET no es una solución, y más bien puede convertirse en problema cuando el PROYECTO REGIONAL DE CONECTIVIDAD no cuente con políticas responsables de uso y una política de seguridad que avalice a las instituciones amazónicas la seguridad de la información que poseen. Por los altos costos de seguridad, es difícil hablar de un sistema cien por ciento seguro. Por eso, se debe optar entre estar expuestos o trabajar con intrusos.

---

1 PROYECTO LATINOAMERICANO DE MEDIOS DE COMUNICACIÓN. Manual de redes sociales y tecnología. Fundación Friedrich Ebert. Quito – 2003, pág.29

2 ECORAE. Proyecto Regional de Conectividad. Quito - 2002

Luego, la solución sería acotar todo el espectro de seguridad, en lo que se refiere a estrategias, procedimientos y plataformas. Así, se puede controlar un conjunto de vulnerabilidades, aunque no se logre la totalidad de la seguridad, lo que de por sí significa un gran avance.

Se han desarrollado documentos, directrices y recomendaciones orientándolas en el uso adecuado de las nuevas tecnologías para evitar su uso indebido y obtener el mayor provecho, ocasionando serios problemas en los bienes y servicios de las instituciones en el mundo.

En este sentido, la Implementación de un Plan de Seguridad Integral surge como una herramienta organizacional para concientizar a cada uno de los beneficiarios del Proyecto Regional de Conectividad que impulsa el ECORAE en cada uno de los cantones de la amazonía ecuatoriana, sobre la importancia y sensibilidad de la información y servicios críticos que posee o que en un futuro cercano poseerá.

Por lo expuesto, el proponer un Plan de Seguridad Integral requiere un alto compromiso con el ECORAE, agudeza técnica para establecer fallas y debilidades, y constancia para actualizar y renovar dicho plan en función de un ambiente dinámico que debe involucrar a los beneficiarios.

Está lejos de la intención del presente trabajo proponer un documento estableciendo lo que debe hacer para lograr seguridad informática total. Lo que plantea este trabajo es, proponer los lineamientos generales que se deben seguir para lograr un documento con estas características, conciente de que esta clase de documentos son ignorados por contener políticas y planes difíciles de lograr y de entender, en un corto plazo.

Por lo tanto, se desea dejar en claro que la Seguridad Informática no cuenta con una solución definitiva aquí y ahora, sino que es y será el resultado de la innovación tecnológica institucional por quienes se responsabilizaran de los sistemas.

Así, al contar con distintas características institucionales, resulta difícil implementar algo global por lo que se ha decidido armar un plan integral contando con políticas y procedimientos por un lado y con la parte física por otro.

Con esto, se puede decir que una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales lo que está permitido en el área de seguridad durante la operación general del mismo.

Metodología

La política de seguridad será un conjunto de requisitos definidos por los responsables de cada enlace satelital, que indica los términos generales que está y que no está permitido en el área de seguridad durante la vida útil y operación general de cada enlace satelital dotado.

Se ha seleccionado como metodología la definida por la RFC 1244 que define a una política de seguridad como "... un documento de alto nivel en el que se dan estrategias generales. Los procedimientos de seguridad necesitan partir, en detalle, los pasos precisos para tomar las protecciones respectivas."[3]

La política debe reflejarse en una serie de normas a seguir, donde se definen medidas a tomar para proteger la seguridad del sistema; pero ante todo, una política de seguridad debe ser una forma de comunicarse con los usuarios, teniendo en cuenta que la seguridad comienza y termina con las personas y ésta debe:

- Ser holística, es decir que debe cubrir todos los aspectos relacionados con la misma. No tiene sentido proteger el acceso con una puerta blindada si no esta cerrada con llave.
- Adecuarse a los recursos y a las necesidades. No tiene sentido adquirir

3 HOLBROOK, P.; REYNOLDS, J. RFC 1244- Site Security Handbook. ISRI Editors. Julio 1991. Pág.19

una caja fuerte para proteger un lápiz.

- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir criterios generales y estrategias a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Así, la política de seguridad debe contemplar los elementos claves de seguridad como son: Integridad, Disponibilidad, Privacidad y, además: Control, Autenticidad y Utilidad.

Por lo tanto, la política de seguridad no debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Más bien es una descripción de lo que se desea proteger y el porque de ello.

1.1 Definición de los objetivos de diagnóstico

Para obtener un diagnóstico adecuado de la situación actual, se deben tener en cuenta los siguientes aspectos:

1.1.1 Evaluación de Riesgos

De acuerdo al concepto, su análisis supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas, y se debe:

- Obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir)
- Tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. Así, se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado.
- Tener bien claro que se quiere proteger, cómo y dónde asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información,

personal, accesorios, etc.) con que se cuenta y las amenazas a las que se esta expuesto.

La evaluación de riesgos y su presentación de respuestas se debe preparar en una forma personalizada para cada institución, presuponiendo algunas preguntas que ayudan en la identificación de lo expuesto. Preguntas tales como:

- ¿ Qué puede ir mal?
- ¿ Con qué frecuencia puede ocurrir ?
- ¿ Cuáles serían sus consecuencias?
- ¿Qué fiabilidad tienen las respuestas a las anteriores preguntas?
- ¿Se está preparado para continuar con los tramites institucionales sin sistemas, por un día, una semana, cuánto tiempo?
- ¿Cuánto cuesta una hora sin procesar, un día, una semana?
- ¿Cuánto tiempo se puede estar fuera de línea sin que los beneficiarios del sistema se molesten?
- ¿Se tiene forma de detectar a un funcionario deshonesto en el sistema?
- ¿ Se tiene control sobre las operaciones de los distintas sistemas?
- ¿Cuántas personas dentro de la institución (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?
- ¿Se tiene identificada la información confidencial y/o sensitiva?
- ¿La información confidencial y sensitiva permanece así en los sistemas?
- ¿La seguridad actual cubre los tipos de ataques existentes y esta preparada para adecuarse a los avances tecnológicos esperados?
- ¿ A quién se le permite usar que recurso ?
- ¿Quién es el propietario del recurso?, y ¿ quién es el usuario con mayores privilegios sobre ese recurso?
- ¿Cuáles serán los privilegios y responsabilidades del administrador vs. la del usuario?
- ¿Cómo se actuaría si la seguridad es violada?

Una vez obtenida la lista de cada uno de los riesgos se efectuara un resumen del

tipo:

Tipo de riesgo	**Factor**
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Tabla No. 1 . Asignación de factores

Y según esto, se deberán tomar las medidas pertinentes de seguridad para cada caso en particular, cuidando incurrir en los costos necesarios según el factor de riesgo representado.

Niveles de riesgo

Como puede apreciarse en la tabla anterior los riesgos se clasifican por su nivel de importancia y por la severidad de su perdida:

1. Estimación del riesgo de perdida del recurso (Ri)
2. Estimación de la importancia del recurso (Ii)

Para la cuantificación del riesgo de perder un recurso, se puede asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

El riesgo de un recurso será el producto de su importancia por el riesgo de perderlo: $WRi = Ri * Ii$

Luego con la siguiente fórmula, basada en Microsoft Security, es posible calcular el riesgo general de los recursos de la red:

$$W_R = \frac{WR_1 * I_1 + WR_2 * I_2 + ... + WRn * In}{I_1 + I_2 + ... + In}$$

Otros factores que se debe considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial, los cuales pueden incorporarse a la fórmula para ser evaluados.

1.1.2 Identificación de amenaza

Cuando ya se han conocido los riesgos, los recursos que se deben proteger y como el daño puede influir en la institución, se identifica cada una de las amenazas y vulnerabilidades que pueden causar. Se debe considerar que si existe una amenaza es por que existe una vulnerabilidad, existiendo una relación directa.

Por lo general, las amenazas pueden dividirse según su ámbito de acción:

- Seguridad Física: Desastre del entorno
- Seguridad Lógica: Amenazas del sistema
- Comunicaciones: Amenazas en la red
- Recurso Humano: Amenazas de personas.

Es responsabilidad de los administradores de la red institucional, disponer de una lista actualizada de amenazas para identificar los distintos métodos, herramientas y técnicas de ataque que pueda utilizar, y que estos evolucionen en forma continua.

1.1.3 Evaluación de costos

Consiste en cuantificar los daños que cada posible vulnerabilidad puede causar. Un planteamiento posible para desarrollar esto, es el análisis de lo siguiente:

- ¿Qué recursos se quiere proteger?

- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué se puede hacer para proteger los bienes institucionales de una manera oportuna y económica?

Esto sirve para conocer cuales recursos vale la pena proteger. Lo que se pretende es lograr que un ataque a los bienes sea mas costoso que su valor, invirtiendo menos de lo que vale. Para esto se definen tres costos fundamentales:

- **CP:** Valor de los bienes y recursos protegidos
- **CR:** Costo de los medios necesarios para romper las medidas de seguridad establecidas.
- **CS:** Costo de las medidas de seguridad.

Para que la política de seguridad tenga lógica y sea consistente se debe cumplir:

- CR > CP: el costo de un ataque debe ser mayor al costo de los bienes. Los beneficios obtenidos de romper las medidas de seguridad no deben compensar el costo del desarrollo del ataque.
- CP > CS: el costo de los bienes protegidos debe ser mayor que el costo de la protección.

Luego CR > CP > CS y lo que se busca es:

- Minimizar el costo de la protección manteniéndolo por debajo de los bienes protegidos
- Maximizar el costo de los ataques manteniéndolo por encima de los bienes protegidos.

1.2 Definición de los alcances del plan de implementación

Para establecer un plan adecuado es conveniente pensar en una política de protección en los distintos niveles que debe abarcar y que no son ni mas ni menos que el nivel físico, lógico, humano y la interacción que existe entre estos niveles.

En cada caso considerado, el plan de implementación debe incluir una estrategia proactiva y una reactivo.

La estrategia proactiva (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y desarrollar planes de contingencia. La determinación del daño que va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

La estrategia reactiva (perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y a aprender de la experiencia y a conseguir que el sistema se normalice lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- Lo que no se permite expresamente esta prohibido: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa esta prohibida.
- Lo que no se prohíbe expresamente esta permitido: significa que, a menos que se indique expresamente que cierto servicio no esta disponible, todos los demás si lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir que acciones se toleran y cuales no son guías de administradores de servicios

Actualmente, gracias a las acciones que atentan contra los sistemas informáticos, los expertos se inclinan por recomendar la primera política mencionada.

1.2.1 Implementación

La implementación de medidas de seguridad es un proceso técnico - administrativo. Como este proceso debe abarcar toda la institución, sin exclusión alguna, ha de estar fuertemente apoyado por la máxima autoridad, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Se deberá tener en cuenta que la Implementación de Políticas de Seguridad, trae aparejado varios tipos de problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad con lleva a incrementar la complejidad en la operatoria de la institución, tanto técnica como administrativamente.

Por esto, será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.
Por lo tanto, el Plan de Seguridad Integral para el Proyecto Regional de Conectividad deberá abarcar:

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad de cada uno de los servicios, recursos y responsables en todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.

- Definición de violaciones y las consecuencias del no cumplimiento de la política.
- Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud que pasara o cuando algo sucederá; ya que no es una sentencia obligatoria de la ley.
- Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porque de las decisiones tomadas.
- Finalmente, como documento dinámico de la organización, debe seguir un proceso de actualización periódica sujeto a los avances tecnológicos y a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación del personal, desarrollo de nuevos servicios y se debe realizar controles de cumplimiento de las políticas.

Se comienza realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.
Luego de evaluar estos elementos y establecida la base del análisis, se origina un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

Para que todo llegue a un buen fin debe realizarse un control periódico de estas políticas, que asegure el fiel cumplimiento de todos los procedimientos enumerados. Para asegurar un marco efectivo se realiza una auditoria a los archivos reporte de estos controles.

Con el objeto de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del sistema. Esta simulación y los costos reales registrados generan una realimentación y revisión que permiten adecuar las políticas generadas en

primera instancia.

Por último, el plan de contingencia es el encargado de suministrar el respaldo necesario en caso en que la política falle.

Es importante destacar que la seguridad debe ser considerada desde la fase de diseño de un sistema. Si la seguridad es contemplada luego de la implementación del mismo, el personal se enfrentara con problemas técnicos, humanos y administrativos mucho mayores que implicaran mayores costos para lograr, en la mayoría de los casos, un menor grado de seguridad.

Construya la seguridad desde el principio. Recuerde que es más caro añadir después de la implementación. "... Para mantener un completo control, debemos realizar una aproximación más activa a la seguridad, una aproximación que comienza con la evaluación destinada a identificar posibles riesgos."[4]

4 McNAB Chris. Seguridad de Redes.Ediciones Anaya Multimedia .2004. Pág.37

CAPÍTULO 2. ANÁLISIS, DIAGNÓSTICO Y SITUACIÓN ACTUAL DE LA ADMINISTRACIÓN DE LA SEGURIDAD.

Para lograr un adecuado entendimiento de lo que implican las amenazas y vulnerabilidades en el Proyecto Regional de Conectividad que el Instituto para el Ecodesarrollo de Región Amazónica Ecuatoriana se encuentra impulsando en la región, se ofrece un acercamiento a una metodología sistemática en la importante tarea de administrar la seguridad.

Ésta se basa en un diagnóstico de la situación actual en los sitios donde se encuentran implementada la infraestructura comunicacional, para lo cual se han generado preguntas realizadas en base a muchas características propias de los entrevistados, que se ha basado en entrevistas, recolección de documentos organizacionales y reconocimiento del medio ambiente de trabajo.

2.1 ANÁLISIS Y DIAGNÓSTICO DE LA SEGURIDAD LÓGICA Y FÍSICA

Cabe aclarar que, al ser un proyecto de inclusión digital a las Tecnologías de Información y Comunicación, en el Proyecto Regional de Conectividad participan dos actores principalmente:

- Las Secretarías Técnicas Provinciales del ECORAE ubicadas en cada capital provincial amazónica; y
- Gobiernos Municipales Cantonales ubicados en cada una de las provincias amazónicas.

2.1.1 SEGURIDAD LÓGICA

En este punto se han evaluado los controles de accesos de los usuarios y a datos que se gestionan, para señalar las irregularidades que obstaculicen la disponibilidad, exactitud y confidencialidad de la información, y así obtener las mejoras que fueran factibles de efectuarse, con el afán de estandarizar un procedimiento para implantarlo en todos los usuarios incluidos en el proyecto.

Identificación de usuarios

- **Dar de alta a nuevos usuarios.** Al tener diversos actores y por no tener una unificación de gestión informático comunicacional, no existe un procedimiento unificado a seguir para realizar estas tareas ya que en el Proyecto Regional de Conectividad, como es de esperarse, cada institución tiene su propio procedimiento para dar de alta a nuevos usuarios o simplemente no existe ninguno. Lo que se ha logrado detectar para ingresar una nueva cuenta son:
    - Identificación del usuario. Inicialmente será la primera letra de su nombre seguida por el primer apellido completo.
    - Clave de acceso, inicialmente será el mismo de su identificación, inmediatamente se lo instruye para que pueda modificarlo.
    - Nombres y apellidos completos que se los obtiene del mismo usuario que solicita la creación de la cuenta.
    - Departamento (o su equivalente) donde trabaja.
    - Fecha de ingreso a la institución. Aunque para algunos usuarios este campo no se completa.

- Dar de baja a usuarios. No hay ningún procedimiento formal para dar de baja a un usuario del sistema. El administrador conoce que un funcionario se ha desvinculado de la institución y allí procede a dar de baja a ese usuario, y esa cuenta se elimina del sistema. De esta forma los datos de las cuentas dadas de baja no quedan almacenados en el disco y es muy probable repetir las identificaciones de usuarios anteriores para los nuevos.

Mantenimiento

Se ha podido verificar que no se lleva a cabo ningún control ni revisión periódica sobre el buen funcionamiento de las cuentas de los usuarios, peor aún sobre los permisos que se tienen asignados.

Permisos

El control de acceso se basa solo en los perfiles de los usuarios y la asignación o denegación de permisos responsabilidad del administrador del sistema quién es el encargado de la asignación de permisos. Además, no existe una lista de control

de acceso que se utilice para identificar los tipos de permiso que tiene cada usuario. Al no existir, resulta complicado identificar que datos puede modificar cada usuario. Por último, se ha detectado que no se tiene en cuenta ninguna restricción horaria para el uso de los recursos ni tampoco se considera una restricción física sobre la máquina desde donde ingresa cada usuario.

Inactividad

Cuando un usuario permanece un período de tiempo ingresado sin actividad, el sistema no ejecuta ninguna acción; los administradores solo advierten verbalmente a los usuarios sobre la necesidad de no dejar las máquinas ingresadas e inactivas. Si las cuentas de usuarios permanecen varios días sin actividad, por licencias o por vacaciones no pasan a un estado de suspensión.

Cuentas de usuario

No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar simultáneamente. No se eliminan los usuarios que vienen por defecto en el sistema operativo, como son las cuentas “Invitado”, éstas cuentas permanecen activas en el sistema sin que ningún usuario las utilice.

Se ha detectado que solo una persona tiene un perfil de administrador, con su cuenta y clave de acceso personal. Además, el administrador puede ingresar desde cualquier computador de la institución lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando esa terminal ingresada con su usuario administrador.

Autenticación

En la pantalla de ingreso de los sistemas se muestran los siguientes datos:

- Nombre de usuario (a completar por el usuario),
- Contraseña (a completar por el usuario),
- Conectarse a (opción para escoger el dominio o este equipo)

Una vez que algún usuario ha logrado ingresar, aparece en pantalla el mensaje cargando su configuración e ingresa. Se ha detectado que no se usa ningún tipo

de firma digital, ni para mensajes internos ni para los externos en los datos enviados vía mail. Y en cuanto a la configuración de las estaciones de trabajo, no hay ningún control de acceso a su sistema BIOS, de manera que al momento del encendido de la máquina cualquier persona podría modificar sus opciones de configuración.

Claves de acceso

- Generación

Las claves de acceso que tienen los usuarios son generados en forma manual, sin procedimientos automáticos de generación.

Cuando se da de alta un empleado en el sistema, su clave de acceso se inicializa con el mismo nombre de la cuenta (que es igual a la primera letra del nombre seguida del apellido completo), advirtiéndole al usuario que lo cambie, pero sin realizar ningún control sobre la modificación del mismo.

- Cambios

Los cambios en las claves de acceso lo hace el administrador bajo un pedido verbal del usuario. No se controla si el usuario utiliza siempre la misma clave de acceso. Si un usuario olvida su clave de acceso, debe advertirle al administrador del sistema, el cual se fijará en su listado cuál es la clave del usuario. Al decírsela, no se requiere que el usuario la modifique, no se controla esta situación.

Segregación de funciones

No se implementa ningún régimen de separación de tareas, para evitar que un solo empleado realice la totalidad de una operación.

2.1.2 SEGURIDAD FÍSICA

Se evaluaron los centros de cómputo (donde existen), los equipos, los dispositivos, los medios de almacenamiento y las personas que conforman el sistema informático, en espera de que cumplan con las medidas necesarias en lo relativo a la infraestructura física y mantenimiento de la seguridad de los recursos.

Equipamiento

Características de las PC´s

Se realizó una verificación del equipamiento informático en la oficina matriz del ECORAE en la ciudad de Quito que consta en el ANEXO1 y en cada una de las Secretarías Técnicas Provinciales que consta en el ANEXO 2.

Control de acceso físico a los centros de cómputo

En las Secretarías Técnicas Provinciales y en la mayoría de municipios no existe un centro de cómputo específico para su función. Las instituciones encuestadas cuentan con guardias de seguridad; en horarios laborales se ubican en el interior y exterior de la misma, y cuando se cierra la institución solo quedan en el exterior. El personal que tiene el acceso permitido a la oficina donde está el equipo que cumple las funciones de proxy es el técnico informático de la institución, pero cualquier persona ajena a la institución que necesite realizar alguna tarea, deberá anunciarse en la puerta de entrada y el técnico informático permitirá sus acceso, escoltándolo todo el tiempo.

Control de acceso a equipos

Todas las máquinas de la institución disponen de disqueteras y lectoras de CD, aunque la mayoría de ellos no las necesita. Estos dispositivos están habilitados y no hay ningún control sobre ellos. Los gabinetes donde se ubican los switches de cada una de las secretarías, no están cerrados con llave y están expuestos. No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC´s, de manera que alguien podría sacar o poner alguno.

Una vez que se ha completado la instalación de algún equipo, el técnico informático no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

El equipo que cumple las funciones de proxy se apaga cuando finaliza la sesión de trabajo.

Dispositivos de soporte

En las secretarías técnicas disponen de los siguientes dispositivos para soporte del equipamiento informático:

- Aire acondicionado y la temperatura se mantiene entre 18ºC y 24ºC. Cuentan con un sistema de ventilación para esta área, con el fin de mantener esta temperatura.
- No existen alarmas contra intrusos.
- Existe un UPS: (Uninterruptible Power Supply) en cada equipo
- Cada equipo cuenta con un estabilizador de tensión
- La corriente eléctrica proviene de un tablero independiente al que llega la línea de energía.
- Se ha realizado una instalación a tierra con una barra de cobre que funciona como descarga a tierra.
- No existe luz de emergencia.
- No existe piso aislante.

Cableado estructurado

La instalación del cableado la realizó el técnico informático de la institución. El tendido del cableado es de fácil accesibilidad ya que se sacan los paneles que lo componen. Desde allí los cables pasan por las columnas del edificio, desde las cuales bajan hasta los equipos de los usuarios. Estos cables están conectados al switch. En todo el trayecto del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además no hay distancias grandes recorridas con cables UTP. En el switch hay un conector dedicado para cada máquina, y conectores de sobra por una posible ampliación de la red. Además hay un concentrador que llega al switch, el cual conecta ocho máquinas respectivamente. Esto se configuró porque la institución disponía del concentrador, aunque se disminuye la velocidad de la red. Para que no haya interferencias se utilizó cableado UTP categoría 5. Los cables están numerados de manera que se los puede identificar fácilmente.

Ancho de banda de la red

La institución tiene un ancho de banda de 128/64 asimétrico obtenidos de un enlace satelital directo no compartido

Falla en la red

Por norma, cuando hay un corte de luz se graban los datos y se deja de trabajar en línea. Si el corte supera los quince minutos de duración, entonces apagan todos los equipos como una medida de prevención.

