ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA UNA ENTIDAD FINANCIERA, CON EL PROPÓSITO DE MITIGAR LOS RIESGOS QUE PODRÍAN PRESENTARSE A CAUSA DE ATAQUES CIBERNÉTICOS, INTERNOS O EXTERNOS Y SALVAGUARDAR LA INTEGRIDAD DE LA INFORMACIÓN, BASADOS EN EL ESTÁNDAR ISO 27001."

TRABAJO DE TITULACIÓN

Previo a obtención de Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

VICENTE HERNÁN SACOTO MOSQUERA

Guayaquil - Ecuador

2019

AGRADECIMIENTO

Agradezco a mis padres Vicente y Rosa quienes me ayudaron siempre con buen ejemplo me inculcaron el amor por el aprendizaje.

Vicente Hernán Sacoto Mosquera

DEDICATORIA

Dedico este trabajo a mis padres Vicente y Rosa quienes siempre han sido un apoyo para mí y siempre me incentivaron a alcanzar nuevas metas.

Vicente Hernán Sacoto Mosquera

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire C., MSIG.

DIRECTOR MSIG - MSIA

Ing. Lenin Freire C., MSIG.

DIRECTOR DE PROYECTO DE GRADUACIÓN

Ing. Omar Maldonado D., MSIG.

MIEMBRO DE TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Titulación de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

(Reglamento de Graduación de la ESPOL).

Vicente Hernán Sacoto Mosquera

RESUMEN

Atendiendo el requerimiento del directorio financiero de la entidad, se ha determinado la necesidad de trasladar la matriz de la institución a la ciudad de Guayaquil, ya que actualmente se encuentra en la ciudad de Quito y por las nuevas necesidades de la empresa se requiere el cambio a la ciudad de Guayaquil, convirtiéndose la sucursal de la ciudad de