2.2 ANÁLISIS Y DIAGNÓSTICO DE LA SEGURIDAD EN LAS COMUNICACIONES

Lo que se ha pretendido con este diagnóstico es optimizar el componente de comunicaciones del sistema de información (cableado, dispositivos de interconexión –concentradores, switches, netmodems, antenas, etc.), para que los canales funcionen de manera estable y continua (disponibilidad), pudiéndose establecer la identidad de los participantes (autenticación), que los datos transmitidos puedan ser accesados únicamente por personas autorizadas (confidencialidad), que esos datos no puedan ser modificados durante su transmisión (integridad) y que se pueda establecer el origen de toda comunicación (no repudio).

2.2.1 SEGURIDAD DE LAS COMUNICACIONES

Se ha evaluado la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

Situación actual

Actualmente, las Secretarías Técnicas Provinciales del Ecorae cuentan con un enlace satelital a través de una antena VSAT que tiene las siguientes características:

Equipamiento:

Netmodem iDirect 120

1 BUC de 2 Watts

1 adaptador de corriente

1 UPS

1 Segmento de cable UTP cat.5 con 2 conectores RJ 45

Gráfico No.1 Netmodem Satelital

Antena:

8 Metter C-Band Cross-Pol Antenna

Channel Master Model 183

1.8M Reflector Mfg P/N 611611831

TX/RX C-Band Mount Mfg P/N 611610203

C-Band TX Feed Assembly (X-POL) WR1 Mfg P/N 611618421

Gráfico No.2 Antena y Equipamiento Satelital

Direcciones IP:

Direcciones asignadas	5
Direcciones Usables	4

Diagrama

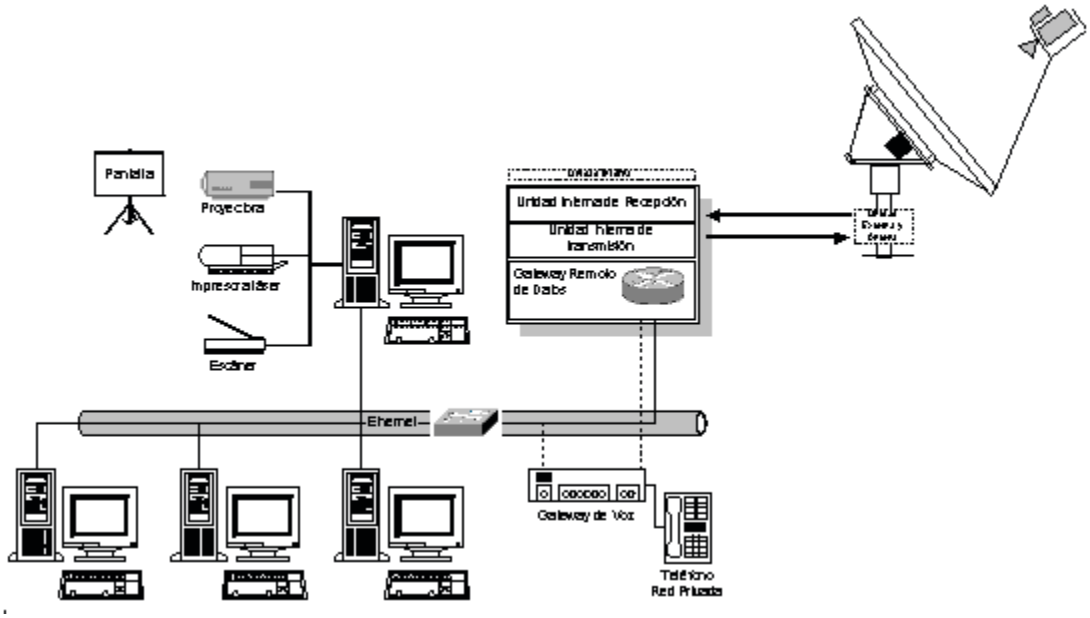


Gráfico No.3 Diagrama de enlace satelital

TOPOLOGÍA DE RED EN SECRETARIAS TÉCNICAS PROVINCIALES

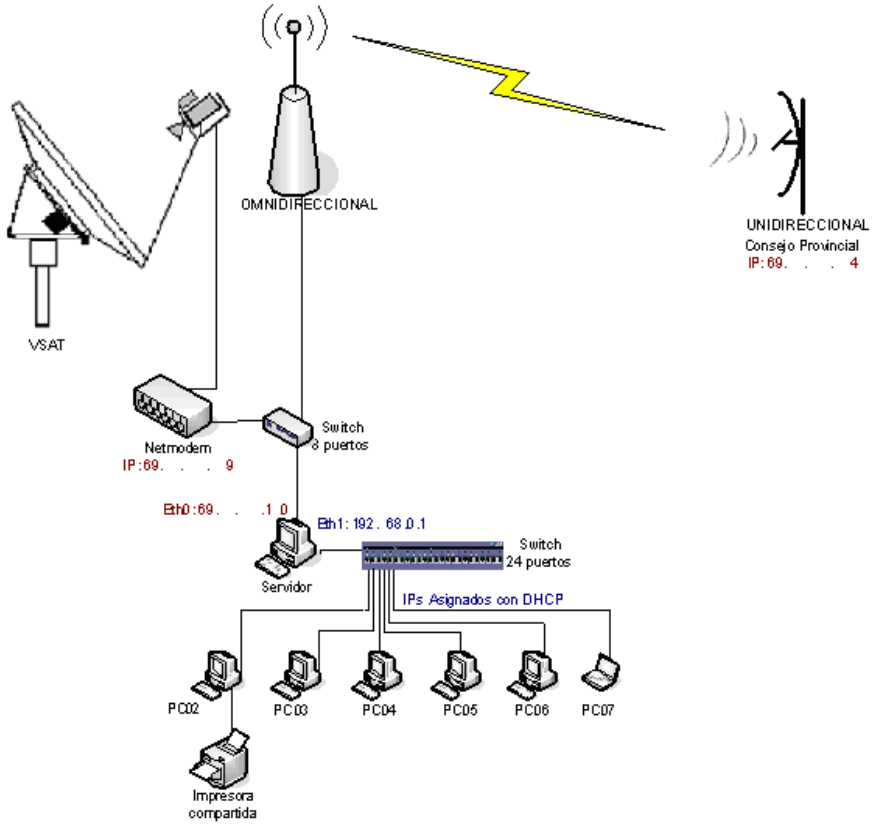


Gráfico No.4 Topología de red del ECORAE

Servidor de Internet

Para la conexión a Internet en las Secretarías Técnicas Provinciales del ECORAE se utiliza un servidor IBM con Linux Red Hat v9.0 que cumple las funciones de proxy con squid e interconecta a las máquinas Windows con Samba. Además el equipo de cara al Internet. Su salida al exterior es a través de una conexión satelital de 128/64 Kbps, suministrada por el ISP institucional. Como conexión de respaldo a Internet se puede utilizar una conexión vía módem.

Recursos compartidos

El entorno de red de cada uno de los usuarios está configurado para que el usuario pueda compartir carpetas y archivos con los demás funcionarios de la secretaría. No hay ninguna medida tomada para que un usuario no comparta sus datos con otro usuario, todo queda a la necesidad de ese momento.

Herramientas

La institución cuenta con dos portales: el Portal Técnico que está alojado en el servidor de Internet de la institución bajo el URL: www.ecorae.org.ec, y el Portal Comunicacional que se aloja en un servidor ajeno, y tiene el URL: www.ecorae.org

Correo Electrónico

Todos los funcionarios del ECORAE tienen una cuenta de correo institucional. Este medio se utiliza para enviar todo tipo de información. El correo se lee con la pestaña Correo Electrónico del Portal Técnico. Usa el SendMail de LINUX y un administrador de correo denominado SquirreMail que está configurado para brindar el servicio a través del Portal Técnico

Usuarios de Correo Electrónico

A todo funcionario del ECORAE se le asigna una casilla de correo. Para generar una nueva cuenta de mail, el funcionario solicita verbalmente a la administradora del correo en la ciudad de Quito que le cree una cuenta. Esta crea una cuenta con la primera letra del nombre y el apellido del funcionario. De igual manera se crea el clave de acceso y se le comunica al funcionario. Si éste decide cambiar el clave de acceso, le avisa a dicha funcionaria para que realice el cambio. Esto impide que un funcionario utilice la cuenta de otro, ya que la única persona que conoce las contraseñas es la administradora del correo electrónico.

Recepción y envío de Correo Electrónico

Los usuarios chequean su correo cada cierto tiempo. El mail queda en el servidor por lo que se debe crear procedimientos continuos con los usuarios para limpiar sus bandejas.

Los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. Es posible ver los mail que se envían, pero actualmente no se realizan controles, de manera que pueden usarlo para cualquier fin. No se hace ningún control para comprobar si los usuarios se suscriben a listas de correo, no hay prohibiciones en este sentido.

Cuotas de disco

No existen cuotas de disco razón por la que se ha generado mucha saturación en el disco duro del servidor, teniendo que realizar constantes limpiezas manuales por parte de los usuarios tras un procedimiento creado para la situación.

Opciones seguras de configuración

- Antivirus. El antivirus que está en el servidor de Internet chequea el mail, inspeccionando todos los mensajes entrantes y salientes, y sus archivos adjuntos. En el caso de encontrar un mail infectado, se encarga de borrarlo.
- Chat y File Sharing. No están prohibidos los programas de chateo (generalmente se usa el MSN). Tampoco están prohibidos los programas de file sharing. Esto se da porque los servicios que utilizan estos programas no están deshabilitados.
- Prioridades. No se implementa un sistema de prioridades de los mensajes.
- Copia de seguridad. No se generan copias de seguridad de los mensajes.
- Privacidad – Firma digital – Encriptación de mails. No se utilizan firmas digitales ni encriptación en el correo electrónico.

Algunos usuarios utilizan firmas de Outlook para enviar sus mensajes. No hay prohibiciones de envíos de archivos confidenciales vía mail.

Antivirus

En la institución no ha habido grandes problemas con virus, a excepción de una gran cantidad de PC´s con Windows infectadas con algunos virus, pero que no han afectado a los servidores. Para el efecto, el ECORAE dispone de una versión corporativa del Panda Antivirus, de manera que en el servidor de aplicaciones hay una versión para el servidor y en el resto de las PC´s hay una versión cliente de este antivirus. En el servidor de Internet también está instalada la versión de Panda para el control de virus. Ambos antivirus están ejecutándose continuamente y controlan la recepción y el envío de mail, tanto en el servidor como en las PC´s.

Actualización

De Internet se actualizan las listas de virus del Panda Antivirus a través de la actualización del archivo pav.sig, que se almacena en una carpeta del servidor.

Verificación de virus

No se hacen verificaciones periódicos buscando virus en los servidores ni en las PC´s. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable. En algunas máquinas (en las que han tenido problemas frecuentes con virus), cuando el equipo se inicia, entonces comienza una verificación del Panda antes del inicio de Windows.

Configuración de servicios del Firewall

El firewall existente está configurado de manera que se prohíben todos los servicios y solo se habilitan los necesarios (postura de negación preestablecida por el ISP).

Se configuró en base a una política del ISP que discrimina tres clases de paquetes de red:

- los paquetes entrantes a la red,
- los paquetes salientes de la red,
- los paquetes en tránsito.

Algunos servicios no son necesarios y sin embargo se encuentran habilitados para situaciones específicas, como el FTP, ya que existe un usuario que debe utilizar este servicio para comunicarse con el proveedor de servicio para la actualización de una página web de un proyecto productivo de la institución al menos una vez por mes.

En el servidor de Internet se encuentran habilitados permanentemente los puertos necesarios para el funcionamiento de la red y algunos servicios están deshabilitados y se activan solo cuando son necesarios, estos son llamados servicios bajo demanda.

Verificación de la red

El encargado de mantenimiento controla que los servicios permitidos sean los correctos, pero esta tarea la realiza sin ninguna frecuencia. Debido a que estas pruebas que se realizan no son formales, no se genera documentación alguna.

Nunca se hicieron pruebas de auto-intrusión, ni verificaciones, ni intentos de intrusión o de escucha. Tampoco se hace una verificación periódica de puertos o de los servicios que están habilitados. Solo se revisan las instalaciones cuando hay quejas de los usuarios.

El firewall monitorea los intentos de ingresos, generando reportes y correos por cada evento, pero no genera alertas ni precauciones ante algún supuesto problema.

Falla en servidores

En el caso que haya algún problema con el servidor de Internet, no se usaría el servidor de aplicaciones como reemplazo. Para la institución es preferible prescindir de los servicios de Internet hasta que el servidor sea reparado. En el caso que falle el firewall sería una falla segura, ya que los controles funcionan a bajo nivel (a nivel del kernel) y esta falla implicaría que el sistema operativo del servidor está inestable, de manera que nadie tendría acceso desde ni hacia la red externa (Internet).

Ataques de red

En la institución no disponen de herramientas destinadas exclusivamente para prevenir los ataques de red, en principio debido a que no se han presentado, hasta el momento, problemas en este sentido. Tampoco hay zonas desmilitarizadas, pero se dispone de un servidor de cara al Internet y que es administrado remotamente por el proveedor del servicio de Internet.

Sistema de detección de intrusos (IDS - Intrusion Detection System)

En la institución no se han registrado intrusiones. No hay herramientas para detección de intrusos, solo se cuentan con la configuración del firewall.

Negación de Servicio (DOS - Denial Of Service)

No hay controles con respecto a la ocurrencia de Negación de Servicio. No existen herramientas que lo detecten, ni hay líneas de base con datos sobre la actividad normal del sistema para así poder generar avisos y limitar el tráfico de red de acuerdo a los valores medidos. Se dispone de una herramienta de monitoreo provista por el ISP, que se ejecuta en una página HTML con datos sobre el tráfico de red,

Ataque a los Claves de acceso

El archivo de los claves de acceso del sistema se almacena en el directorio por defecto del Linux, en el /etc/passwd. Se usa encriptación *one way* (en un solo sentido), de manera que no es posible desencriptar. En el momento del ingreso, se encripta la contraseña ingresada por el usuario y se compara ésta contraseña encriptada con el dato almacenado que también está cifrado, si ambos son diferentes el ingreso será fallido. Para modificar las claves de acceso, Linux accede a los datos simulando ser super usuario, por lo que es posible la transacción.

2.3 ANÁLISIS Y DIAGNÓSTICO DE LA SEGURIDAD DE LAS APLICACIONES

En los últimos años se ha logrado materializar un importante avance en materia informática - comunicacional del ECORAE, que se detalla a continuación:

Primero fue el desarrollo de información cartográfica generada en la Zonificación Ecológica Económica (ZEE) misma que fue concebida para la conformación de una gran Geo Data Base pero que en la actualidad se encuentra desactualizada y no tiene una validación geográfica en sitio.

En segundo lugar se implementó un sistema de Control de Trámites Internos y Externos institucional que permite integrarlos en una misma aplicación y hacer un seguimiento adecuado y oportuno. Este Sistema es un aplicativo informático multiusuario, desarrollado específicamente para el Control Global de los Tramites

de la Institución. Permite integrar todos los procesos de creación, elaboración de Tramites internos, trámites externos extra e inter departamentales realizados anualmente. Tiene las siguientes opciones:

- PERÍODO ANUAL
- ACTUALIZACION DE TRÁMITES
- TRÁMITES INTERNOS
- TRÁMITES EXTERNOS
- REPORTE DE TRÁMITES
- UTILITARIOS
- AYUDA EN LINEA

El sistema es integrado totalmente, permitiendo que tanto el personal operativo y técnico como las autoridades ejecutivas de la misma integren todos los procesos de control de trámites bajo una misma aplicación, la cual permita realizar tanto las tareas operativas diarias, como elaborar las hojas de control, informes globales de trámites y otros. Así como obtener reportes consolidados e individuales de los trámites , por departamento, sección, subsección persona, Provincia, Cantón, Parroquia y Lugar de cada uno de los meses del año y del total acumulado a una determinada fecha de corte.

En tercer lugar se inaugura la página web institucional denominada Portal Comunicacional en agosto de 2002. Es una Extranet de colaboración y de comunicación que utiliza la tecnología Internet, y que interconecta al ECORAE al mundo permitiendo que accedan a determinadas funcionalidades de información de la región amazónica ecuatoriana como de la generada al seno de la institución. Para materializar este proyecto y hacer viable su explotación, se dispone de una completa plataforma y solución computacional con alojamiento externo para agilitar la comunicación. Su diseño es dinámico, fácil, amigable e interactivo. Se utilizan enlaces que facilitan la navegación y perfiles de usuario que facultan o restringen el acceso a la información. Esta página se encuentra en el URL www.ecorae.org.

En cuarto lugar se inaugura la Red Virtual Institucional o Portal Técnico en

diciembre del mismo año, que además cuenta con el servicio de correo electrónico institucional. Conscientes de que las comunicaciones y la información institucional representan uno de los desafíos más importantes para mejorar la intercomunicación institucional y de esta manera obtener una eficiente y eficaz administración de los recursos disponibles. En este contexto, el Portal Técnico o Red Virtual se ha transformado en una herramienta muy poderosa que contribuye en forma decidida a mejorar cada vez más la gestión de la institución. Para ingresar al portal técnico, se digita en el URL del navegador la dirección www.ecorae.org.ec . a través de las cual se encuentran tres opciones:

- **TRABAJO COOPERATIVO**: Es el portal técnico institucional. Para su ingreso, cada usuario debe estar autorizado previamente por el administrador del portal y es restringido el uso de todos los funcionarios de la institución. Cada uno tendrá un Nombre de Usuario y Contraseña el que le permitirá acceder al portal y tener su propia configuración personal. Una vez ingresado estos datos tendrá acceso a la pantalla principal del Portal, donde se encuentran los siguientes módulos:

  Calendario
  Contactos
  Foro
  Archivos
  Proyectos
  Asistencia
  Notas
  Opciones

- **PORTAL DE CONTENIDO:** Permite el ingreso a un Portal dinámico en el que se puede obtener información del ECORAE y acceso a distintos módulos que permiten una comunicación con usuarios externos que les interese la información institucional.
- **CORREO ELECTRÓNICO:** Permite el ingreso al servidor de correo institucional.

En quinto y último lugar se desarrolló e implementó el Sistema Financiero Contable GESTA, que es una potente herramienta para el manejo contable y financiero de acuerdo a las necesidades de la Institución. Este sistema es una aplicación multiusuario desarrollado en Visual FoxPro que ofrece un panorama completo y acceso inmediato a las opciones y procesos disponibles, que cuenta con:

- CONTABILIDAD
- TESORERIA
- PRESUPUESTO
- PROYECTOS
- INVENTARIOS
- COMPRAS
- ROL DE PAGOS
- ACTIVOS FIJOS
- VIATICOS

El módulo de CONTABILIDAD a su vez despliega el siguiente menú de opciones:

- Un contenedor de Editores, donde se encuentran botones de acceso a formularios que le permitirán añadir, eliminar o cambiar registros. Por ejemplo: Catálogo de Cuentas, Asientos Contables, Beneficiarios, Saldos Iniciales, Puntos Contables, Movimientos de la Cuenta, Tipos de Transacciones y Constantes.
- Un contenedor de Informes y Listados donde se encuentra información que podrá imprimirse, Vista preliminar o enviarse a un archivo de texto que luego podrá recuperarse y editarse en una hoja electrónica. Están disponibles los siguientes Informes y Listados: Catálogo de Cuentas, Balance General, Estado Sit. Finan. Comparat., Estado de Resultados, Estado Resultados Comparat., Balance de Comprobación, Libro Mayor, Libro Diario, SRI Compras, SRI: Talón y Archivos y Flujo de Efectivo.
- Un el contenedor de Utilitarios, donde están disponibles procedimientos generales de mantenimiento y administración del Sistema. Estos son: Depuración de Tablas, Remayorizar Movimientos, Asientos descuadrados,

- Respaldo de Datos, Contraseñas del Sistema, Inicialización Anual, Inicialización de Saldos, Tablas y Cierre de Períodos Mensuales.

En lo que ha software licenciado se refiere, el ECORAE cuenta con: 74 licencias Open St. de Windows Pro 2000 Spanish, 59 licencias Open St. de Windows CAL 2000 English, 03 licencias Open St. de Windows XP Professional XP Spanish, 02 licencias Open St. de VStudio.NET EntDev 2002 English, 03 licencias Open St. de Office Dev XP Win32 English, 55 licencias Open St. de Office Pro XP Win32 Spanish, 22 licencias Open St. de Office XP Win32 Spanish, 39 licencias Open St. de Project 2000 Win32 Spanish, 04 licencias Open St. de Visio Pro 2002 Win32 Spanish.

Control de aplicaciones en PC's

No hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PC's. Solo hay una instalación básica de Internet Explorer. En el caso de que una PC presente errores en su configuración, no se utilizan herramientas de reparación de errores y se procede a la reinstalación total del sistema causando una pérdida innecesaria de tiempo.

Tampoco se realizan actualizaciones de los programas instalados, como el Internet Explorer y el Microsoft Office. No se buscan actualizaciones ni nuevas versiones. La política de actualización de programas que se lleva a cabo permite actualizar los programas solo si es necesario debido a algún mal funcionamiento o nuevo requerimiento, lo que facilita la continuidad de los programas.

Se realizan actualizaciones periódicas del Sistema Financiero Contable GESTA. Estas actualizaciones se realizan directamente en el servidor, lo que evita hacer el control en cada una de las máquinas. Solamente el encargado de sistemas es el encargado de las instalaciones en las PC's.

Aunque para los usuarios no existen restricciones con respecto a la instalación de programas. Pueden bajar de la web cualquier aplicación e instalarla en su PC sin

ningún control sobre las licencias ni autorización previa. Esto se debe a que, para controlar problemas de licencias, virus o programas no permitidos, no hay ninguna herramienta en uso ni se realizan auditorias internas periódicas.

2.4 ANÁLISIS Y DIAGNÓSTICO DE LAS AUDITORIAS Y REVISIONES

Se ha evaluado las metodologías de control, auditorias internas y revisiones que se lleven a cabo en forma periódica, con el fin de encontrar debilidades y proponer mejoras, con base en las normativas que asesoran en el buen desempeño de la auditoría interna en una Organización.

Chequeos del sistema

Herramientas de generación y administración de reportes

En la institución las siguientes aplicaciones o sistemas generan reportes de auditoría:

- El kernel del sistema operativo de los servidores (Linux)
- El antivirus y el Proxy del servidor de Internet

Los chequeos de reportes se hacen manualmente visualizando los reportes del sistema ya que no hay una aplicación de administración de reportes, ni hay alarmas en el sistema que avisen al administrador de la ocurrencia de un evento en particular. Todos los reportes contienen los siguientes campos:

- Fecha y hora
- Fuente (el componente que disparó el evento)
- ID del evento (número único que identifica el evento)
- Computadora (máquina donde se ingresó el evento)
- Descripción (datos asociados con el evento o mensajes de error)

Reportes de los servidores

El kernel de Linux monitoriza los servidores generando entre otros, reportes sobre:

- servicios de red,
- configuración,
- utilización del CPU,

- reinicio de servidores.

Auditorias Internas

En la institución no se realizan auditorias programadas, ni rutinas de chequeos de reportes, debido a que la política actual de la institución es realizar controles solo cuando se presentan problemas o ante necesidades puntuales.

Responsabilidades de los encargados de seguridad

El técnico informático en Secretarías Técnicas Provinciales tiene las siguientes responsabilidades:

- Monitorizar y reaccionar a los avisos (precauciones) y reportes.
- Realizar chequeos aleatorios para verificar el cumplimiento de los requerimientos procedimientos de seguridad.
- Revisar los reportes de auditorias cuando es advertido de anomalías.

Auditorias de Control de Acceso

– **Control de acceso a reportes**

Los reportes se almacenan en el servidor de aplicaciones, por lo que cuentan con el control de acceso físico al servidor, pero no hay ningún control de acceso lógico a las carpetas donde están almacenados. Éstos pueden ser accedidos desde cualquier máquina conectada a la red o conociendo la clave de administrador.

– **Control de acceso a Internet**

Con respecto a las conexiones a Internet, existen registros con información sobre el número IP de la máquina conectada y la dirección de las páginas visitadas.

Cambio de clave de acceso

No se generan reportes cuando un usuario modifica su clave de acceso, no se guardan las contraseñas anteriores (para evitar la repetición), no se determina que aplicación se ha usado para realizar el cambio ni, en caso que el cambio

resulte fallido, el motivo del fallo.

Reportes del administrador

No se chequean periódicamente para verificar que sean válidos, que no haya habido intrusiones, o que no se registren ningún tipo de problemas.

Restricción de un usuario

La única manera de restringir a un usuario es porque ingresó mal el clave de acceso dos veces consecutivas, pero no se genera un registro de este evento, sino que el usuario debe avisar al administrador del sistema.

Perfil de usuario

Con los reportes que existen en la institución sería posible generar perfiles de los requerimientos de cada usuario, pero no se hacen estas tareas, los datos se encuentran en bruto sin analizar.

Auditorias de redes

- **Reportes de correo**

De los reportes de los correos no se calculan estadísticas, no se sacan líneas de base ni se grafican. El administrador solo los lee cuando supone que puede haber algún problema, a pedido de los usuarios por una supuesta falla en el servicio de mail. En el caso que se llene el espacio en disco de alguna cuenta, se envía un correo al súper usuario indicando el problema, pero no se emiten alarmas ni se generan reportes.

No se generan estadísticas sobre el departamento o usuario de la institución quién utiliza más el servicio de correo, o si a algún usuario le llegan más correos que la cantidad promedio, pero en los reportes figuran los datos del usuario que sería necesario para realizar dichos cálculos.

- **Estadísticas de red**

Existen gráficos sobre el tráfico en la red y datos detallados sobre el consumo de ancho de banda de la institución, proporcionados por el proveedor de servicio de

Internet. No existe, de manera de tener la posibilidad de individualizar, cuál de las terminales usa más tráfico de red o en que parte de la línea el tráfico es más intenso. Solo existen datos indicando la cantidad de bytes entrantes y salientes, pero no se detalla desde dónde se generan, ni con que aplicación (mail, datos, aplicaciones, mensajes, Internet, etc.).

Tampoco existen reportes sobre las aplicaciones utilizadas por cada usuario, ni las prioridades de estas aplicaciones con el fin de discriminar que cantidad de tráfico genera cada aplicación. Sería útil para ver que aplicación usa más recursos, y restringir en el caso que sea necesario. No hay datos estadísticos de los intentos de ataques. Cada vez que ocurre uno desde el exterior de la institución el sistema operativo envía un correo al súper usuario advirtiendo de esta situación.

No se hace ningún seguimiento de los reportes en busca de cambios en las estadísticas como un incremento en el uso de Internet, incremento en los ataques o la modificación en los permisos.

2.5 ANÁLISIS Y DIAGNÓSTICO DEL PLAN DE CONTINGENCIAS

Basándose en el análisis de riesgos desarrollado en el presente trabajo, se deberá determinar cuáles son los activos con mayor nivel de impacto y más vulnerables de la institución, con el fin de asesorar en el futuro un posible desarrollo de un plan de contingencia y de continuidad de servicios críticos, teniendo en cuenta los riesgos más probables y considerando las distintas soluciones posibles.

Plan de administración de incidentes

Se ha detectado que no hay planes formales para la administración de incidentes, como planes de contingencia, de recuperación de desastres o de reducción de riesgos. Pero se dispone asistencia inmediata para garantizar la continuidad de los servicios ante alguna contingencia. Actualmente las emergencias son administradas por el técnico informático aunque no hay responsabilidades

formales asignadas a los empleados.

Equipamiento de los servidores

El ECORAE en su oficina matriz cuenta con el siguiente equipamiento y plataforma de equipos servidores:

- 1 Servidor de archivos y de impresoras marca Compaq Proliant ML 350 con procesador Intel Xeo de 2.2 Ghz, dos discos duros particionados en Aplicaciones (4,45 Gb.), Respaldo (34,3 Gb.), General (4,7 Gb.) y Usuarios (4,7 Gb.), con memoria RAM de 256 Mb. y CD-ROM. El sistema operativo es Windows 2000 Server.
- 1 Servidor para el Sistema Financiero GESTA de marca Compaq Proliant ML 330 con procesador Intel Pentium III de 1.2 Ghz, dos discos duros: Local (10 Gb.), Respaldo (8 Gb.), con memoria RAM de 512 Mb. y CD-ROM. El sistema operativo es Windows 2000 Server.
- 1 Servidor de Páginas Web y Correo Electrónico de marca Compaq Proliant ML 330 con procesador Intel Pentium III de 1.2 Ghz, dos discos duros: Local (10 Gb.), Respaldo (8 Gb.), con memoria RAM de 512 Mb. y CD-ROM. El sistema operativo es Linux Red Hat ver 9.0.
- 1 Firewall de marca Dell Power Edge 2400 con un procesadores Intel Pentium III de 1.2 Ghz, dos discos duros de 10 Gb con memoria RAM de 512 Mb. y CD-ROM. El sistema operativo es Linux Red Hat ver 9.0.

Equipamiento de red

El Instituto para el Ecodesarrollo de la Región Amazónica ECORAE en su oficina matriz de la ciudad de Quito, cuenta con una red LAN para servicio de archivos, de impresión, uso del sistema administrativo financiero, alojamiento de su portal técnico y para uso del correo electrónico institucional.

Características de la red LAN:

Topología:

Lógica: Ethernet

Física: Estrella

nodos en red: 37

Velocidad: 100 Mbps.

Cableado Estructurado (Parte Pasiva)

Cables: El enlace de última milla para acceso a Internet se lo hace a través de cable UTP conectado al anillo de Fibra Óptica del proveedor de servicio (TELCONET). La red LAN interna tiene un cableado estructurado con cable de red UTP cat. 5.

Patch Cables: Los Patch cables extienden la distancia de una workstation hacia un CONCENTRADOR. La distancia máxima que hay desde el CONCENTRADOR a una estación es de 60 metros. La longitud total de la red LAN varía según las conexiones de las estaciones.

Conector: Conectores RJ45

Patch Panels: Un patch panel se usa para organizar el cable con la parte activa. Un conector estándar se usa para conectar el patch panel al bloque de punchdown.

Parte Activa (Concentrador y Switches)

Adaptadores Ethernet: Las tarjetas NIC de las PC son Ethernet y están disponibles en modelos de 10/1000 Mbits/sec.

CONCENTRADOR: Dos concentradores Nortel Networks modelo BayStack 60-24T Concentrador de 24 puertos cada uno conecta a 37 estaciones de trabajo usando como cable de red UTP cat. 5 con conectores RJ45 como medio.

SWITCH: 1 switch Cisco System modelo Catalyst 2900 series XL de 24 puertos

Estrategias de recuperación de desastres

Estrategia preactiva

- Constitución del grupo de desarrollo del plan. En el caso en que se genere un plan de emergencia, el responsable del desarrollo e implementación del plan debería ser el técnico informático en Secretarías Técnicas Provinciales y el responsable de la red en oficina matriz.
- Sistemas de información. No hay ningún responsable por la información de cada departamento, cada usuario es responsable de sus datos. Tampoco están identificados todos los sistemas de información, a modo de inventario, contemplando sus características principales, de manera que no es posible

asignarles prioridades y así determinar que sistema es más importante a la hora de recuperar la operatividad luego de un desastre. Para el efecto se ha propuesto la creación del Sistema de Información Gerencial del ECORAE que actualmente se encuentra en la aprobación del Plan para su desarrollo.

- Establecimiento del plan de acción. En caso de una emergencia sería necesario desarrollar un plan de acción, en el cual los servidores de archivos, del portal técnico y de correo electrónico serían los activos con mayor importancia al momento de continuar con las tareas, debido a que en ellos se encuentran los sistemas propios de la institución y sus datos.

Los activos más críticos a proteger serían:

- Datos:
    - Base de datos
    - Programas fuentes y ejecutables de los sistemas institucionales.
- Hardware:
    - Servidores, switch central y switches de las secretarías técnicas provincias, netmodems satelitales, equipos de radio, equipamiento informático y cables.
    - Soporte físico de backups.

Definición de niveles críticos de servicio

Los servicios más críticos de la institución son la disponibilidad de la red, el sistema de documentación, el sistema financiero Gesta y el correo electrónico institucional. Para mitigar estos riesgos es necesario que los usuarios no dejen abiertas las aplicaciones o las cierren correctamente. Para eliminar estos archivos los usuarios tienen una aplicación en los escritorios de sus PC´s. En esta situación el riesgo está controlado, pero no hay documentación formal que determine los responsables a cargo de esta contingencia, las aplicaciones y equipos a los que afecta este problema. No se hacen simulaciones de siniestros para el entrenamiento del personal.

Estrategia de acción

No hay funciones claras que debe realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas. Las situaciones se resuelven a medida que transcurren, sin la implementación de una norma a seguir

formalmente documentada.

CAPÍTULO 3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN – ASPECTOS TÉCNICOS

El propósito de establecer la implementación de este Plan de Seguridad Integral para el Proyecto Regional de Conectividad del ECORAE es para proteger la información y los activos de la institución e instituciones que se integren al proyecto, para lograr conseguir integridad, confidencialidad y disponibilidad de los datos; y las responsabilidades que deben asumir cada uno de los funcionarios encargados mientras permanezcan en cada una de las instituciones involucradas.
La propuesta de estas políticas emergen como el instrumento para concienciar a los integrantes del Proyecto Regional de Conectividad acerca de la sensibilidad e importancia que tiene la información y los servicios críticos, de tal forma que permitan al ECORAE cumplir con su misión.

Al proponer esta política de seguridad el ECORAE tiene un alto compromiso con los involucrados, agudeza técnica para establecer fallas y deficiencias, y constancia para renovar y actualizar dicha política en función de un ambiente dinámico y consensuado.

3.1 DEFINICIÓN.

Una política de seguridad integral se define como un conjunto de reglas y normas aplicadas a todas las actividades relacionadas al manejo de la información de una institución, con el fin de proteger los recursos, la información, y la reputación la misma. Esta política es una guía para asegurar la protección y la integridad de los datos y los equipos dentro del Proyecto Regional de Conectividad que el ECORAE se encuentra impulsando en la Región Amazónica Ecuatoriana.

3.2 CUMPLIMIENTO OBLIGATORIO

El cumplimiento de los estándares de seguridad y las políticas emitidas en este documento es obligatorio y debe ser considerado como una condición para la

inclusión en el Proyecto Regional de Conectividad. El ECORAE puede obviar algunas de las políticas de seguridad definidas en este documento, únicamente cuando se haya demostrado claramente que el cumplimiento de dichas políticas tendría un impacto significativo e inaceptable para el instituto. Toda excepción a estas políticas debe ser documentada y aprobada por la gerencia de Planificación del Desarrollo Sustentable del ECORAE detallando el motivo que justifica el no-cumplimiento de la política.

3.3 ORGANIZACIÓN DE LA SEGURIDAD

En esta política se definen los roles y responsabilidades a lo largo de la institución con respecto a la protección de recursos de información. Esta política se aplica a todos los funcionarios del ECORAE tanto en oficina matriz como en Secretarías Técnicas Provinciales y a todas las instituciones amazónicas que se integren al Proyecto Regional de Conectividad, ya que cada uno cumple un rol en la administración de la seguridad. Todas las instituciones son responsables de mantener un ambiente seguro y los responsables informáticos del ECORAE deben monitorear el cumplimiento de la política de seguridad definida y realizar las actualizaciones que sean necesarias producto de cambios en el entorno institucional.

3.4 EVALUACIÓN DE RIESGO

El costo de los controles y medidas de seguridad no deben exceder la pérdida que se espera evitar. Para la evaluación del riesgo se deben seguir los siguientes pasos:

- Clasificación del acceso a la información
- Ejecución del análisis del riesgo identificando áreas vulnerables, pérdida potencial y selección de controles y objetivos de control para mitigar los riesgos, de acuerdo a los siguientes estándares:

3.4.1 INVENTARIO DE ACTIVOS

Ayudan a garantizar la vigencia de una protección eficaz de los recursos, y también pueden ser necesarios para otros propósitos institucionales. El proceso de compilación de un inventario de activos es un aspecto importante de la administración de riesgos. Las instituciones involucradas en el Proyecto Regional de Conectividad deben contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, se puede asignar niveles de protección proporcionales al valor e importancia de los activos. Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo.

Se pueden tener los siguientes tipos de activos:

- Recursos de información: bases de datos y archivos importantes, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, etc.
- Recursos de software: software de aplicaciones, de sistemas, herramientas de desarrollo y utilitarios.
- Activos fijos: equipamiento informático, equipo de comunicaciones, medios magnéticos, mobiliario, etc.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales como ventilación, iluminación, energía eléctrica, aire acondicionado, etc.

3.4.2 CLASIFICACIÓN DEL ACCESO A LA INFORMACIÓN

Toda la información debe ser clasificada como:

- Restringida: Información con mayor grado de sensibilidad; el acceso a esta información debe ser autorizado
- Confidencial: Información sensible que sólo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones
- Uso interno: Datos generados para facilitar las operaciones diarias; deben ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad
- Uso general: Información que es generada específicamente para su

divulgación.

La clasificación de información debe ser documentada por el propietario. Frecuentemente la información deja de ser sensible o crítica después de cierto tiempo después de que se ha hecho pública.

3.4.3 APLICACIÓN DE CONTROLES PARA LA INFORMACIÓN CLASIFICADA

Las medidas de seguridad a ser aplicadas a los activos de información clasificados, incluyen pero no se limitan a los siguientes:

- Todo contenedor de información en medio digital debe presentar una etiqueta con la clasificación correspondiente
- La información en formato digital clasificada como de uso general puede ser almacenada en cualquier equipo de la institución.
- Todo usuario, antes de transmitir información clasificada como Restringida o Confidencial, debe asegurarse que el destinatario de la información este autorizado a recibirla
- Todo usuario que requiere acceso a información clasificada como Restringida o Confidencial, debe ser autorizado por el propietario y esa autorización debe ser documentada
- La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la misma, luego de justificar el cambio
- Información en formato digital clasificada como Restringida, debe ser encriptada por un método aprobado por los encargados de la administración de seguridad

3.4.4 ANÁLISIS DE RIESGO

Los propietarios de la información y custodios son conjuntamente responsables del desarrollo de análisis de riesgos anual de los sistemas a su cargo. Como parte del análisis se debe identificar las aplicaciones de alta criticidad como críticas para la recuperación ante desastres. Es importante identificar:

- Áreas vulnerables
- Pérdida potencial
- Selección de controles y objetivos de control para mitigar los riesgos

indicando las razones para su inclusión o exclusión.

Adicionalmente, un análisis de riesgo debe ser conducido luego de cualquier cambio significativo en los sistemas.

El análisis de riesgo debe tener un propósito claramente definido y delimitado, existiendo dos posibilidades: cumplimiento con los controles y/o medidas de protección o la aceptación del riesgo.

3.4.5 CUMPLIMIENTO

El cumplimiento satisfactorio del proceso de evaluación del riesgo se caracteriza por:

- Identificación y clasificación correcta de los activos a ser protegidos.
- Aplicación consistente y continua de los controles y/o medidas para mitigar el riesgo
- Detección temprana de los riesgos, reporte adecuado de pérdidas, así como la respuesta oportuna y efectiva ante las pérdidas ya materializadas.

3.4.6 ACEPTACIÓN DE RIESGO

Se debe aceptar el riesgo sólo cuando ha sido claramente demostrado y que las opciones disponibles para lograr el cumplimiento han sido identificadas y evaluadas, y que éstas tendrían un impacto significativo.

La aceptación de riesgo por falta de cumplimiento de los controles y/o medidas de protección debe ser documentada, revisada por las partes involucradas, comunicada por escrito y aceptada por las áreas responsables de la administración de la seguridad de la institución.

3.5 SEGURIDAD PERSONAL

Los estándares relacionados al personal deben ser aplicados para asegurarse que deban ser identificados fácilmente y que el acceso a la institución sea revocado oportunamente cuando ya no es parte de la misma. Deben desarrollarse estándares adicionales para asegurar que el personal sea consciente de todas

sus responsabilidades y acciones apropiadas en el reporte de incidentes. Esta política se aplica a todos los empleados, trabajadores, personal contratado y proveedores.

Se debe tener bien claro que los empleados y trabajadores son el recurso más valioso de la institución. Sin embargo, un gran número de problemas de seguridad de cómputo pueden ser causados por descuido o desinformación. Se deben implementar procedimientos para manejar estos riesgos y ayudar al personal de la institución a crear un ambiente de trabajo seguro.

Medidas de precaución deben ser tomadas cuando se contrata, transfiere o despide al personal. Deben establecerse controles para comunicar los cambios del personal y los requerimientos de los recursos de cómputo a los responsables de la administración de la seguridad de la información. Estos cambios deben ser atendidos a tiempo.

3.5.1 SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y RECURSOS

El departamento de Recursos Humanos o su equivalente dependiendo de la institución debe de notificar al área de informática, la renuncia o despido de empleados o trabajadores así como el inicio y el fin de los períodos de vacaciones de los mismos. Cuando se notifique un despido o transferencia, el custodio de la información debe de asegurarse que el identificador de usuario sea revocado. Todas las herramientas entregadas como computadoras, dispositivos, software, datos, documentación, manuales, llaves, tarjetas de identificación, etc., deben ser entregados a su jefe inmediato superior o al responsable de Recursos Humanos.

La seguridad es responsabilidad de todos los funcionarios involucrados con la institución y todos los dispositivos personales de información como computadoras personales o asistentes digitales personales que interactúen con los sistemas institucionales deben ser probados y autorizados por el responsable del área informática.

3.5.2 CAPACITACIÓN DE USUARIOS

Es responsabilidad del área informática promover constantemente la importancia

de las seguridad a todos los usuarios de los sistemas de información. El programa de concientización en seguridad debe contener continuas capacitaciones y charlas, adicionalmente se pueden emplear diversos métodos como afiches, mensajes, etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información.

En lo que respecta a la capacitación en seguridad se debe incluir, pero no estar limitado, a los siguientes aspectos:

- Requerimiento de identificador de usuario y contraseña
- Seguridad del PC incluyendo protección de virus
- Responsabilidades de la organización de seguridad de información
- Programas de cumplimiento
- Guías de acceso a Internet
- Guía de uso del correo electrónico
- Procesos de monitoreo de seguridad de la información utilizados
- Persona de contacto para información adicional

3.5.3 PROCEDIMIENTO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD

El personal encargado del área informática debe ser plenamente identificado por todos los funcionarios de la institución. Se debe tener el nombre del funcionario, la dirección de su vivienda, su(s) teléfono(s) particular, y la dirección y teléfono de un familiar . Si un funcionario detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al personal de informática. Si se sospecha la presencia de un virus en un sistema, el usuario debe desconectar físicamente el equipo de la red de datos, notificarlo para que el área de soporte técnico proceda a la eliminación del virus antes de reestablecer la conexión. Es responsabilidad del usuario con la asistencia respectiva, asegurarse que el virus haya sido eliminado por completo del sistema antes de conectar nuevamente el equipo a la red de datos. Lo mismo sucederá si se detecta una vulnerabilidad en la seguridad del sistema, asimismo, está prohibido para el funcionario realizar pruebas de dicha vulnerabilidad o aprovechar ésta para propósito alguno.

El área informática de cada institución debe documentar todos los reportes de

incidentes de seguridad.

3.5.3.1 Registro de fallas (Mesa de Ayuda)

El personal encargado de operar los sistemas informáticos institucionales debe registrar todos los errores y fallas que ocurren en los mismos. Estos registros deben incluir lo siguiente:

- Nombre de la persona que reporta la falla
- Fecha y hora de la ocurrencia de la falla
- Descripción del error o problema
- Responsable de solucionar el problema
- Descripción de la respuesta inicial ante el problema
- Descripción de la solución al problema
- Fecha y hora en la que se solucionó el problema

Los registros de fallas deben ser revisados semanalmente. Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una solución y deben ser almacenados para una posterior verificación.

3.5.3.2 Intercambios de información y correo electrónico

Los mensajes de correo electrónico deben ser considerados de igual manera que un memorando formal teniéndose en cuenta los tamaños, los contenidos y la identificación de particular o institucional según sea el caso. Además, deben estar sujetos a monitoreo y auditoría. Los sistemas de correo no deben ser utilizados para lo siguiente:

- Enviar cadenas de mensajes
- Enviar mensajes relacionados a seguridad, exceptuando al personal del área informática
- Enviar propaganda política
- Actividades ilegales, no éticas o impropias
- Actividades no relacionadas con el quehacer de la institución
- Publicar direcciones de correo electrónico a listas públicas

No deben utilizarse reglas de reenvío automático o direcciones que no pertenecen a la institución.

Debe establecerse un proceso formal a través de un comité institucional para aprobar la publicación de información institucional e incluir los requerimientos de información estipulada en la Ley Orgánica de Transparencia y Acceso a la Información.

3.6 ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

La administración de las comunicaciones y operaciones tanto de las oficinas del ECORAE como de las instituciones que se integran al Proyecto Regional de Conectividad, son esenciales para mantener un adecuado nivel de servicios. Los requerimientos de seguridad deben ser desarrollados e implementados para mantener el control sobre las comunicaciones y operaciones.

Los procedimientos operacionales y las responsabilidades para mantener accesos adecuados a los sistemas, así como el control y la disponibilidad de los mismos, deben tener un procedimiento formal en la institución y un formato institucional definido para todos los integrantes del proyecto. Todas las comunicaciones e intercambio de información deben ser aseguradas de acuerdo al valor de la información.

3.6.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES

3.6.1.1 Procedimientos operativos documentados

Todos los procedimientos de operaciones de los sistemas deben ser documentados y los cambios realizados a dichos procedimientos deben ser autorizados por autoridad respectiva.

Todos los procedimientos de encendido y apagado de los equipos deben ser documentados; dichos procedimientos deben incluir el detalle de personal clave a ser contactado en caso de fallas no contempladas en el procedimiento regular

documentado.

Todas las tareas programadas para su realización periódica, deben ser documentadas. Este documento debe incluir tiempo de inicio, tiempo de duración de la tarea, procedimientos en caso de fallas entre otros.

Los procedimientos para la solución de errores deben ser documentados, entre ellos se debe incluir:

- Errores en la ejecución de procesos por lotes
- Fallas o apagado de los sistemas
- Códigos de error en la ejecución de procesos
- Información de los contactos que podrían colaborar con la solución de errores.

3.6.1.2 Administración de incidentes de seguridad

Luego de reportado el incidente de seguridad, éste debe ser investigado por el área informática. Se debe identificar la severidad del incidente para tomar las medidas correctivas. El personal encargado debe realizar la investigación en forma oportuna y confidencial. Se debe mantener una documentación de todos los incidentes de seguridad ocurridos.

3.6.2 PROTECCIÓN CONTRA VIRUS

El área informática debe realizar esfuerzos para determinar el origen de la infección por virus informático, para evitar la re infección de los otros equipos. La posesión de virus o cualquier programa malicioso está prohibida a todos los usuarios. Todos los archivos adjuntos recibidos a través del correo electrónico desde el Internet deben ser revisados por un antivirus antes de abrirlos o ejecutarlos. El programa antivirus debe encontrarse habilitado en todas las computadoras de la institución y debe ser actualizado periódicamente. Es obligatorio emplear sólo los programas cuyas licencias han sido obtenidas formal y legalmente por la institución

3.6.3 COPIAS DE RESPALDO

Los responsables del área informática deben definir un cronograma para la

retención y rotación de la copias de respaldo, incluyendo el almacenamiento en uno o más ubicaciones distintas a las del área informática. Deben asegurar que se generen copias de respaldo del software legal adquirido por la institución, con etiquetas, rotación, tipo de almacenamiento y tipo de respaldo. Debe formalmente definirse procedimientos para la creación y recuperación de copias de respaldo.
Las copias de respaldo deben ser enviadas a un local remoto periódicamente, basándose en un cronograma determinado.

3.7 CONTROL DE ACCESO DE DATOS

La información manejada por las instituciones que conforman el Proyecto Regional de Conectividad y las redes asociadas deben estar adecuadamente protegidas contra modificaciones no autorizadas, divulgación o destrucción. El uso adecuado de controles de acceso previene errores o negligencias del personal, así como reduce la posibilidad del acceso no autorizado.

3.7.1 IDENTIFICACIÓN DE USUARIOS

Cada usuario de un sistema automatizado debe ser identificado de manera única, y el acceso del usuario así como de su actividad en los sistemas debe ser controlado, monitoreado y revisado.

Cada usuario de un sistema debe tener un código de identificación que no sea compartido con otro usuario. Para lograr el acceso a los sistemas automatizados, se requiere que el usuario provea una clave que solo sea conocida por él.

Debe establecerse un procedimiento para asegurar que el código de identificación de un usuario sea retirado cuando es despedido o transferido.

Cada computador personal debe bloquearse luego de quince minutos de inactividad. El usuario tendrá que autenticarse antes de reanudar su actividad.

El usuario debe ser instruido en el uso correcto de las características de

seguridad y funciones de todas las plataformas, computadoras personales, etc., y debe cerrar la sesión o bloquear su estación de trabajo cuando se encuentre desatendida.

3.7.2 SEGURIDAD DE CONTRASEÑAS

3.7.2.1 Estructura

Todas las contraseñas deben tener una longitud mínima de seis caracteres alfanuméricos y no deben contener espacios en blanco.

Las contraseñas deben ser difíciles de adivinar. Palabras de diccionario, identificadotes de usuario y secuencias comunes de caracteres no deben ser empleadas. Así mismo, detalles personales como los nombres de familiares, número de cédula de identidad, números telefónicos o fechas de cumpleaños no deben ser usadas salvo que vayan acompañadas de otros caracteres adicionales que no tengan relación directa. Las contraseñas deben incluir al menos un carácter alfabético en minúscula y uno en minúscula.

3.7.2.2 Vigencia

Todas las contraseñas deben expirar dentro de un período que no exceda los sesenta días.

3.7.2.3 Reutilización de contraseñas

No debe permitirse la reutilización de ninguna de las últimas 30 contraseñas. Esto asegura que los usuarios no utilicen las misma contraseñas en períodos regulares. Los usuarios no deben poder cambiar sus contraseñas más de una vez al día.

A los usuarios con privilegios administrativos, no se les debe permitir la reutilización de las últimas 13 contraseñas.

3.7.2.4 Intentos fallidos de ingreso

Todos los sistemas deben estar configurados para deshabilitar los identificadores

de los usuarios en caso de ocurrir tres intentos fallidos de autenticación, adicionando los liberados por el administrador.

3.7.2.5 Seguridad de contraseñas

Es importante que todos los funcionarios protejan sus contraseñas, debiéndose seguir las siguientes regulaciones:

- Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados.
- Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido de una autoridad con la autorización por escrito respectiva. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso.
- El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario.
- Los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que sean recuperadas u observadas.
- Las contraseñas deben estar siempre encriptadas cuando se encuentran almacenadas o cuando sean transmitidas a través de redes.
- El control de acceso a archivos, bases de datos, computadoras y otros sistemas mediante contraseñas compartidas está prohibido

3.7.3 CONTROLES DE ACCESO DE PROGRAMAS

Los controles de acceso de programas deben asegurar que los usuarios no puedan acceder a la información sin autorización.

Los programas deben poder generar una pista de auditoría de todos los accesos y violaciones. Éstas deben ser registradas y revisadas por el propietario o por el personal de informática.

Se debe tener cuidado particular en todos los ambientes para asegurar que ninguna persona tenga control absoluto. Los operadores de sistemas, por

ejemplo, no deben tener acceso ilimitado a los identificadores de superusuario,

3.7.4 ADMINISTRACIÓN DE ACCESO A USUARIOS

La asignación de identificadores de usuarios privilegiados deben ser revisadas cada cierto tiempo. Los propietarios de la información son responsables de revisar los privilegios periódicamente y de retirar todos aquellos que ya no sean requeridos por los usuarios. Es recomendable realizar revisiones trimestrales debido al continuo cambio de los ambientes de trabajo y la importancia de los datos.

Es responsabilidad de los propietarios de la información y de los administradores de los sistemas ver que los privilegios de acceso estén alineados con las necesidades de la institución, sean asignados basándose en requerimientos y que se comunique la lista correcta de acceso a los respectivos responsables.

En las situaciones donde los usuarios con acceso a información altamente sensible sean despedidos, se debe coordinar con el área informática para eliminar ese acceso. Se debe buscar el desarrollo de soluciones técnicas para evitar el uso de accesos privilegiados innecesarios.

Todos los usuarios que tienen acceso a cuentas privilegiadas deben tener sus propias cuentas personales para uso institucional, por lo tanto, los administradores y funcionarios con acceso a cuentas privilegiadas deben usar sus cuentas personales para realizar actividades de tipo no privilegiadas.

Cuentas de usuario que no son utilizadas por noventa días deben ser automáticamente deshabilitadas.

Todos los accesos a sistemas de información institucional deben ser controlados mediante un método de autenticación incluyendo una combinación mínima de identificador usuario / contraseña. Dicha combinación debe proveer la verificación de la identidad del usuario.

Para los usuarios con tareas similares, se debe utilizar grupos o controles de acceso relacionados a roles para asignar permisos y acceso a las cuentas.

Todos los usuarios de los sistemas institucionales deben tener un identificador de usuario único que sea válido durante su período laboral. Estos identificadores no deben ser utilizados por otros usuarios incluso luego de que el usuario original haya renunciado o ya no labore en la institución.
Los sistemas institucionales no deben permitir que los usuarios puedan tener sesiones múltiples para un mismo sistema, salvo bajo autorización específica.

3.7.5 RESPONSABILIDADES DEL USUARIO.

Todo equipo de cómputo institucional incluso el alquilado si lo hubiera, serán usados sólo para actividades relacionadas con la institución. Los sistemas institucionales no pueden ser usados para desarrollar otro software personal o externo.

El equipo computacional institucional no debe ser usado para preparar documentos para uso externo, salvo bajo la aprobación escrita de alguna autoridad.
Se deben implementar protectores de pantalla livianos con el logotipo de la institución para todos los computadores institucionales activándose luego de diez minutos de inactividad con la contraseña de desactivación.
Toda la actividad realizada utilizando un identificador de usuario determinado, es de responsabilidad del funcionario a quién le fue asignado. Por consiguiente, los usuarios no deben compartir la información de su identificador para realizar cualquier acción.

También, los usuarios están prohibidos de realizar cualquier acción utilizando un identificador que no sea el propio.

3.7.6 SEGURIDAD DE COMPUTADORAS

Se debe mantener un inventario actualizado del todo el software y hardware institucional, la responsabilidad del mantenimiento del inventario es del custodio institucional. Todo traslado o asignación de equipos debe ser requerido por alguna autoridad institucional y es responsable el técnico informático de la institución la verificación y realización del requerimiento.

Es de responsabilidad del usuario, efectuar un correcto uso del equipo de cómputo que le fue asignado, así como de los programas instalados; cualquier cambio y/o traslado deberá ser solicitado con anticipación por se respectiva área.

Asimismo, el usuario debe verificar que cualquier cambio y/o traslado del equipo de cómputo asignado, se realice por personal técnico autorizado propio de la institución, así como la instalación o desinstalación de software.
Todos los programas instalados en las computadoras de la institución deben ser legales, aprobados y periódicamente inventariados.

El uso de programas de juegos, de distribución gratuita o de propiedad personal están prohibidos salvo que sean aprobados por alguna autoridad institucional y se haya revisado la ausencia de virus.

3.7.7 CONTROL DE ACCESO A REDES.

3.7.7.1 Conexiones con redes externas

Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos y conexiones con redes externas exponen a los sistemas institucionales a niveles de mayor riesgo. Las conexiones realizadas entre la red interna de la institución e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados. El responsable informático institucional debe aprobar todas las conexiones con redes o dispositivos externos.

El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos usando paredes de fuego. Esto evita que personas externas y ajenas a la institución puedan obtener información fácil sobre la estructura de la

red institucional y sobre computadoras internas.

Para eliminar las vulnerabilidades inherentes al protocolo TCP/IP, equipo activo y firewall deben rechazar conexiones externas que parecieran originarias de direcciones internas.

3.7.7.2 Estándares generales

Los accesos a los recursos de información deben solicitar como mínimo uno de los dos factores de autenticación:

- Factor de conocimiento: algo que solo el usuario conoce. Por ejemplo contraseña
- Factor de posesión: algo que solo el usuario posee. Por ejemplo token

La posibilidad de efectuar encaminamiento y re-direccionamiento de paquetes, debe ser configurada estrictamente en los equipos que necesiten realizar dicha función.

Todos los componentes de la red deben ser identificados de manera única y su uso restringido. Esto incluye la protección física de todos los puntos vulnerables de la red. Las estaciones de trabajo y computadoras personales deben ser bloqueadas mediante la facilidad del sistema operativo, mientras se encuentran desatendidas.

Todos los dispositivos de red, así como el cableado deben ser ubicados de manera segura. Cualquier unidad de control ubicado fuera de un área con seguridad física, debe estar protegido de un acceso no autorizado.

3.7.7.3 Segmentación de redes

La arquitectura de red de las instituciones que formen parte del Proyecto Regional de Conectividad debe considerar la separación de redes que requieran distintos niveles de seguridad. Esta separación debe realizarse de acuerdo a la clase de información incluyendo equipos de acceso público si es que los ubiere.

3.7.7.4 Análisis de riesgo de red

Cualquier nodo de la red, debe asumir el nivel de sensibilidad de información más

sensible al que tenga acceso. Se deben implementar controles que compensen los riesgos más altos y tablas de valores y estados actuales.

3.7.8 CONTROL DE ACCESO AL SISTEMA OPERATIVO

3.7.8.1 Estándares Generales

Los usuarios que posean privilegios de superusuario, no necesariamente deben utilizar el mismo identificador con el que se autentican normalmente en los sistemas. Los administradores deben otorgarle los privilegios especiales o los identificadores de los usuarios que los necesiten. Todos los usuarios deben poseer un único identificador. El uso de identificadores de usuario compartidos debe estar sujeto autorización. Cada cuenta de usuario debe poseer una contraseña asociada, la cual solo debe ser conocida por el dueño del identificador de usuario. Seguridad adicional puede ser añadida al proceso como generadores de contraseñas dinámicas.

3.7.8.2 Limitaciones de horario

Las aplicaciones críticas deben estar sujetas a períodos de acceso restringidos, el acceso en un horario distinto debe ser deshabilitado o suspendido.

3.7.8.3 Administración de contraseñas

Los técnicos informáticos institucionales deben realizar pruebas mensuales sobre la calidad de las contraseñas empleadas. Para esta actividad se pueden emplear herramientas para la obtención de contraseñas.

Todas las bases de datos o aplicaciones que almacenen contraseñas deben ser aseguradas, de tal manera, que solo los responsables tengan acceso a ellas.

3.7.8.4 Inactividad del sistema

Las sesiones en los sistemas que no se encuentren activas por más de 30 minutos deben ser concluidas de manera automática. Las computadoras personales como portátiles y servidores deben ser configurados con un protector

de pantalla con contraseña, cuando sea aplicable. El período de inactividad para la activación del protector de pantalla debe ser de cinco minutos.

3.7.8.5 Estándares de autenticación en los sistemas

Los sistemas, durante el proceso de autenticación, deben mostrar avisos preventivos sobre los accesos no autorizados a los sistemas.
Los identificadores de los usuarios deben ser bloqueados luego de tres intentos fallidos, el desbloqueo de la cuenta debe ser realizado manualmente por el responsable de informática.

Los sistemas deben ser configurados para no mostrar ninguna información que pueda facilitar el acceso a los mismos, luego de intentos fallidos de autenticación usando MD5

3.7.9 MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS

3.7.9.1 Sincronización del reloj

Los relojes de todos los sistemas institucionales deben ser sincronizados para asegurar la consistencia de todos los registros de auditoría. Debe desarrollarse un procedimiento para el ajuste de cualquier desvío en la sincronización de los sistemas. Esta sincronización se hará contra un servidor internacional.

3.7.9.2 Responsabilidades generales

Los técnicos informáticos institucionales deben realizar monitoreo periódico como parte de su rutina diaria de trabajo, este monitoreo no debe estar limitado solamente a la utilización y ejecución del sistema sino que debe incluir el monitoreo del acceso de los usuarios.

3.7.9.3 Registro de eventos del sistema

Todos los eventos de seguridad relevantes de una computadora que tiene información importante para la institución, deben ser registrados en un reporte de eventos de seguridad. Esto incluye errores en autenticación, modificaciones de datos, utilización de cuentas privilegiadas, cambios en la configuración de acceso

a archivos, modificación a los programas o sistemas operativos instalados, cambios en los privilegios o permisos de los usuarios o el uso de cualquier función privilegiada del sistema.

Las bitácoras de seguridad deben ser almenados por un período de al menos tres meses, luego se almacenará permanentemente en una base de datos. El acceso a los reportes se permitirá solo a personal autorizado. En la medida de lo posible, los reportes deben ser almacenados en medios de “solo lectura”.

3.8 DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

El diseño de la infraestructura institucional, las aplicaciones institucionales y las aplicaciones de usuario final deben soportar los requerimientos generales de seguridad documentados en la política de seguridad institucional. Estos requerimientos deben ser incorporados en cada paso del ciclo de desarrollo de los sistemas, incluyendo todas las fases de diseño, desarrollo, mantenimiento y producción.

Los requerimientos de seguridad y control deben estar :

- determinados durante cualquier diseño de sistemas
- desarrollados dentro de la arquitectura del sistema,
- implementados en la instalación final del sistema

Adicionalmente, todos los procesos de desarrollo y soporte a estos sistemas deben seguir los requerimientos de seguridad incluidos en esta política de seguridad.

3.8.1 REQUERIMIENTOS DE SEGURIDAD DE SISTEMAS

3.8.1.1 Control de cambios

El área informática institucional debe retener todos los formularios de solicitud de cambio, planes de cambio de programa y resultados de prueba. Los procedimientos de prueba deben estar documentados en los formularios de

solicitud de cambio. Si se notaran problemas durante el proceso de prueba, se debe documentar el problema, realizar las modificaciones apropiadas en el ambiente de desarrollo y entregarlo para que se vuelva a probar.

3.8.1.2 Análisis y especificación de los requerimientos de seguridad

Para todos los sistemas desarrollados para las instituciones que forman parte del Proyecto Regional de Conectividad, se debe determinar los requerimientos de seguridad antes de comenzar la fase de desarrollo de la aplicación. Durante la fase de diseño del sistema, los propietarios de la información y el área informática institucional deben determinar un control adecuado para el ambiente de la aplicación.

3.9 CUMPLIMIENTO NORMATIVO

Toda ley, norma, regulación o acuerdo contractual debe ser documentado y revisado por el área legal de cada institución. Requerimientos específicos para controles y otras actividades relacionadas a estas regulaciones legales deben ser delegados al área organizacional respectiva de cada institución la cual es responsable por el cumplimiento de la norma en cuestión.
Los recursos informáticos institucionales deben ser empleados exclusivamente para tareas vinculadas con la institución.

3.9.1 REVISIÓN DE LA POLÍTICA DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

Los jefes departamentales deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente.
Es responsabilidad del personal del área informática verificar el cumplimiento de las políticas de seguridad. Las excepciones deben ser reportadas a la autoridad respectiva.

3.9.2 PROPIEDAD DE LOS PROGRAMAS

Cualquier programa escrito por algún funcionario de la institución dentro del alcance de su trabajo así como aquellos adquiridos por la institución son de propiedad de la institución.

Los contratos para desarrollo externo deben acordarse por escrito y deben señalar claramente el propietario de los derechos. En la mayoría de casos, la institución debería ser propietaria de todos los programas desarrollados, debiendo pagar los costos de desarrollo.

3.9.3 COPIAS DE RESPALDO

Los contratos con proveedores y paquetes propietarios de software deben definir claramente los límites de uso. Los funcionarios están prohibidos de copiar o utilizar dicho software de manera contraria a la provisión del contrato. Toda infracción de los derechos de autor de software tiene sanciones legales.

Los productos adquiridos por la institución para ejecutarse en una unidad de procesamiento o en un sitio particular no deben ser copiados o ejecutados en procesadores adicionales sin algún acuerdo por parte del proveedor.

Los programas no pueden ser copiados salvo dentro del límite acordado con el proveedor. Los funcionarios o asesores externos que realicen copias adicionales para evitar el costo de adquisición de otro paquete serán hechos responsables de sus acciones. Una copia tendrá el responsable informático y otra será manejada por el personal de soporte institucional.

3.9.4 INFORMACIÓN ALMACENADA EN MEDIOS DIGITALES Y FÍSICOS

Toda información almacenada en cualquier dispositivo o medio institucional, incluyendo disquetes, reportes, códigos fuentes de programas de computadora, correo electrónico y datos son de propiedad de la institución.
Las prácticas de seguridad de datos deben ser consistentes para ser efectivas. Los datos sensibles deben ser protegidos, sin importar la forma en que sean

almacenados.

3.9.5 COPIAS DE LA INFORMACIÓN

Reportes confidenciales y restringidos no deben ser copiados sin la autorización del propietario de la misma. Estos pueden ser copiados sólo para funcionarios autorizados a conocer su contenido. Los jefes departamentales son los responsables de determinar dicha necesidad, para cada persona a la cual le sea distribuido dicho reporte.

Los reportes restringidos deben ser controlados por un solo custodio, quién es responsable de registrar los funcionarios autorizados que soliciten el documento.

3.9.6 ELIMINACIÓN DE LA INFORMACIÓN

La eliminación de documentos y otras formas de información deben asegurar la confidencialidad de la información. Se deben borrar los datos de los medios magnéticos como disquetes, discos duros, cintas, CD´s que se dejen de usar debido a daño u obsolescencia, antes de que sean eliminados o dados de baja. Para no poder recuperar datos borrados, se recomienda realizar encerar los medios magnéticos de almacenamiento.

CAPÍTULO 4. PLAN DE IMPLEMENTACIÓN

Para obtener el Plan de Implementación se ha determinado un conjunto de actividades importantes a ser realizadas por las instituciones que van conformando la red del Proyecto Regional de Conectividad, las cuales van a permitan elaborar las Políticas de Seguridad desde la perspectiva de cada institución que conforma el grupo regional.

Estas actividades describen un componente muy importante dentro del plan como es el objetivo que debe cumplirse en su totalidad, el tiempo estimado de ejecución y las etapas ha ser cubiertas en cada actividad identificada.
Las actividades ha ser realizadas por cada una de las instituciones que forman parte de la red regional de conectividad son las siguientes:

- Campaña de concientización de usuarios
- Revisión y adaptación de procedimientos.
- Implementación de la política de seguridad
- Cronograma tentativo de implementación
- Evaluación de costos
- Seguridad de redes y comunicaciones
- Estandarización de la configuración del software base

Para cada actividad se ha elaborado una breve descripción (objetivo), las tareas ha ser desarrolladas (etapas), la relación de precedencia que presenta con otras actividades y un tiempo estimado de duración. El tiempo estimado para el desarrollo de cada etapa debe ser revisado antes de iniciar la misma y puede sufrir variaciones de acuerdo a dicha evaluación final.

4.1 SEGURIDAD DE RED Y COMUNICACIONES

Dependencia	Ninguna
Tiempo estimado	12 – 18 semanas

Objetivo	Para evitar manipulación de los equipos de comunicaciones por personal no autorizado y garantizar la configuración de equipos ya configurados

Etapas	I. Adaptación de sistemas de comunicaciones a políticas de seguridad (Tiempo estimado 5 semanas) - Elaboración de un inventario de equipos de comunicaciones (routers, switches, hubs, etc) - Elaboración de estándares de configuración para los equipos de comunicaciones (basarse en la documentación del proveedor) - Evaluación de equipos identificados - Adaptación de los equipos a la política de seguridad II. Adaptación a la arquitectura de red propuesta (Tiempo estimado 8 semanas) - Implementación de un firewall institucional. Controlar mediante un firewall la comunicación entre la red interna y el mundo exterior para evitar el ingreso de personas no autorizadas y el ingreso de correos no deseados. - Implementar una zona desmilitarizada (DMZ). Para esta zona se debe unificar un servidor de inspección de contenido y se la empleara para manejo de puertos y la implementación de nuevos servicios. - Implementar un sistema de antivirus para servicios de Internet (SMTP, HTTP, FTP, etc) . - Implementar un sistema de monitoreo de intrusos para detectar los intentos de intrusión o ataque desde redes externas hacia la red institucional. Asimismo se recomienda la implementación del sistema en la red interna para detectar intentos de intrusión o ataque realizados en la red interna. III. Proyectos complementarios (Tiempo estimado 4 semanas) - Evaluación de seguridad de la red inalámbrica y aplicación de controles de ser necesarios - Verificación de la configuración del firewall y otros archivos importantes del equipo servidor – Evaluación de seguridad de la red inalámbrica y aplicación de controles de ser necesarios – Verificación de la configuración del firewall y otros archivos importantes del equipo servidor

4.2CAMPAÑA DE CONCIENTIZACIÓN DE USUARIOS

Dependencia	Ninguna
Tiempo estimado	5 – 7 semanas
Objetivo	Con el objetivo de lograr un compromiso y concientización de los usuarios en temas referentes a la seguridad, se debe realizar una campaña de concientización del personal la cual esté orientada a todo el personal como conceptos básicos de seguridad y a grupos específicos con temas correspondientes a sus responsabilidades en cada institución

Etapas	Definición del mensaje a transmitir y material a ser empleado para los distintos grupos de usuarios, entre ellos: personal en general, información general sobre seguridad, políticas y estándares incluyendo protección de virus, contraseñas, seguridad física, sanciones, correo electrónico y uso de Internet Personal de sistemas: Políticas de seguridad, estándares y controles específicos para la tecnología y aplicaciones utilizadas Gerencias y jefaturas: Monitoreo de seguridad, responsabilidades de supervisión, políticas de sanción. Identificación del personal de cada departamento que se encargará de actualizar a su propio grupo en temas de seguridad. Establecimiento de un cronograma de capacitación el cual debe incluir empleados nuevos, requerimientos anuales de capacitación, actualizaciones. Desarrollar el cronograma de presentaciones - Realizar una campaña según el cronograma elaborado, asegurándose de mantener un registro actualizado de la capacitación de cada usuario e institución.

4.3 ESTANDARIZACIÓN DE LA CONFIGURACIÓN DE SOFTWARE BASE

Dependencia	Ninguna
Tiempo estimado	12 semanas
Objetivo	Con el objetivo de proteger adecuadamente la información existente en servidores y estaciones de trabajo, se debe realizar una adecuada configuración de los parámetros de seguridad del software base que soporta las aplicaciones de cada una de las instituciones de las instituciones integrantes.

Etapas	– Finalización del proceso de migración de las estaciones de trabajo al sistema operativo licenciado que tenga la institución – Elaboración de un inventario de sistema operativo de servidores y estaciones de trabajo – Elaboración de estándares de configuración para el sistema operativo instalado en las computadoras de cada institución – Elaboración de un inventario de base de datos existentes – Evaluación de los sistemas identificados – Adaptación del software base a la política de seguridad

4.4 IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

Para la implementación de la política se han elaborado los siguientes documentos que son base para trasladarlos a cada institución y han sido desarrollados para implementarlo en el ECORAE:

4.4.1 POLÍTICA DE USO DE EQUIPO COMPUTACIONAL

Esta política está orientada a establecer normas y procedimientos relacionados con el buen uso que se debe dar al equipo computacional propiedad del ECORAE.

Propósito

El uso del equipo computacional (computadores, impresoras y periféricos) es para fines laborales autorizados. Es necesario asegurar que existan controles adecuados para impedir daños u otras consecuencias negativas para el equipo computacional institucional.

Es indispensable adoptar procedimientos para minimizar el riesgo de uso indebido y lograr que el equipo que usan los funcionarios del ECORAE sea el adecuado.

Esta política será actualizada periódicamente para verificar que continúa satisfaciendo las necesidades laborales del ECORAE, sin exponer a la institución a ninguna clase de amenazas a su equipo computacional.

Definiciones de equipo computacional y usuarios

El equipo computacional que facilita la institución para un trabajo eficiente y tecnológico a sus funcionarios es:

- Un PC con procesador Pentium I o más, memoria RAM de 64 Kb. o más, un disco duro de 2 Gb. o superior, monitor VGA de 14", teclado 101 teclas enhanced, unidad de floppy de 3 ½" HD.
- Una impresora matricial, de inyección o laser
- Periféricos adicionales
- Una red LAN a 100 Mbps.
- Acceso a Internet
- Correo Electrónico

Se define usuarios del equipo de computacional a:

- Los funcionarios del ECORAE que trabajen en sus instalaciones
- Los profesionales externos que colaboren con el ECORAE que hayan sido designados como tales y a quienes se les asigne un equipo de cómputo, que tengan necesidad de utilizarlo para desarrollar su trabajo.
- Personal administrativo o técnico de las Secretarias Técnicas del ECORAE que se encuentre asistiendo a algún evento en las oficinas matriz, o al contrario.

El acceso de esos usuarios debe ser controlado.

Funciones y Obligaciones

Son funciones de los usuarios:

- Recibir formalmente el equipo de cómputo entregado para que cumpla con sus funciones con un acta de Entrega – Recepción.
- El tiempo de uso del equipo computacional son todos los días de lunes a viernes, a partir de las 08:00 hasta las 17:00
- De ser necesario, el usuario solicitará formalmente el uso del equipo de cómputo en horario que no sea el definido en el numeral anterior.
- Durante periodos vacacionales el servicio de uso del equipo informático es restringido totalmente.
- Es obligación del usuario prender el equipo de cómputo cuando empieza su trabajo todos los días y debe apagarlo el momento que termine sus labores diarias, sujetándose al horario establecido.
- A cada usuario se le asignará dos clases de claves de acceso. Una a nivel de máquina y otra a nivel de ingreso a la red. Es el único responsable de cuidar esas claves de acceso. Ninguna otra persona podrá ingresar a su computador bajo ninguna circunstancia.
- Cuando sea necesario, se informará por escrito las necesidades de Software que tenga el funcionario, y en un lapso de 24 horas será instalado por el técnico responsable, quién será el único autorizado para realizar esta labor. En caso de deterioro de la información, el usuario es el único responsable.
- El usuario que genere información valiosa relacionada con la misión del ECORAE y crea que se la debe publicar, primero debe remitirse a la dirección interinstitucional y promoción para luego, juntamente con un comité editorial y el usuario, se defina que y cómo se publicará en nuestro portal comunicacional (www.ecorae.org).

Uso

El uso del equipo de computo y software por parte de los usuarios:

- Para hacer uso del equipo informático en horarios extras, los usuarios deberán presentar la autorización emitida por el Asistente Técnico Informático;

- Todo funcionario del ECORAE que requiera el uso de un computador, o que necesiten asesoría sobre el manejo de equipo de cómputo o de algún software, deberá solicitar el servicio al Asistente Técnico y se lo atenderá en función de su disponibilidad.
- Durante el trabajo del usuario en el equipo de cómputo, NO SE PERMITE:
    a. Usar el equipo para fines no laborales (juegos, lucro personal, etc.);
    b. Golpear o maltratar el equipo o cualquiera de sus componentes.
    c. Introducir intencional o no intencionalmente, disquetes con virus informáticos.
    d. Causar daño intencional al software instalado en las máquinas.
    e. Realizar trabajos extra laborales
    f. Copiar el software instalado en el equipo sin previa autorización.
    g. Mover cualquier equipo.
    h. Instalar software ajeno a la institución.
    i. Realizar actividades que pongan en peligro al equipo o a las personas.
    j. Queda prohibido borrar, modificar, dañar o alterar de cualquier manera los programas de cómputo contenidos en los discos duros de las computadoras o en el sistema de red. Solamente el personal de la Gerencia de Tecnología tiene las facultades para hacerlo.
    k. Es responsabilidad del (los) usuario (s) mantener la integridad del equipo que está usando y reportar de manera inmediata cualquier novedad que se presentare;
    l. El Usuario dispone de los primeros 15 minutos cuando inicia sus labores para informar cualquier anomalía en los equipos, manuales o disquetes recibidos. Luego de este lapso, los daños que se presenten se analizará para determinar la causa.
    m. Cualquier material que se preste al usuario y sea dañado o no devuelto deberá reponerse con otro de la mismas características;
    n. La información del disco duro será depurada y verificada de virus, periódicamente por el por el mismo usuario, por lo que no es responsabilidad del Asistente Técnico la pérdida de información de los

usuarios.

Reglas de uso

- Leer su correo periódicamente (la correspondencia es eliminada al cumplirse un mes de haber llegado);
- El uso de una cuenta es estrictamente personal. Bajo ninguna circunstancia un usuario debe permitir que su cuenta sea empleada en actividades fuera de su control directo. El uso que se haga de una cuenta (correo electrónico, transferencia de archivos, etc.), es responsabilidad absoluta del usuario al que le fue otorgada;
- La información del disco duro será depurada periódicamente por lo que no es responsabilidad del Asistente Técnico la pérdida de información de los usuarios.
- Los servicios se deben usar para fines laborales;
- Evitar la transmisión de archivos de gran tamaño (más de un megabyte). Es preferible que el archivo o documento sea fragmentado en segmentos que no superen ese límite. El objetivo de esta norma es evitar saturaciones en los servicios de la red.

4.4.2 POLITICA DE USO DE INTERNET

Esta política está orientada a establecer normas y procedimientos relacionados con el buen uso que se debe dar al sistema de Intranet disponible en el ECORAE.

Propósito

El uso de Internet es para fines autorizados. Es necesario asegurar que existan controles adecuados para impedir violaciones de seguridad u otras consecuencias negativas para la Institución.

Es indispensable adoptar procedimientos para minimizar el riesgo de uso indebido y lograr que los sitios Internet que visitan los funcionarios del ECORAE sean los definidos en el Acuerdo de Uso.

Se reconoce que Internet es una facilidad que está pasando por cambios tecnológicos significativos y esta política será actualizada periódicamente para

verificar que continúa satisfaciendo las necesidades de seguridad de la información del ECORAE, sin exponer a la organización a ninguna de las amenazas a las que podríamos estar sometidos.

Amenazas, riesgos y peligros.

La conexión a Internet es potencialmente peligrosa, a menos que se haga mediante procedimientos de seguridad definidos y comprobados.

Algunas de las amenazas que pueden afectar al ECORAE como resultado de la conexión de los funcionarios a Internet son:

- Acceso al sistema por personas no autorizadas.
- Daños a sistemas (por ejemplo, la infectación por virus).
- Conducta ilegal (acceso a páginas lesivas a la moral), situaciones conflictivas para el funcionario o para el ECORAE.
- Falta de propiedad o responsabilidad legal de los mensajes por Internet.
- Persona o compañía que niega haber enviado un mensaje (repudio)
- Persona que intercepta un mensaje por correo electrónico y luego pretende ser remitente original (spoofing).
- Interrupción del servicio a nuestros contribuyentes por ataque externo.
- Riesgo de pérdida de la información de la Institución

Es importante tomar en cuenta que como Internet es una red de comunicaciones abierta con mensajes que pasan por numerosos servidores:

- Cualquier mensaje, documento, informe, etc. enviado por Internet puede ser potencialmente visto o modificado por un tercero.
- Cualquier mensaje, documento, informe, etc. recibido por Internet puede haber sido visto o modificado.

Acceso y Conexión a Internet

El acceso a Internet

- Debe ser solicitado por los jefes de departamento y autorizado por el Gerente de Tecnología, utilizando para el efecto el Acuerdo de Uso de

Internet.

- Debe apoyar una necesidad de la organización.
- Debe ser utilizado para fines institucionales solamente.

Se permite conexión a Internet a los equipos del ECORAE a través de una puerta manejada y segura, bajo responsabilidad del soporte técnico de la Gerencia de Tecnología de la Información.

Precauciones y Responsabilidades

El software antivirus debe estar configurado para examinar automáticamente archivos al ser abiertos. La verificación de funcionamiento debe ser realizada, en forma conjunta, con el personal técnico al momento en que se habilita el servicio en su PC.

Se debe verificar que no haya virus en ninguno de los archivos, especialmente en los archivos adjuntos a un mensaje de correo electrónico. Cualquier archivo puede ser dañino.

Siempre debe borrarse los mensajes provenientes de fuente desconocida que contengan archivos adjuntos.

Al navegar por Internet o en la intranet verifique que esté autorizado a utilizar cualquier documento o archivo. No se debe ingresar a ningún archivo que contenga material obsceno, ofensivo o ilegal y que viole los derechos de autor.
No realizar algo que pueda causar publicidad adversa o situaciones conflictivas para el ECORAE. Precautele siempre la buena imagen de la Institución.
Éstas precauciones deben ser consideradas en la configuración del firewall institucional.

Restricciones

El envío de información y mensajes previamente autorizados por Internet debe

limitarse a asuntos relacionados con la actividad del ECORAE.

La información no debe contener comentarios insultantes, obscenos o difamatorios, ni material que pueda ocasionar una situación conflictiva para el ECORAE y su personal; ni comentarios personales que puedan ser considerados como posición institucional.

El personal debe asegurarse de estar autorizado a usar cualquier información que obtenga de Internet, que la información sea de dominio público, pueda usarse libremente y que el material respete cualquier restricción de derechos de autor.

Cuando bajo autorización, se publique material de propiedad del ECORAE, verifique que tenga los mensajes apropiados en cuanto a derechos de autor. Ej.: *Este documento (información) es de propiedad del Instituto para el Ecodesarrollo Regional Amazónico. Se reservan todos los derechos. Solamente para uso interno.*

Los usuarios no deben bajar o almacenar en su computadora ningún material que pueda ser interpretado como ofensivo o pornográfico.

El personal no debe "navegar" por Internet para búsqueda de información de interés particular.

Denegación de Responsabilidad

Incluya una denegación de responsabilidad si cualquier material que aparezca en Internet es una opinión personal pero podría ser interpretado como una declaración o política oficial del ECORAE, por ejemplo: *"Las opiniones expresadas son de única responsabilidad del autor y no representan necesariamente las opiniones o la política del Instituto para el Ecodesarrollo Regional Amazónico "*.

Incluya una referencia explícita cuando el pedido o la respuesta sea claramente en nombre del ECORAE.

Los mensajes de correo electrónico por Internet, enviados a través de una puerta segura, tendrán denegaciones de responsabilidad agregadas por la puerta. Los usuarios que envíen mensajes desde computadores autónomos deben agregar lo

siguiente: "*Este mensaje de correo electrónico es confidencial y está destinado a uso exclusivo de (de los) destinatario(s) solamente. No se debe revelar el contenido a ninguna otra persona. Si usted no es el destinatario previsto, por favor notifique al remitente inmediatamente".*

Control

El contenido de la información bajada y enviada será controlado periódicamente en el servidor de correo que tiene el ECORAE.

Todo incidente o uso inapropiado de equipo del ECORAE debe ser puesto en conocimiento del jefe inmediato superior lo antes posible.

Las infracciones de esta política pueden llevar a procedimientos disciplinarios según lo dispuesto en el Código de Conducta y Contrato pertinente.

Las infracciones de esta política serán sancionadas así :

- A toda persona que utilice el Internet para enviar o recibir mensajes no relacionados con la institución se le suspenderá el servicio de Internet durante treinta (30) días.
- Si existe una primera reincidencia, se le suspenderá el servicio definitivamente.

Esta política se aplica de manera obligatoria a todo el personal del ECORAE que utilice el servicio de acceso a Internet de la Institución.

4.4.3 POLITICA DE USO DEL CORREO ELECTRÓNICO

Esta política está orientada a establecer normas y procedimientos relacionados con el buen uso que se debe dar al sistema de correo electrónico disponible en el Instituto para el Ecodesarrollo Regional Amazónico.

Objetivo

El objetivo de esta política es asegurar que todo el personal del ECORAE conozca las responsabilidades y obligaciones que tiene al ser calificado como usuario del correo electrónico interno de la institución.

Prevenir el mal uso accidental o intencional de la información y minimizar el

impacto de amenazas reales tales como saturación del sistema, accesos no autorizados, daños por virus, conducta ilegal, acoso o fraude.

Alcance

Esta política aplica para todas las funciones del sistema de correo electrónico del ECORAE e incluye a todos los servicios de mensajería interna y externa de la Institución .

Administración de usuarios

- La creación de usuario debe ser solicitada por el Jefe de Área, vía correo electrónico, con especificación de las necesidades (correo electrónico) y debe estar autorizada por el Gerente de Tecnología de Información
- Se creará el usuario y se habilitará el correo electrónico, en un máximo de 8 horas laborables después de haber recibido la solicitud correctamente llenada y debidamente autorizada.
- El intervalo de caducidad de la contraseña es de 30 hasta 60 días.
- La identificación de usuario y la contraseña son personales e intransferibles y no se debe hacer uso indebido de ellas.

Responsabilidades y Obligaciones de los Usuarios

- Cumplir con las normas y procedimientos establecidos en esta política.
- Utilizar el sistema de correo electrónico del ECORAE, exclusivamente para asuntos relacionados con su trabajo dentro de la Institución.
- El envío de la información transmitida vía correo electrónico tiene la misma responsabilidad que cualquier envío tradicional de información y requiere se cumpla con las normas dispuestas por el ECORAE.
- Asegurarse que los mensajes no contengan comentarios abusivos, obscenos, difamatorios, ni material alguno que pueda poner en situación conflictiva a el ECORAE y a su personal.
- Informar a su supervisor o jefe inmediato, en caso de recibir mensajes como los descritos en el párrafo anterior que puedan interpretarse como ofensivos.

- Eliminar mensajes que se reciban de fuentes desconocidas, por el riesgo de ataques y contagio de virus.
- Para comunicación con usuarios externos, asegúrese de incluir una denegación de responsabilidad apropiada en cada mensaje de correo electrónico así "*Este mensaje de correo electrónico es confidencial y está destinado al uso exclusivo del (de los) destinatario(s) solamente. Usted no debe revelar el contenido a ninguna otra persona. Si usted no es el destinatario previsto, por favor notifique al remitente inmediatamente*"

Restricciones

El funcionario no debe:

- Utilizar los sistemas de correo electrónico y correo externo y otros recursos de propiedad del ECORAE para beneficio personal.
- Enviar información del ECORAE que haya sido clasificada como “interna” o “confidencial” o que debe ser leída por terceros, salvo que cuente con la debida autorización para hacerlo y esté utilizando medios seguros de transmisión para protegerla adecuadamente. Para estos casos, consulte con el Coordinador de la Gerencia de Tecnología de Información para más detalles.
- Enviar mensajes de correo electrónico que puedan poner en una situación conflictiva al ECORAE, a su personal y a las instituciones públicas y privadas que trabajan coordinadamente con el ECORAE.
- Enviar información ofensiva o pornográfica, mensajes o cualquier otro tipo de material que injurie, intimide, amenace o acose al(a los) destinatario(s).
- Ejecutar archivos de programas de computadora o abrir documentos de una fuente desconocida. (los archivos adjuntos a un mensaje son una forma común de difusión de virus).
- Acceder a archivos de correo electrónico que estén en el buzón de otra persona, excepto con fines de auditoría.
- Utilizar correo electrónico y otros recursos o recibir archivos de ningún tipo infringiendo leyes de derecho de autor, si no se tiene licencia de uso previamente contratada.

Derecho del ECORAE a controlar su correo electrónico

El uso del sistema de correo electrónico del ECORAE por parte de los funcionarios (incluida cualquier persona contratada a fin de trabajar para y en nombre del ECORAE) no es privado. El ECORAE se reserva el derecho de controlar, abrir e inspeccionar el contenido de mensajes de correo. Esto puede suceder:

- Durante el manejo y mantenimiento cotidiano de recursos, previamente autorizado.
- Durante una investigación de posible actividad ilegal o uso indebido, incluido violaciones a esta política.
- Como parte de cualquier acción destinada a proteger y mantener la integridad de las redes de el ECORAE y los derechos de otras personas autorizadas a tener acceso a redes.
- Como respuesta a un proceso jurídico.

El control sólo debe realizarse con el permiso expreso de la Dirección de Recursos Humanos o del Auditor Interno del ECORAE para caso de una investigación.

No cumplimiento

Todo caso de uso inapropiado del sistema de correo electrónico del ECORAE debe ponerse en conocimiento del jefe inmediato o superior lo antes posible.
El material ilícito u ofensivo recibido por este medio, deberá ser puesto en conocimiento del departamento de recursos humanos.
Las infracciones de esta política serán sancionadas así:

- A toda persona que envíe mensajes no relacionados con temas institucionales se le suspenderá el servicio de correo electrónico) durante

treinta (30) días.

- Si existe una primera reincidencia, se le suspenderá el servicio definitivamente.

Confidencialidad

Si se envían mensajes externamente, no utilice el correo electrónico para enviar información clasificada como “interna” o “confidencial” que no puede ser leída por terceros, salvo que esté utilizando medios seguros de transmisión para protegerla adecuadamente.

El cumplimiento de esta política es mandatario para todos y cada uno de los usuarios de estos sistemas.

4.5 REVISIÓN Y ADAPTACIÓN DE PROCEDIMIENTOS COMPLEMENTARIOS

Dependencia	Actividad B
Tiempo estimado	8 semanas
Objetivo	Adaptar los procedimientos y controles complementarios de cada institución de acuerdo a lo estipulado en las políticas de seguridad
Etapas	– Revisión y adaptación de controles y estándares para el desarrollo de sistemas – Elaboración de procedimientos de monitoreo, incluyendo procedimientos para verificación periódica de carpetas compartidas, generación de copias de respaldo de información de usuarios, aplicación de controles de seguridad para información en computadores portátiles, etc. – Elaboración de procedimientos de monitoreo y reporte sobre la administración de los sistemas y herramientas de seguridad, entre ellas: antivirus, servidor proxy, servidor firewall, sistema de detección de intrusos. – Establecimiento de controles para la información transmitida a otras instituciones. – Revisión y establecimiento de controles para el almacenamiento físico de información. – Revisión y establecimiento de controles para personal externo a la institución que puede realizar labores utilizando activos informáticos de la institución para la institución.

4.6 CRONOGRAMA TENTATIVO DE IMPLEMENTACIÓN

Los proyectos antes mencionados deben ser liderados por el área informática de cada institución y sus responsables deben ser definidos individualmente para

cada uno de ellos. A continuación se presenta un cronograma sugerido para la realización de las actividades correspondientes al presente plan:

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10
Clasificación de información										
Seguridad de red y comunicaciones										
Inventario de acceso sistemas										
Campaña de concientización de usuarios										
Estandarización de configuración software base										
Revisión y adaptación de procedimientos complemntarios										

Nota: la duración de los proyectos esta sujeta a variaciones dependientes a la situación existente y al análisis realizado previo a cada actividad de cada institución participante.

4.7 EVALUACIÓN DE COSTOS

Consiste en cuantificar los daños que cada posible vulnerabilidad puede causar. Un planteamiento posible para desarrollar esto, es el análisis de lo siguiente:

- ¿Qué recursos se quiere proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?

- ¿Qué se puede hacer para proteger los bienes institucionales de una manera oportuna y económica?

Esto sirve para conocer cuales recursos vale la pena proteger. Lo que se pretende es lograr que un ataque a los bienes sea más costoso que su valor, invirtiendo menos de lo que vale. Para esto se definen tres costos fundamentales:

- **CP:** Valor de los bienes y recursos protegidos
- **CR:** Costo de los medios necesarios para romper las medidas de seguridad establecidas.
- **CS:** Costo de las medidas de seguridad

Para que la política de seguridad tenga lógica y sea consistente se debe cumplir que:

- CR > CP: el costo de un ataque debe ser mayor al costo de los bienes. Los beneficios obtenidos de romper las medidas de seguridad no deben compensar el costo del desarrollo del ataque.
- CP > CS: el costo de los bienes protegidos debe ser mayor que el costo de la protección.

Luego CR > CP > CS y lo que se busca es:

- Minimizar el costo de la protección manteniéndolo por debajo de los bienes protegidos
- Maximizar el costo de los ataques manteniéndolo por encima de los bienes protegidos .

4.8 Implementación de servicios seguros a nivel de las redes que forman parte del Proyecto Regional de Conectividad

Este es un documento que informa e instruye a los administradores de las redes institucionales que forman parte del Proyecto Regional de Conectividad que el ECORAE se encuentra ejecutando en la Amazonía Ecuatoriana, sobre las técnicas y herramientas apropiadas a usar cuando se aseguran estaciones de trabajo, servidores y recursos de red. También discute cómo hacer conexiones seguras, bloquear puertos y servicios e implementar el filtrado activo para prevenir intrusiones en la red.

Seguridad de las estaciones de trabajo

La seguridad de la red empieza con la estación de trabajo. Bien sea que esté bloqueando su propia máquina personal o asegurando un sistema institucional, una buena política de seguridad comienza con el computador individual. Después de todo, una red es tan segura como su nodo más débil.

Evaluación de la seguridad de la estación de trabajo

Cuando evalue la seguridad de una estación de trabajo de la red institucional, considere lo siguiente:

Seguridad en el BIOS
Seguridad de la contraseña
Controles administrativos
Servicios de red disponibles
Cortafuegos (firewalls) personales
Herramientas de comunicación para mejor seguridad

Seguridad en el BIOS

La protección con contraseña en el BIOS, ayudarará a prevenir que usuarios no autorizados que tengan acceso físico a sus sistemas, arranquen desde medios removibles u obtengan acceso a través del modo monousuario. Pero las medidas

de seguridad que se deberían tomar para protegerse dependen tanto de la confidencialidad de la información que las estaciones tengan como de su ubicación. Por ejemplo, si se utiliza una máquina que no tiene datos confidenciales, entonces puede que no sea crítico prevenir tales ataques. Por otro lado, si la máquia está localizada en un lugar donde sólo los usuarios autorizados o de confianza tienen acceso, entonces la seguridad del BIOS puede que no sea necesaria.

Contraseñas del BIOS

Debido a que los métodos para colocar contraseñas del BIOS varían entre fabricantes de equipos, consulte el manual de su computador para ver las instrucciones específicas.

Si olvida su contraseña del BIOS, usualmente esta se puede reconfigurar bien sea a través de los jumpers en la tarjeta madre o desconectando la batería CMOS. Por esta razón, es una buena idea bloquear el chasis del computador si es posible. Sin embargo, consulte el manual del computador o tarjeta madre antes de proceder a desconectar la batería CMOS.

Seguridad de contraseñas

Las contraseñas son el método principal para verificar la identidad de los usuarios. Por esta razón la seguridad de las contraseñas es de suma importancia para la protección del usuario, la estación de trabajo y la red.

La actividad más importante que un usuario puede hacer para proteger su cuenta contra un ataque, es crear una contraseña robusta, para lo que se recomienda:

- Cree contraseñas de al menos ocho caracteres.
- Mezcle letras mayúsculas y minúsculas.
- Mezcle letras y números.
- Incluya caracteres no alfanuméricos.
- Seleccione una contraseña que pueda recordar

Caducidad de las contraseñas

La caducidad de contraseñas es una técnica que debe ser utilizada para defenderse de las malas contraseñas dentro de la institución. La caducidad significa que luego de un tiempo determinado (60 días) se le pide al usuario que creee una nueva contraseña. Debe cuidarse que al tener tiempo limitado para las contraseñas, los usuarios tienden a escribir sus contraseñas.

Controles administrativos a usuarios

El administrador de sistemas de la institución debe decidir cuánto acceso administrativo se le otorga a los usuarios dentro de la misma a sus máquinas. Se debe permitir algunas actividades normalmente reservadas para superusuarios, tales como el reinicio o el uso de periféricos externos. Sin embargo, otras tareas importantes de administración de sistemas, tales como la modificación de las configuraciones de la red, configurar un nuevo ratón o montar dispositivos de red, son imposibles sin privilegios administrativo. En consecuencia, debe decidir cuanto acceso administrativo deberían recibir los usuarios en su red.

Permitir el acceso como administrador

Si los usuarios dentro de la organización son de confianza e interesados en la computación, entonces darles acceso administrativo quizás no sea una mala idea. Permitir el acceso administrativo a los usuarios significa que los pequeños problemas tales como añadir dispositivos o configurar interfaces de red, pueden ser manejados por los usuarios individuales, dejando a los administradores de sistemas libres para manejar la seguridad de la red y otras cosas de mayor importancia.

Por otro lado, dar acceso de superusuario a usuarios individuales puede conllevar a los siguientes problemas:

Configuración errónea de las máquinas
Ejecutar servicios inseguros
Ejecutar anexos de correo electrónico como administrador

Servicios inseguros en las estaciones de trabajo

Potencialmente, cualquier servicio de red es inseguro. Por eso es que es tan importante desactivar los servicios no utilizados. Las explotaciones a servicios se descubren y emparchan de forma regular. Por tanto es importante mantener los paquetes asociados con cualquier servicio de red actualizados.
Algunos protocolos de red son inherentemente más inseguros que otros. Esto incluye cualquier servicio que haga lo siguiente:

Pasar datos confidenciales sobre la red sin encriptar. Muchos protocolos pasan información sobre la red sin encriptar. Estos protocolos incluyen Telnet, FTP, HTTP y SMTP. Muchos sistemas de archivos de red, tales como NFS y SMB también pasan la información sobre la red sin encriptar. Es la responsabilidad del usuario cuando se estén usando estos protocolos limitar que tipo de datos son transmitidos.

Los servicios de volcado de memoria remota, pasan los contenidos de la memoria sobre la red sin encriptar. Los volcados de memoria pueden contener contraseñas o, peor aún, entradas de la base de datos u otra información confidencial. Ejemplos de servicios inherentemente inseguros incluyen los siguientes:

rlogin
rsh
telnet
vsftpd

FTP no es tan inherentemente peligroso para la seguridad de los sistemas como lo son otros, pero los servidores FTP deben ser configurados y monitoreados cuidadosamente para evitar problemas.

Los servicios que deberían ser implementados con sumo cuidado y colocados detrás de un cortafuegos incluyen:

finger

identd
netdump
netdump-server
nfs
rwhod
sendmail
smb (Samba)
yppasswdd
ypserv
ypxfrd

La próxima sección discute las herramientas disponibles para configurar un firewall o cortafuegos sencillo.

Firewalls personales en las estaciones de trabajo

Una vez configurados los servicios de red necesarios, es importante implementar un firewall. Los firewalls previenen que los paquetes de red accedan a la interfaz de la red del sistema. Si se hace una petición a un puerto que está bloqueado por un firewall, se ignorará la petición. Si un servicio está escuchando en uno de estos puertos bloqueados, no recibirá paquetes y estará efectivamente inhabilitado. Por esta razón, se debe tener cuidado cuando se configure un cortafuegos para bloquear el acceso a los puertos que no se usen, a la vez que no se bloquea el acceso a los puertos usados por los servicios configurados.

Para la mayoría de los usuarios, la mejor herramienta para configurar un cortafuegos es la herramienta de configuración gráfica que viene con el sistema operativo.

Para más información sobre cómo utilizar esta aplicación y las opciones que ofrece, consulte el manual respectivo.

Para usuarios avanzados y administradores de servidores, la mejor opción es configurar manualmente un cortafuegos con iptables.

Infraestructura de servidores

La infraestructura de servidores de las instituciones que forman parte del Proyecto Regional de Conectividad consiste en lo siguiente:

• Servidor de gestión de red LAN y del enlace satelital. Esta plataforma deberá basarse en procesadores Intel y el sistema operativo Linux. Se sugiere este sistema operativo por su funcionalidad y su costo de adquisición.

• Servidor de correo. En el caso de ser necesidad institucional, este servidor proporcionaría servicios de correo electrónico

• Servidor Web. El servidor Web suministraría servicios de Web a la institución y a las otras instituciones que se interconectan a la red local. Los servicios de Web podrían suministrarse por medio del mismo sistema operativo. El servidor Web contendría toda la información basada en la Web incluidos los enlaces a todos los contenidos de la red.

Seguridad de los servidores

Cuando un sistema es usado como el servidor institucional que da la cara al Internet ya sea como administrador de la señal satelital o como administrador de las amplificaciones de esa señal satelital, se convierte en un objetivo para ataques. Por esta razón, es de suma importancia para el administrador institucional fortalecer el sistema y bloquear servicios. Es importante aclarar que

Antes de extenderse en problemas particulares, debería revisar los siguientes consejos generales para mejorar la seguridad del servidor:

Mantener todos los servicios actualizados para así protegerse de las últimas amenazas informáticas y utilizar protocolos seguros siempre que sea posible y luego proporcionar sólo un tipo de servicio de red por máquina siempre que sea posible para finalmente supervizar todos los servidores cuidadosamente por actividad sospechosa.

Aseguramiento de los servicios

Los TCP wrappers proporcionan control de acceso a una variedad de servicios. La mayoría de los servicios modernos de redes, tales como SSH, Telnet y FTP, hacen uso de TCP wrappers, que montan guardia entre las peticiones entrantes y el servicio solicitado.

Los beneficios ofrecidos por TCP wrappers son mejorados cuando se usan en conjunto con xinetd, un super servicio que proporciona acceso adicional, conexión, enlace, redirección y control de la utilización de recursos.

Los TCP wrappers son capaces de mucho más que simplemente negar el acceso a servicios. Con esto, se pretende ilustrar cómo se pueden usar para enviar pancartas de conexión, avisar sobre ataques desde hosts particulares y mejorar la funcionalidad de conexión.

Los TCP Wrappers y las pancartas de conexión

Una buena forma de disfrazar que sistema está ejecutando el servidor, es enviando un mensaje intimidante a las conexiones clientes para un servicio. Esto también permite dejarle saber al atacante que el administrador del sistema está atento y vigilante. Para implementar un mensaje de TCP wrapper para un servicio, utilice la opción banner.

A continuación se presenta un ejemplo que implementa una pancarta para vsftpd. Para comenzar, debe crear un archivo de pancartas. Este puede estar en cualquier lugar en el sistema, pero debe tener el mismo nombre que el demonio. Para este ejemplo, se nombrará al archivo /etc/banners/vsftpd. Los contenidos del archivo se veran así:

```
220-Hello, %c
220-All activity on ftp.example.com is logged.
220-Act up and you will be banned.
```

La señal %c proporciona una variedad de información del cliente, tal como el nombre de usuario y del host, o el nombre del usuario y la dirección IP para hacer la conexión aún más intimidante. Para que esta pancarta sea presentada a las conexiones entrantes, añada la siguiente línea al archivo /etc/hosts.allow:

vsftpd : ALL : banners /etc/banners/

Aumento de la seguridad con xinetd

El super servidor xinetd es otra herramienta útil para controlar el acceso a servicios subordinados. Se puede utilizar xinetd para colocar servicios de trampa y así controlar la cantidad de recursos otorgados para frustrar posibles ataques de DoS.

Control de recursos del servidor

Una característica importante de xinetd, es su habilidad para controlar la cantidad de recursos que los servicios bajo su control pueden utilizar.

Esto se hace a través de las siguientes directrices:

cps = <number_of_connections> <wait_period>.- Indica el número de conexiones permitidas al servicio por segundo. Esta directiva acepta solamente valores enteros.

instances = <number_of_connections>.- Indica el número total de conexiones permitidas al servicio. Esta directiva acepta bien sea un valor entero o UNLIMITED.

per_source = <number_of_connections>.- Indica las conexiones permitidas a un servicio por cada máquina. Esta directiva acepta un valor entero o UNLIMITED.

rlimit_as = <number[K|M]>.- Indica la cantidad de espacio de direcciones de memoria que el servicio puede ocupar, en kilobytes o megabytes. Esta directiva acepta valores enteros o UNLIMITED.

rlimit_cpu = <number_of_seconds>.- Indica la cantidad de tiempo en segundos que un servicio puede ocupar el CPU. Esta directiva acepta un valor entero o

UNLIMITED.

Usando estas directivas puede ayudar a prevenir que cualquier servicio xinetd sobresature el sistema, resultando en un rechazo de servicio.

Protección de FTP

El Protocolo de transferencia de archivos o FTP, es un protocolo de TCP antiguo diseñado para transferir archivos sobre la red. Debido a que todas las transacciones con el servidor no son encriptadas, incluyendo la autenticación de usuarios, se considera un protocolo inseguro y debería ser configurado cuidadosamente.

La mayoría de distribuciones Linux proporciona un servidor FTP denominado vsftpd, que es una implementación de servicio FTP independiente y orientado a la seguridad. Las siguientes pautas de seguridad son para la configuración del servicio FTP vsftpd.

Pancarta de saludo de FTP

Antes de suministrar un nombre de usuario y contraseña, a todos los usuarios se les presenta una pancarta de saludo. Por defecto, esta pancarta incluye información relacionada con la versión, lo que es útil para los maleantes informáticos que estén intentando averiguar las debilidades del sistema.

Para cambiar la pancarta de bienvenida para vsftpd, añada la directiva siguiente a /etc/vsftpd/vsftpd.conf:

ftpd_banner=<*insert_greeting_here*>

Reemplace <*insert_greeting_here*> en la directiva de arriba con el texto de su mensaje de bienvenida.

Para hacer referencia a este archivo desde vsftpd, añada la siguiente directiva al archivo

/etc/vsftpd/vsftpd.conf:

banner_file=/etc/banners/ftp.msg

Acceso anónimo

La presencia del directorio /var/ftp/ activa la cuenta anónima. La forma más fácil de crear este directorio es instalando el paquete vsftpd. Este paquete configura un árbol de directorios y configura los permisos en estos directorios como de sólo lectura para los usuarios anónimos. Por defecto los usuarios anónimos no pueden escribir a estos directorios.

Carga anónima

Si desea permitir a los usuarios anónimos que carguen archivos al servidor, se recomienda que cree un directorio de sólo escritura dentro de /var/ftp/pub/.
Para hacer esto escriba: mkdir /var/ftp/pub/upload

Luego, cambie los permisos para que los usuarios anónimos no puedan ver que hay dentro del directorio, escribiendo: chmod 730 /var/ftp/pub/upload

Un listado de formato largo del directorio debería verse como:

Adicionalmente, bajo el comando vsftpd, añada la línea siguiente a /etc/vsftpd/vsftpd.conf: anon_upload_enable=YEX

Cuentas de usuarios

Debido a que FTP pasa los nombres de usuarios y contraseñas sobre redes inseguras sin encriptar, es una buena idea negar a los usuarios del sistema el acceso al servidor desde sus cuentas de usuario.
Para inhabilitar las cuentas de usuarios en vsftpd, añada la siguiente directiva a /etc/vsftpd/vsftpd.conf:

local_enable=NO

Verificación de puertos que están escuchando

Una vez que haya configurado los servicios en la red, es importante poner

atención sobre cuáles puertos estan escuchando en realidad en las interfaces de red del sistema. Cualquier puerto abierto puede ser una evidencia de una intrusión.

Existen dos soluciones básicas para listar cuales puertos están escuchando en la red. La solución menos confiable es consultar la pila de la red tipeando comandos tales como netstat -an o lsof -i. Este método es menos confiable puesto que estos programas no conectan a la máquina desde la red, sino más bien verifican que está ejecutándose en el sistema. Por esta razón, estas aplicaciones son objetivos frecuentes de atacantes para reemplazarlas. De esta forma, los instrusos intentan cubrir sus rastros si abren puertos no autorizados. Una forma más confiable de verificar que puertos están escuchando en la red es usar un escaner de puertos tal como nmap.

El comando siguiente ejecutado desde la consola, determina cuáles puertos están escuchando por conexiones TCP desde la red:

nmap -ST -O localhost

La salida de este comando es parecida a lo siguiente:

Starting nmap 3.55 (http://www.insecure.org/nmap/) at 2006-05-03 13:49 EDT
Interesting port on localhost localdomain)127.0.0.1)
(The 1653 ports scanned but not shown below are in state: closed)

Esta herramienta pueden revelar mucha información sobre el estado de los servicios ejecutándose en la máquina. Esta herramienta es flexible y puede proporcionar gran cantidad de información sobre los servicios de red y la configuración. Se recomienda la revisión de las páginas man para lsof, netstat, nmap, y services.

CONFIGURACION DE EQUIPOS DE AMPLIFICACIÓN

Mediante este procedimiento se indica como instalar el Punto de acceso “Equipo de Radio” en modo de **Station/Bridge** “Cliente” en la red básica paso a paso.

Configuración MODO CLIENTE (Station/Bridge)

Para configurar un Equipo de Radio para que funcione en Modo Cliente se deberá

realizar los siguientes pasos:

- Se debe actualizar el firmware que viene por defecto en el equipo de radio de 2.0 a 2.4, para que se puede configurar como Cliente / Acces Point.

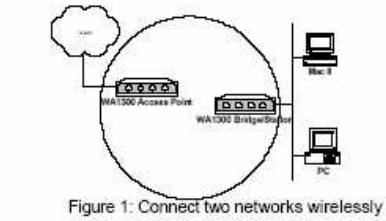


Figure 1: Connect two networks wirelessly

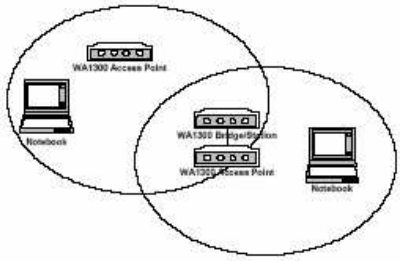


Figure 2: AP Repeater

Gráfico No.5 Configuración de equipo de radio

- Conectar mediante un cable cruzado el equipo de radio y el computador donde se va a realizar la configuración del equipo.
- Conectar el adaptador de poder del equipo de radio.
- Abrir el navegador Web para entrar en el Punto de acceso Web.
- Digitar en el Navegador Web la IP que por default viene en el equipo de Radio 192.168.1.99

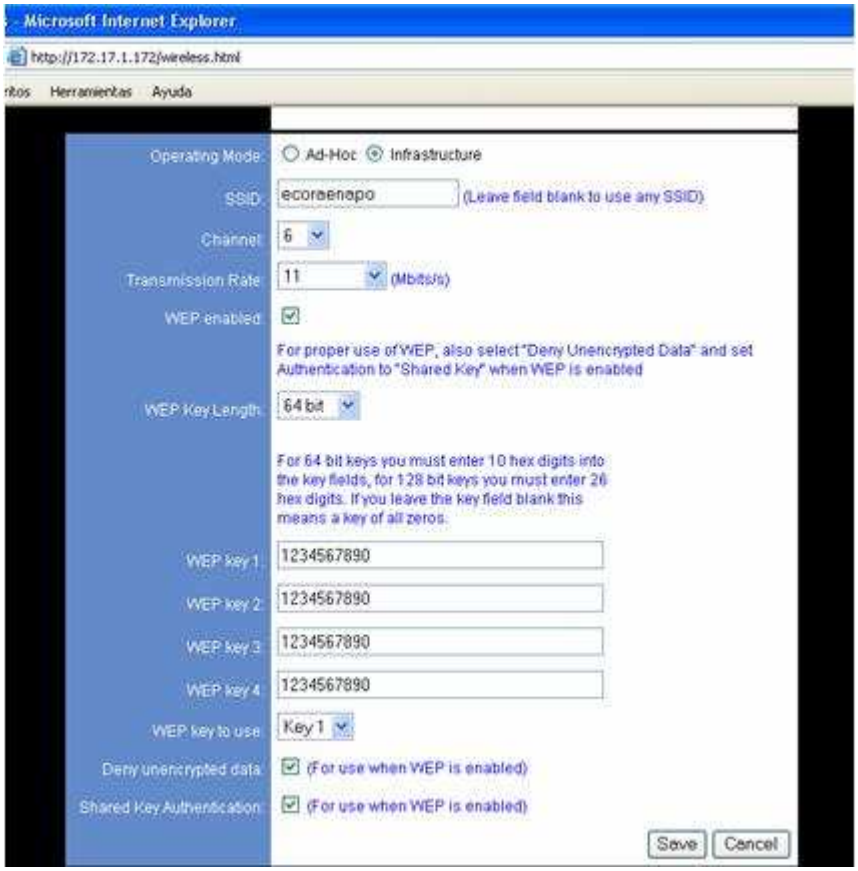
Una vez ingresado aparecerá la siguiente Ventana, en la que por defecto se ingresa automáticamente.

Una vez ingresado los datos procedemos a la configuración de las siguientes pestañas :

Pestaña de información.

que muestra toda la información general del equipo de radio: versión firrware, conexión del SSID, channel usando, MAC del equipo Acess Point, etc.

Luego procedemos a configurar la pestaña de la configuración:



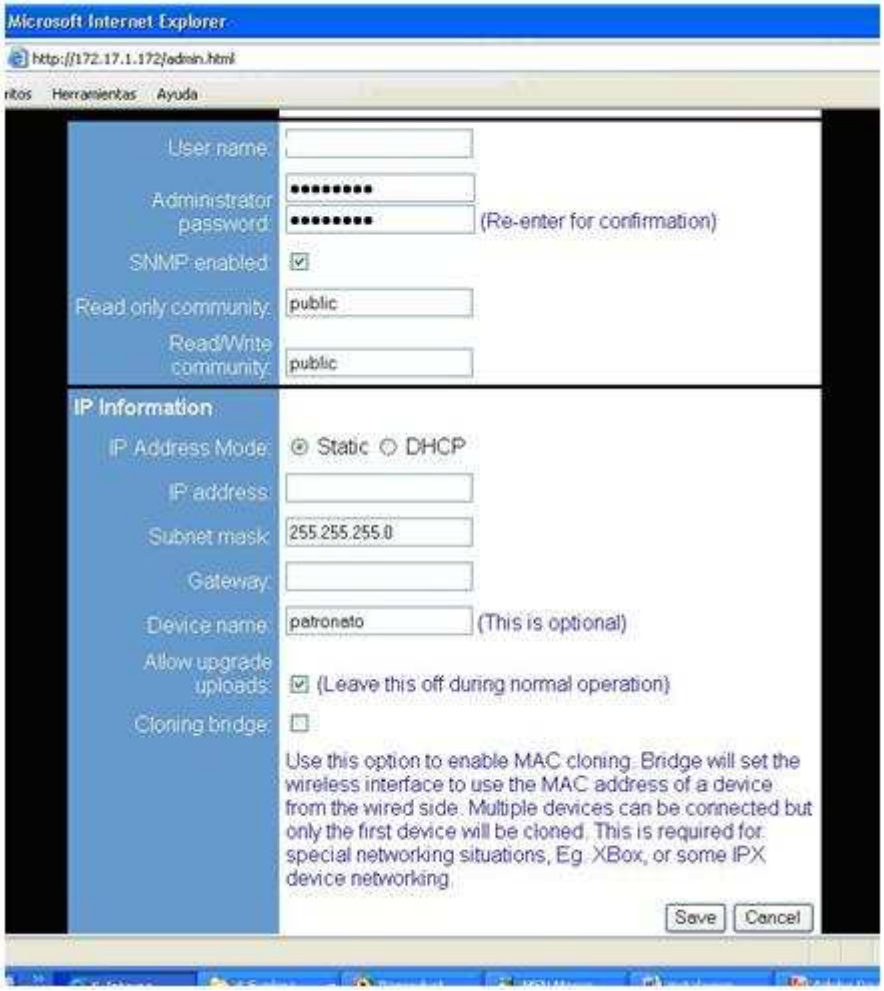
Donde se debe configurar las siguientes opciones:

Modo de Conexión	:	Debe se habilitada en Modo Infraestructura.
SSID	:	Nombre de la Red Wirelles.
Tipo de Channel	:	6 channel
Rango de Tramision	:	11 Mbps.
WEP Enable	:	activado.
Wep key Letgh	:	64 Bit.

Ingresar los Web Key 1, 2, 3, 4 que son las claves de proteccion WEP.

En la Pestaña Station, se indica las ip de las computadoras enganchadas a este equipo de Radio.

Luego de haber configurado el equipo de radio con los datos establecidos, se procede a configurar la Pestaña de administración:

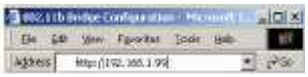


Para establecer seguridades, es preferible poner la clave del administrador y la ip del equipo de radio.

Configuración MODO AP (Access Point)

Para configurar un Equipo de Radio en Modo Acces Point se deberá realizar los siguientes pasos:

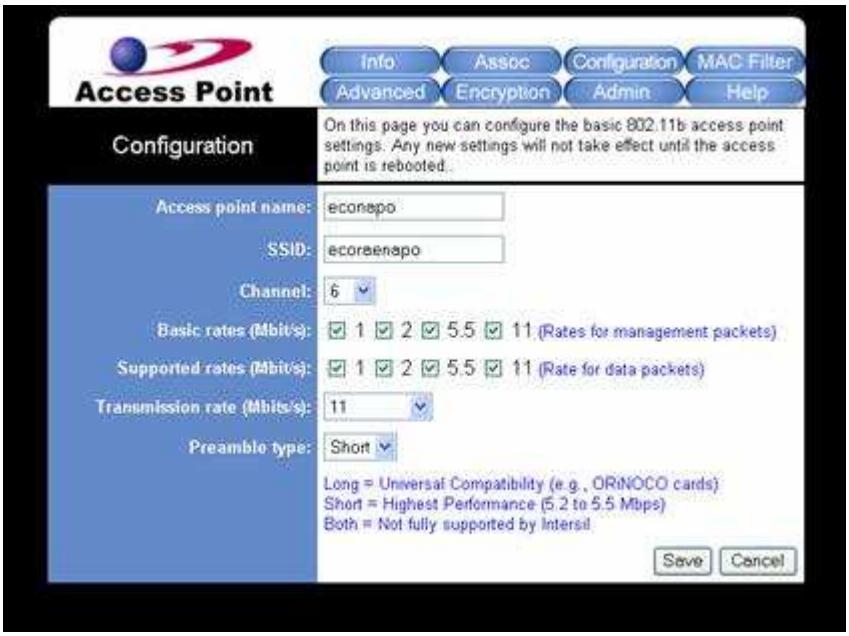
- Tiene que actualizar el firmware que viene por defecto en el equipo de radio de 2.0 a 2.4, para que se puede configurar como access point.
- Mediante el navegador Web digitar la ip por default.
- Digitar en el Navegador Web la IP que por default viene en el equipo de Radio 192.168.1.90



Una vez ingresado aparecerá la siguiente Ventana, en la que por Default se ingresa automáticamente.

Una vez ingresada la información correspondiente procedemos a configurar las siguientes pestañas:

Pestaña Configuration:



Mac Filter (Para aseguramiento mediante la dirección MAC de la tarjeta)

Para la encriptación se procede de la siguiente manera:

CAPITULO 5. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Para nadie es un secreto la importancia de implementar un plan integral de seguridad, especialmente el Proyecto Regional de Conectividad que es único y se ejecuta en una región donde la tecnología de información y comunicaciones comienza a tener un auge importante. Es efectivo utilizar una metodología comprobada que diseñe el plan de seguridad con base en las necesidades propias de cada institución participante.

- La clave para desarrollar con éxito el plan integral efectivo de seguridad consiste en recordar las políticas, estándares y procedimientos de seguridad son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica. Muchas instituciones participantes en el Proyecto Regional de Conectividad ignoran esta interrelación en un esfuerzo por simplificar el proceso de desarrollo. Sin embargo, estas mismas relaciones son las que permiten que las instituciones exijan y cumplan los requerimientos de seguridad contemplados en el plan.

- Por lo general se argumenta que las instituciones requieren una Política de Seguridad para cumplir con sus requerimientos de seguridad. Ciertamente, muchas de estas instituciones no tienen requerimientos de seguridad como tal sino que tienen necesidades institucionales que deben desarrollar e implementar. Las instituciones gubernamentales están sujetas a reglamentaciones por lo que deben ser diligentes en sus operaciones y tener responsabilidad ante la información que poseen, por lo que se requiere que se proteja la información que utilizan y a la que tienen acceso. Entonces surge la necesidad de proteger la información que se intenta manejar en un contexto regional.

- Las instituciones podrían o no necesitar más recursos, esto depende del enfoque adoptado por la organización para el desarrollo de las políticas.

RECOMENDACIONES

– Una política de seguridad generalmente exige que, en este caso, todas las

instituciones protejan la información institucional para cumplir con sus responsabilidades reglamentarias y jurídicas. Se usa mal y con frecuencia las palabras “generalmente” y “proteger” para justificar mayor inversión cuando no es necesario. Esto puede parecer contrario a la intuición, pero la inversión adicional para proteger la información no siempre garantiza el éxito. Pero si es recomendable tener un presupuesto asignado para cumplir con estos fines. Para evaluar las necesidades de inversión, debe consultar estas “reglas” en orden secuencial:

- Regla No. 1: Saber que información tiene y donde se encuentra.
- Regla No. 2 : Saber el valor de la información que se tiene y la dificultad de volverla a crear si se daña o pierde
- Regla No. 3: Saber quienes están autorizados para acceder a la información y que pueden hacer con ella.
- Regla No. 4: Saber la velocidad con que se puede acceder a la información si no esta disponible por alguna razón.

Estas cuatro reglas aparentemente son simples. Sin embargo, sus respuestas permitirán el diseño e implementación de un programa de protección a la información puesto que las respuestas pueden ser muy difíciles. No toda la información tiene el mismo valor y por lo tanto no requiere el mismo nivel de protección.

- Es clave entender por qué se necesita proteger la información.

  Desde el punto de vista regional con la implicación, en algún momento, de los 41 cantones amazónicos y sus instituciones es clave determinar la necesidad de tener una Política de Seguridad Regional. Para ello, se necesitará saber cual es la información y en donde se encuentra para que pueda proceder a definir los controles que se necesitan para protegerla.

  - Características principales de una Política de Seguridad:
    - Debe estar escrita en un lenguaje simple, pero jurídicamente viable
    - Debe basarse en las razones que tiene la institución para proteger su información
    - Debe ser consistente con las demás políticas institucionales

  - Debe hacerse cumplir – se exige y mide el cumplimiento
  - Debe tener en cuenta los aportes hechos por las personas afectadas por la política
  - Debe definir el papel y responsabilidades de las personas, departamentos y organizaciones para los que se aplica la política
  - No debe violar las políticas locales y estatales
  - Debe definir las consecuencias en caso de incumplimiento de la política
  - Debe estar respaldada por documentos aprobados, como los estándares y procedimientos para la seguridad que se adapten a los cambios en las operaciones institucionales, las necesidades, los requerimientos jurídicos y los cambios tecnológicos
  - Debe ser aprobada y firmada por la máxima autoridad institucional. No obtener este compromiso significa que el cumplimiento de la política es opcional lo que hará que fracasen.

- Redactar una política para la seguridad puede ser sencillo comparado con su viabilidad e implementación. La política organizacional y las presiones por lo general aseguran que habrá dificultad y consumo de tiempo para crear y adoptar una Política de Seguridad.

REFERENCIAS BIBLIOGRÁFICAS

1. LIBROS Y PUBLICACIONES

Holbrook P., Reynolds J. RFC 1244 – Site Security Handbook. CicNet, Isi Editors, Julio 1991

Instituto Para el Ecodesarrollo de la Región Amazónica Ecuatoriana. Proyecto Regional de Conectividad. Quito, Ecuador, 2003.

Kobashi R. Manual de Redes Sociales y Tecnología. Coordinar General CDI-SP

McClure S.,Scambray J., Kurtz G. Hackers – Secretos y soluciones para la seguridad de redes. Mc Graw Hill, España, 2003

McNab C. Seguridad de Redes. Anaya Multimedia, España, 2004.

Real Academia Española. Diccionario de la Lengua Española. Espasa, España, 2001

2. URL´s

BugTraq
http://www.securiryfocus.com/archive/1

VulnWatch
http://www.vulnwatch.org

Nmap-hackers
http://list.insecure.org/nmap-hackers/

CERT vulnerability notes
http://www.kb.cert.org/vuls

RFC 1244 – Site Security Handbook
http://www.faqs.org/rfcs/rfc1244.html

ANEXO 3

ANÁLISIS DE RIESGOS

1- INTRODUCCIÓN

El presente análisis de riesgo fue desarrollado con el propósito de determinar cuáles de los activos de las instituciones que integran el Proyecto Regional de Conectividad son más vulnerables frente a factores internos o externos que vayan a afectarlos, calculando la posibilidad de su ocurrencia, evaluando sus probables efectos, y considerando el grado en que el riesgo puede ser controlado. Para obtener esta información se desempeñaron las siguientes actividades:

Listado de los activos de la institución: se evaluaron los distintos activos físicos y de software, generando un inventario institucional.

Priorización de los activos: los activos fueron clasificados según el impacto que sufriría la institución si faltase o fallara tal activo.

Definición de factores de riesgos: luego se listaron los factores de riesgo relevantes a los pueden verse sometidos cada uno de los activos arriba nombrados.

Descripción de consecuencias: teniendo presente el inventario, se generó una descripción de las consecuencias que podría sufrir la institución si los activos son afectados por sus respectivos factores de riesgo, detallando la manera en que se protege al activo contra ese ataque en particular, y puntualizando en que grado son efectivas estas medidas.

Se asignaron las probabilidades de ocurrencia de los factores de riesgo: teniendo en cuenta los datos arriba mencionados fue posible estimar la probabilidad de ocurrencia que cada uno de los factores de riesgo representaba con respecto a los activos listados, considerando para esta estimación las medidas tomadas por la institución para mitigar su acción.

Se calcularon niveles de vulnerabilidad: una vez identificados los riesgos, se procedió a su análisis. Con toda la información recolectada, se determinó el nivel de vulnerabilidad que se asocia con cada activo listado.

Conclusiones: luego se pudo evaluar la situación actual de la institución en relación a los incidentes que pueden afectarla, calculando el porcentaje de los riesgos cubiertos y descubiertos, y un análisis sobre la escala de importancia de los activos.

Consecuencias: luego de identificar, estimar y cuantificar los riesgos, las autoridades de la institución deben determinar los objetivos específicos de control y, con relación a ellos, establecer los procedimientos de control más convenientes, para enfrentarlos de la manera más eficaz y económica posible.

En general, aquellos riesgos cuya concreción esté estimada como de baja frecuencia, no justifican preocupaciones mayores. Por el contrario, los que se estiman de alta frecuencia deben merecer preferente atención. Entre estos extremos se encuentran casos que deben ser analizados cuidadosamente, aplicando elevadas dosis de buen juicio y sentido común.

2 - ACTIVOS Y FACTORES DE RIESGOS

Presentamos los distintos activos reconocidos en cada una de las instituciones integrantes del proyecto, asignando un valor a la importancia que tienen en la institución, ponderada en una escala del 1 al 10. Esta importancia es un valor subjetivo que refleja el nivel de impacto que puede tener la institución si un incidente afecta a los activos, sin considerar las medidas de seguridad que existan sobre los mismos.

Activos a proteger	Importancia
Servidores y equipo satelital	10
Bases de datos	10
Software de aplicación, programas fuente, sistemas operativos	9
Backup	9
Datos de configuración, datos en medios externos	8
Administrador de sistemas (Departamento de sistemas)	7
Cableado, antenas, switch, hubs, módems	6
Red	6
Usuarios	5
Documentación de programas, sistemas, procedimientos administrativos locales, manuales, etc.	4
Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	3
Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	2
Datos de usuarios	1

A continuación se listan los factores de riesgo que pueden afectar a dichos activos, indicando la probabilidad de que estas contingencias ocurran, en una

escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la institución.

Probabilidad	Factores de Riesgo
Abuso de puertos para el mantenimiento remoto	1
Acceso no autorizado a datos (borrado, modificación, etc.)	2
Almacenamiento de passwords negligente	2
Ancho de banda insuficiente	1
Aplicaciones sin licencia	3
Base de datos compleja	2
Borrado, modificación o revelación desautorizada o inadvertida de información	1
Browsing de información	1
Condiciones de trabajo adversas	2
Conexión de cables inadmisible	2
Conexiones todavía activas	3
Configuración impropia del sendmail	1
Configuración inadecuada de componentes de red.	2
Conocimiento insuficiente de los documentos de requerimientos en el desarrollo	1
Copia no autorizada de un medio de datos	1
Corte de luz, UPS descargado o variaciones de voltaje	1
Daño de cables inadvertido	1
Deficiencias conceptuales en la red	3
Descripción de archivos inadecuada	2
Destrucción negligente de equipos o datos	2
Destrucción o mal funcionamiento de un componente	1
Documentación deficiente	2
Documentación insuficiente o faltante, Funciones no documentadas	2
Negación de servicio	2
Entrada sin autorización a oficinas	3
Entrenamiento de usuarios inadecuado	2
Errores de configuración y operación	1
Errores de software	2
Factores ambientales	2
Falla de base de datos	1
Falla del sistema	1
Falla en medios externos	2
Falta de auditorías	3
Falta de autenticación	1
Falta de compatibilidad	1
Falta de confidencialidad	1
Falta de cuidado en el manejo de la información (Ej. Password)	2
Falta de espacio de almacenamiento	1

Interferencias	1
Límite de vida útil - Máquinas obsoletas	2
Longitud de los cables de red excedida	3
Mal mantenimiento	2
Mal uso de derechos de administrador	1
Mal uso de servicios de mail	2
Mala administración de control de acceso (salteo del login, etc.)	1
Mala configuración del schedule de backups	3
Mala integridad de los datos	2
Mantenimiento inadecuado o ausente	1
Medios de datos no están disponibles cuando son necesarios	1
Modificación de paquetes	2
Modificación no autorizada de datos	1
No-cumplimiento con las medidas de seguridad del sistema	1
Penetración, intercepción o manipulación de líneas	3
Pérdida de backups	2
Perdida de confidencialidad en datos privados y de sistema	2
Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema	2
Pérdida de datos	2
Desvinculación del personal	3
Poca adaptación a cambios en el sistema	2
Portapapeles, impresoras o directorios compartidos	3
Prueba de software deficiente	2
Recursos escasos	3
Reducción de velocidad de transmisión	1
Reglas insuficientes o ausencia de ellas	1
Riesgo por el personal de limpieza o personal externo	3
Robo	3
Robo de información	3
Robo por uso de laptops	2
Rótulos inadecuados en los medios de datos	1
Sabotaje	3
Seguridad de base de datos deficiente	2
Sincronización de tiempo inadecuada	3
Software desactualizado	2
Spoofing y sniffing	3
Transferencia de datos incorrectos o no deseados	3
Transporte inseguro de medios de datos	2
Uso de derechos sin autorización	2
Uso descontrolado de recursos (DoS)	1
Uso sin autorización	2
Virus, gusanos y caballos de Troya	1

3 - POSIBLES CONSECUENCIAS Y MEDIDAS EXISTENTES

A continuación se listan los activos institucionales, los factores de riesgos que los afectan directamente y las consecuencias que puede acarrear la ocurrencia de estos factores. Se agrega información referida a las medidas tomadas para mitigar estas consecuencias. Por último, se ha evaluado estas medidas, indicando si son deficientes, mejorables o eficientes.

(Deficiente - Mejorable - Eficiente)

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Servidores y equipo satelital	Acceso no autorizado a datos	Robo, modificación de información	S	Seguridad física y control de acceso lógico	M
	Corte de luz, UPS descargado o variaciones de voltaje	Falta del sistema y acceso a Internet	N		D
	Destrucción o mal funcio-namiento de 1 componente	Pérdida de tiempo por necesidad de reemplazo	S	Cumplimiento de Garantía Técnica y seguro	M
	Error de configuración y operación	Aumento de vulnerabilidades e inestabilidad del sistema	S	Apoyo del equipo de la empresa proveedora	M
	Límite de vida útil – máquinas obsoletas	Deterioro en la perfomance del sistema	S	Equipamiento actual y asesoramiento permanente	M
	Mal manteni-miento	Interrupciones en el funcionamiento del sistema	S	Mantenimiento interno periódico	M
	Modificación no autorizada de datos	Inconsistencia de datos, mala configuración, fraude	S	Controles de acceso físico y lógico al servidor	M
	Robo	Pérdida de equipa-miento o información	S	Controles de acceso físico y guardias de seguridad	E
	Virus, gusa-nos y Caba-llos de Troya	Fallas generales del sistema y en la red	S	Antivirus y firewall	M

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Bases de datos	Base de datos compleja	Muchos módulos y demora en el posicionamiento	N		D
	Browsing de información	Información en malas manos	N		D
	Copia no autorizada de un mediode datos	Fuga de información	N		D
	Errores de software	Falla en el sistema	S	Asistencia inmediata por el proveedor	M
	Falla de base de datos	Obtención de información incongruente	S	Revisión constante	M
	Falla en medios externos	Pérdida de respaldos	N		D
	Mala integridad de datos	Obtención de información incongruente	S	Revisión por personal especializado	M
	Pérdida de backups	Falta de secuencia	N		D
	Pérdida de confidencialidad en datos	Modificación de datos y resultados irreales	N		D
	Portapapeles Impresoras o directorios compartidos	Intercambio y fuga de información	N		D
	Robo de información	Ataques externos	N		D
	Robo por uso de laptops	Pérdida de tiempo y de información	S	Asegurado el equipamiento	M
	Sabotaje	Pérdida de información y daño de equipos	N		D
	Spoofing y sniffing	Captura de datos	N		D
	Transferencia de datos incorrectos	Incoherencia en reportes finales	S	Revisión por personal especializado	M
	Virus, gusanos y caballos de Troya	Fallas generales del sistema y en la red	S	Antivirus y firewall	M

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Software de aplicación, programas fuente, sistemas operativos	Acceso no autorizado a datos	Robo de información	S	Control de acceso de usuarios	M
	Almacena-miento de password negligente	Conocimiento de password por otros funcionarios	S	Accesos denegados a passwords	D
	Aplicaciones sin licencia	Amonestaciones y multas	S	Exigiendo la instalación de sólo software licenciado	D
	Borrado mo-dificación o revelación desautoriza de infor.	Cambio de datos en información relevante para la institución	N		D
	Condiciones de trabajo adversas	Falta de motivación para el funcionario	S	Se provee de un buen ambiente de trabajo	M
	Configuración impropia del sendmail	Acceso externo a correos y recepción de correo no deseado	S	Firewall y configuració n	M
	Descripción de archivos inadecuada	Confusión y fallas en la búsqueda	N		D
	Documenta-ción deficiente	Falla la asistencia inmediata	S	Exigencia al proveedor	D
	Entrenamient o de usuarios inadecuado	Mal uso del equipo informático	S	Capacitación ocasional	D
	Errores de software	Obtención de mala información	S	Se provee de software licenciado	M
	Falta de compatibilidad	Errores al transportar archivos	S	Estandarizad o el uso del software	M
	Modificación de paquetes	Inadecuado ingreso de datos	N		D
	Pérdida de datos	Información incoherente	S	Respaldos continuos	D
	Software des-actualizado	Incompatibilidad en trasporte de información	N		D
	Uso sin autorización	Amonestaciones y multas	N		D
	Virus, gusa-nos y caballos de Troya	Fallas generales del sistema y en la red	S	Antivirus y firewall	M
Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Backup	Configuración inadecuada de componentes de red	No se puede obtener respaldos	N		D
	Copia no autorizada de un medio de datos	Fuga de información institucional	N		D
	Falla del sistema	No se puede obtener respaldos	N		D
	Robo de información	Obtención de información por personas inescrupulosas	N		D
	Transferencia de datos incorrectos o no deseados	No tener información importante y relevante para la institución	N		D
	Virus, gusanos y caballos de Troya		N		D

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Datos de configuración, datos en medios externos	Acceso no autorizado a datos	Desconfiguración de equipos	S	Por medio de claves y logs de acceso	M
	Destrucción negligente de equipos o datos	Falta de servicio	S	Las configuraciones son manejadas por personal autorizado	M

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Administrador de sistemas	Conexión de cables inadmisible	Mal funcionamiento de equipos y de la red	S	Cableado protegido	D
	Conexiones todavía activas	Base de datos llena y peligro de accesos no autorizados	N		D
	Configuración impropia del sendmail	Ingresos no autorizados y spam	S	Revisión de logs y firewall	M
	Configuración inadecuada de componentes de red.	Mal funcionamiento en la red y de sus servicios	S	Revisión periódica	M
	Falta de autentifica-ción	Inseguridad en el manejo de la red	N		D
	Falta de confidencia-lidad	Inseguridad en la veracidad de los datos	N		D
	Falta de cuidado en el manejo de la información	Ingresos inseguros, red expuesta, inseguridad, datos dudosos	N		D
	Mal uso de derechos de administrador	Inseguridad en los datos, inasistencia	N		D
	Mal uso de servicios de mail	Huecos de seguridad, spam, correo no institucional	N		D
	Mala Adm.-nistración de control de acceso	Login sin expiración, logias conocidos	N		D
	Mantenimien-to inadecuado o ausente	Falla en los equipos	S	Se realiza mantenimien to por demanda de fallas	D
	No cumplimiento con las medidas de seguridad	Abuso en el uso de los servicios informáticos y de comunicaciones institucionales	N	No existe	D
	Desvincula-ción del personal	Mal ambiente de trabajo y falta de reportes de daños	N		D

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Cableado, antenas, switch, hubs, modems	Conexiones de cable inadmisible	Fallas en el servicio	S	Cableado recubierto	D
	Cortes de luz, UPS descargado o variaciones de voltaje	No se brinda servicio	S	UPS y conexiones eléctricas	M
	Daño de cables inadvertido	Mal funcionamiento de equipos y de la red	S	Cableado protegido	D
	Deficiencias conceptuales en la red	Mal uso del equipo activo	S	Revisión periódica	M
	Interferencias	Baja en la velocidad de acceso a la red, mal funcionamiento de equipo activo	S	Cubierta de cables eléctricos y de red	M
	Longitud de los cables de red excedida	Falla en el servicio	S	Cumpliendo estándares	E
	Penetración, intercepción o manipulación de líneas	Permite el acceso a intrusos	S	Firewall local y global (proveedor)	M
	Reducción de velocidad de transmisión	Falla en el servicio a clientes internos y externos	S	A través del control que hace el proveedor	M

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Red	Ancho banda insuficiente	Imposibilidad de ampliar la cobertura	S	Compromisos con interesados	M
	Configuración inadecuada de componentes de red	Falla en el servicio	S	Revisión constante y asistencia inmediata	M
	Deficiencias conceptuales en la red	Mal uso del equipo activo	S	Revisión periódica	M
	Negación de servicio	Imposibilidad de trabajo	S	Revisiones periódicas	M
	Falla del sistema	Exigencia de usuarios	S	Asistencia y mantenimiento constantes	M
	Pérdida de confidencialidad o integridad de datos	Información incongruente	N		D
	Pérdida de datos	Información incompleta	N		D
	Recursos escasos	Demora en entrega de información	S	Aceptación constante de pedido de recursos	M
	Reglas insuficientes o ausencia	No se puede controlar el trabajo de usuarios	S	No existe el compromiso de autoridades	D
	Riesgo por el personal de limpieza o personal externo	Robo de información o fallas en el sistema	S	Personal conocido y guardias	M
	Uso descontrolado de recursos	Realización de actividades ajenas a la institución	S	Falta de normas	D
	Virus, gusanos y Caballos de Troya	Fallas generales del sistema y en la red	S	Antivirus y firewall	M

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Usuarios	Acceso no autorizado a datos	Robo de información	S	Claves de acceso y manejo de dominios	M
	Aplicaciones sin licencia	Uso de software no autorizado	S	Control y exigencia verbal	D
	Base de datos compleja	Dificultad y demora en el acceso de datos	S	Capacitación y mejoras constantes	M
	Borrado, modificación o revelación desautorizada d información	Pérdida y fuga de información	S	Control de acceso de usuarios	D
	Entrenamiento de usuarios inadecuado	Mal uso del equipo informático	S	Capacitación deficiente y no a todos	D
	Desvinculación del personal	Usuarios no comprometidos con trabajo institucional	S	Reuniones esporádicas y no consensuadas	D
	Poca adaptación a cambios en el sistema	Lentitud en el ingreso de datos y en el uso de equipo	N		D

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Documentación de programa sistemas, procedimientos, manuales	Conocimiento insuficiente d documentos d requerimientos desarrollo	Desconocimiento en el manejo actualización de software	N		D
	Documentación deficiente	Mal uso de procedimientos para adquisición de software	N		D
	Documentación faltante. Funciones no ducumentadas	Mal uso de paquetes por parte de usuarios. Dependencia del desarrollador	N		D
	Mala evaluación de datos de auditoria	Desconocimiento de recomendaciones	S	Dando a conocer resultados	D

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?

Hardware	Destrucción negligente de equipo	Daño del equipo	S	Capacitación	D
	Mal funciona-miento de un componente	Falla del equipo	S	Revisiones y mantenimien-to periódicos	M
	Mal mante-nimiento	Falla y destrucción del equipo	S	Revisión de normas de mantenimiento	M
	Robo	Pérdida del equipo. Devolución	S	Asegurando el equipo	M
	Uso sin autorización	Modificación en configuraciones de hardware y software	S	Restringiendo el acceso a personal externo	D

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Insumos	Corte de luz	Paralización del trabajo	S	Con UPS y plantas	M
	Falla en medios externos	Paralización del trabajo	S	Adquisición periódica de insumos	D
	Recursos escasos	No continuidad en el trabajo	S	Adquisición periódica de recursos	D

Nombre del activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Datos de usuarios	Acceso no autorizado a datos	Alteración en permisos de uso a usuarios	S	Protección en servidores	M
	Almacena-miento de password negligente	Acceso a la red de personas no autorizadas	S	Protección en servidores y restricción en acceso	M
	Documentaci ón deficiente	Desconocimiento de perfiles de los usuarios	N		D
	Mal uso de derechos de administrador	Cambios en perfiles de usuarios. Accesos no autorizados	S	Restricción de claves	M

ANEXO 4

CUESTIONARIO

Para el desarrollo del presente trabajo se entrevistaron a los distintos usuarios que forman parte del Proyecto Regional de Conectividad, donde se listan los dos cuestionarios utilizados para la realización de las mismas:

HARDWARE

- Topología y protocolos de red
  - Características del servidor
  - Impresoras y gestión de impresión
  - PC's
  - Web
  - Respaldos

SOFTWARE

- Software de servidor
- Sistema Operativo y software de las PC's
- Aplicaciones
- Gestión de virus
- Gestión de red física y lógica
- Licencias

Cuestionario 2.

¿Qué puede ir mal?
¿Con qué frecuencia puede ocurrir ?
¿Cuáles serían sus consecuencias?
¿Qué fiabilidad tienen las respuestas a las anteriores preguntas?
¿Se está preparado para continuar con los tramites institucionales sin sistemas, por un día, una semana, cuánto tiempo?
¿Cuánto cuesta una hora sin procesar, un día, una semana,...?
¿Cuánto tiempo se puede estar fuera de línea sin que los beneficiarios del sistema se molesten?
¿Se tiene forma de detectar a un funcionario deshonesto en el sistema?
¿ Se tiene control sobre las operaciones de los distintas sistemas?.
¿Cuántas personas dentro de la institución (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?.
¿Se tiene identificada la información confidencial y/o sensitiva?
¿La información confidencial y sensitiva permanece así en los sistemas?
¿La seguridad actual cubre los tipos de ataques existentes y esta preparada para adecuarse a los avances tecnológicos esperados?
¿A quien se le permite usar que recurso?
¿Quién es el propietario del recurso? Y ¿ quién es el usuario con

mayores privilegios sobre ese recurso?
¿Cuáles serán los privilegios y responsabilidades del administrador vs. la del usuario?
¿Cómo se actuaría si la seguridad es violada?

Una vez obtenida la lista de cada uno de los riesgos se efectuara un resumen del tipo:

Tipo de riesgo	Factor

El análisis de riesgo de cada recurso de la red.

Recurso	Riesgo (Ri)	Importancia (Ii)	Riesgo evaluado (Ri*Ii)

Para la obtención del riesgo total de la red se calcula:

W_R = ---------- =

Un esquema gráfico de cada enlace con IP´s públicas como privadas.
Descripción detallada de cada máquina conectada a cada enlace.

ANEXO 5
FORMULARIOS

ECORAE
Instituto para el Ecodesarrollo Regional Amazónico

FORMULARIO PARA DAR DE ALTA, BAJAS Y CAMBIOS EN LOS PERFILES DE USUARIO

Nombres completos del usuario: _____
Dirección y/o área: _____
Fecha de solicitud: _____

Tarje en la casilla correspondiente si lo requiere y marque con una X si no lo necesita

Usuario Nuevo:	Sistemas de la red		Dominio	
	Red		ECORAE	
Dirección a la que pertenece:	Correo Electrónico		ECOFIN	

Usuario que sale de la institución	Eliminar cuentas de:		Respaldos / Reasignaciones	
	Red		El responsable inmediato debe solicitar el respaldos de archivos, la custodia de ellos así como l reasignación de tareas y de equipos a la persona que reemplace al ex-usuario	
	Correo			

De ser posible, especificar las opciones dentro de la red Windows:
_____
_____
_____.

f) Director del Área del Usuario:_____ f) Director de Sistemas:_____

f) Usuario:_____

El director responsable del área a la que pertenece el usuario, es el encargado de solicitar al administrador de usuarios de la red del ECORAE dar de alta, de baja o la modificación de un usuario dentro del sistema. El usuario al recibir un identificador debe cambiar la clave de acceso que recibe mediante este formato y firmar por la recepción del mismo. La vigencia de esa clave es temporal y esta definido dentro del sistema. Cada vez que el sistema solicite cambio de clave de acceso al mismo, los usuarios son responsables del cambio del mismo. El identificador del sistema es personal e intransferible. El usuario es el único responsable de mantener la confidencialidad de sus claves de acceso y de todos los accesos que se realicen al sistema con su identificador. El usuario será responsable absoluto del uso que se le de a la información que tiene acceso su identificador. En caso de que el usuario olvide o extravíe su clave de acceso, debe solicitar al administrador de usuarios del sistema el cambio del mismo. El administrador de usuarios del sistema de la red del ECORAE es el único autorizado para cambiar o pedir el cambio de claves.
Habiendo leído todas las normas anteriores, los arriba firmantes están de acuerdo y al firmar aceptan la responsabilidad y obligación de velar por el cumplimiento de las mismas.

ECORAE
Instituto para el Ecodesarrollo Regional Amazónico

SOLICITUD DE USUARIOS

SISTEMA:		
Nombre, código y extensión del usuario		
Puesto:		
Dirección:		
Solo para llenado de Sistemas	Ingreso al Sistema Operativo	Ingreso al Sistema
identificador		
Clave de acceso		

Tipo de solicitud: (Tarque donde corresponda)

_____ Alta (Creación)

_____ Modificación (Cambios de perfil)

_____ Baja (Eliminación de cuentas)

POLITICAS Y RESPONSABILIDADES DEL USUARIO:
El director responsable del área a la que pertenece el usuario, es el encargado de solicitar al administrador de usuarios de la red del ECORAE dar de alta, de baja o la modificación de un usuario dentro del sistema. El usuario al recibir un identificador debe cambiar la clave de acceso que recibe mediante este formato y firmar por la recepción del mismo. La vigencia de esa clave es temporal y esta definido dentro del sistema. Cada vez que el sistema solicite cambio de clave de acceso al mismo, los usuarios son responsables del cambio del mismo. El identificador del sistema es personal e intransferible. El usuario es el único responsable de mantener la confidencialidad de sus claves de acceso y de todos los accesos que se realicen al sistema con su identificador. El usuario será responsable absoluto del uso que se le de a la información que tiene acceso su identificador. En caso de que el usuario olvide o extravíe su clave de acceso, debe solicitar al administrador de usuarios del sistema el cambio del mismo. El administrador de usuarios del sistema de la red del ECORAE es el único autorizado para cambiar o pedir el cambio de claves.
Habiendo leído todas las normas anteriores, los arriba firmantes están de acuerdo y al firmar

aceptan la responsabilidad y obligación de velar por el cumplimiento de las mismas.

Persona que firma:	Firma	Fecha
Director / Responsable del área del usuario		
Administrador de usuarios del sistema		
Director del área de sistemas		
Usuario		

Original: Administrador de usuarios del sistema
Copia: Usuario

ANEXO 6

USO DE LA RED CORPORATIVA E INTRANET

Red Corporativa

Definiciones

Para propósitos del presente proyecto, se utilizarán las siguientes definiciones:

Usuario: se refiere a cualquier funcionario de nombramiento o contratado por la Institución, que este autorizado para hacer uso de las Facilidades Tecnológicas Institucionales.

Equipo Institucional: aquel equipo (computadoras de escritorio, portátiles, servidores, equipos de comunicación y otros equipos electrónicos) propiedad de la Institución.

Equipo Personal: aquel equipo que perteneciendo al Usuario, hace uso de programas y facilidades informáticas brindadas por la Institución dentro de la misma.

Software Institucional: aquel software que el Subproceso de Tecnología de la información ha definido como "Software de Uso", del cual la Institución ha adquirido.

Facilidades Tecnológicas Institucionales: todos aquellos recursos de tecnología de información disponibles al Usuario que son propiedad de la Institución. Entre ellos se encuentran las licencias de uso de software, los sistemas automatizados de uso institucional, las computadoras, los servidores, las redes de transmisión de datos y sus medios de acceso, etc.

Comunicaciones electrónicas: todo tipo de comunicación enviada por medios

digitales en cualquier tipo de formato.

Uso de la red institucional y sus recursos

Las identificaciones y claves de entrada a la Red Institucional, la Intranet o a cualquier otro recurso Tecnológico son propiedad de la Institución. Estas identificaciones y claves son para uso estrictamente personal del Usuario al que se le asignan y por lo tanto la responsabilidad por el uso correcto de las mismas recae exclusivamente en el Usuario mismo.

El Usuario no deberá sin permiso expreso y por escrito hacer modificaciones a la Red Institucional, la Intranet o a sus recursos. No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la Red. Ante cualquier acción de este tipo la Institución procederá a ejecutar cualquier acción de carácter administrativo o laboral que corresponda.

En la Red Institucional no está permitida la operación de software para la descarga y distribución de archivos de música, videos y similares. Cualquier aplicación de este tipo que requiera ser utilizada, deberá ser previamente consultada con el Subproceso Sistema Integrado de Información.

Instalación y uso de software

El único software que será instalado en el computador del Usuario, será aquel que previamente haya sido estandarizado y/ o autorizado por la Institución y para lo cual esta dispone de las licencias respectivas a su nombre.

Todo Usuario está obligado a conocer el alcance de uso de cada una de las licencias de software a su disposición. Esta información debe solicitarla al encargado de asistencia a usuarios.

Adicionalmente, todo Usuario debe garantizar el cumplimiento de los siguientes lineamientos:

- El Usuario no deberá participar en la copia, distribución, transmisión o cualesquiera otras prácticas no autorizadas en las licencias de uso de software.
- Toda instalación, desinstalación o traslado de software (incluyendo aquellos de "dominio público" o de "distribución libre"- "shareware", "freeware", etc.) desde y hacia el Equipo Institucional requiere autorización y coordinación

previas con el Subproceso Sistema Integrado de Información.

- Si el Usuario requiere la instalación de en su Equipo Personal, deberá firmar un documento de responsabilidad de uso, previa coordinación con el Subproceso Sistema Integrado de Información y previa autorización del Director respectivo.
- Cualquier requerimiento de licencias de software que deban ser consideradas como parte del Equipo Institucional y que podrían ser utilizadas por el Usuario para el desarrollo de la actividad de la Institución, deberá ser solicitado en forma escrita al Subproceso Sistema Integrado de Información para su respectiva valoración y autorización.
- Cualquier software que se haya instalado en el Equipo Institucional que no cumpla con lo estipulado anteriormente, será desinstalado sin que ello derive ninguna responsabilidad para la Institución. Al usar una licencia de software que ha sido instalado en el Equipo Institucional o en el Equipo Personal, el Usuario reconoce los derechos de la Institución anteriormente descritos y consiente en ellos.

Facultades y deberes de la Institución

La Institución adquirirá software exclusivamente bajo licencia, en propiedad, en un proceso debidamente documentado y autorizado por el Usuario y en algunos casos por el Subproceso Sistema Integrado de Información.

La Institución delega al Subproceso Sistema Integrado de Información, la administración, resguardo e instalación del software licenciado. Asimismo, le queda prohibido hacer copias (incluyendo las de respaldo cuando no estén permitidas) o instalaciones en exceso del número de licencias disponibles y legalmente negociadas con el proveedor del software.

El responsable del Subproceso Sistema Integrado de Información deberá mantener un registro permanente del Software Institucional, el cual debe considerar al menos los siguientes aspectos:

Nombre del software

Proveedor

Propósito del software

Número de licencias adquiridas
Número de licencias instaladas
Ubicación de las licencias instaladas
Fecha de la última revisión de las instalaciones realizadas
Responsable de la revisión de las instalaciones realizadas

Con el objetivo de identificar amenazas, vulnerabilidad, impacto y riesgo al que está expuesta la Institución, el área responsable debe realizar una revisión semestral de una muestra del Equipo Institucional (no así en el Personal) sobre los riesgos asociados con el incumplimiento de la presente Política por parte del Usuario, debiendo considerarse los siguientes aspectos:
Las revisiones versarán únicamente sobre el Software instalado en el Equipo Institucional.
Para efectos de dicha revisión, y cada vez que se le requiera con ese propósito, el Usuario deberá facilitar el Equipo Institucional y prestar toda la colaboración que le sea posible.

Incumplimiento

La Institución hará responsable al Usuario del conocimiento del la presente Política y las consecuencias que se derivarían de su incumplimiento. Asimismo, el Usuario deberá conocer estas políticas desde su ingreso a la Institución.
La Institución se reserva el derecho de evaluar periódicamente el cumplimiento de estas Políticas. Cualquier acción disciplinaria derivada del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo a los procedimientos establecidos.
En materia de irregularidades o incumplimiento en el uso del software, el Usuario que no cumpla con esta política, será directamente responsable de las sanciones legales (que por responsabilidad laboral, penal y/o civil se incurra) derivadas de sus propios actos. Igualmente, será responsable de los costos y gastos en que pudiera incurrir la Institución derivados de la defensa por el uso no autorizado o indebido de licencias de software.

Responsables y funciones

Los Responsables en las diferentes secretarias técnicas provinciales son los técnicos informáticos y deben dominar la información general de su secretaría.

Cada Secretaría Técnica Provincial puede contar con apoyo de los técnicos informáticos de matriz o de las otras secretarías, para que puedan implementar de una forma más adecuada el desarrollo operativo y actualización permanente del equipo informático comunicacional.

En coordinación con el encargado del Subproceso Sistema Integrado de Información, los Responsables deben definir y escribir los términos de referencia de cualquier proyecto tecnológico que se proponga implementar.

Los Responsables deben llevar un control periódico del pago que se hace al Proveedor del servicio satelital tanto de la secretaría técnica provincial como de los municipios que conformen el Proyecto Regional de Conectividad de su provincia.

Otras que se indiquen en otros apartados de esta Política.

Fotografías

Todas las fotografías que sirvan para uso institucional deben tener un tamaño máximo de 1,000 píxeles y los únicos formatos permitidos son “jpg” o “gif”.

Si se desean poner al aire videos, se pueden colocar archivos que contengan videos para que sean descargados en las computadoras de los usuarios.

Del hospedaje de otros sitios en los servidores la Institución

En los servidores de la Institución se hospedarán, sólo por tiempo limitado, otros Sitios Internet sólo si la Institución es patrocinador oficial del proyecto.

Intranet

El acceso a la Intranet está limitado sólo al personal que en forma permanente trabaja para la Institución en cualquiera de sus sedes. La Gestión de Recursos Organizacionales es quien debe indicar que personas están en la nómina institucional.

El/la responsable del Subproceso Sistema Integrado de Información es la única autorizada para asignar y distribuir las palabras clave que sean necesarias para

ingresar a la Intranet.

Se pueden desarrollar accesos parciales a la Intranet para el personal que sin ser permanente, requiere tener acceso a ciertas secciones e información.

En la Intranet se puede colocar toda la información de las distintas secretarías técnicas o áreas que así lo expresen, con la debida autorización del responsable del Subproceso Sistema Integrado de Información Director.

Conocimiento y aceptación de la política por parte del usuario

En consideración de lo expresado en la política anterior, yo, _____ en mi calidad de funcionario del ECORAE portador de la cédula de ciudadanía número _____, manifiesto que he leído y entendido enteramente esta Política por lo que cumpliré con ella en su totalidad. Asimismo, reconozco que mi incumplimiento para con esta Política podría acarrear la responsabilidad civil y penal no sólo para mi persona sino también para la Institución. Por ésta razón, acepto que puedo ser sancionado por la Institución como corresponda; sin perjuicio de la aplicación de las responsabilidades civiles y penales respectivas.

Firma _____

Nombre _____

GLOSARIO DE TÉRMINOS

Control: capacidad de comprobación e inspección para ejercer o dirigir una influencia sobre una situación dada o hecho. Acción tomada para hacer un hecho conforme a un plan.

Decisión: Resolución que se toma o se da en una cosa ante la que existen dos o más alternativas.

Estrategia: Arte de coordinar un conjunto de decisiones que se toman para determinar políticas, metas y programas.

Meta: Fin u objetivo cuantificado a valores predeterminados.

Norma: Regla sobre la manera como se debe hacer o realizar un procedimiento o proceso.

Plan: Determinación de algunos objetivos precisos y de los medios que deben emplearse para alcanzarlos en un plazo dado.

Política: Definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

Procedimiento: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.

Programa: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

Pronóstico: Señalar por donde se conjetura un comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en

acontecimientos futuros.

Proyección: Predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas

Riesgo: Contingencia o posibilidad de que suceda un daño, desgracia o contratiempo. Cada uno de los imprevistos, hechos desafortunados, etc. , que puede tener un efecto adverso. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.[5]

5 Diccionario de la Real Academia de la Lengua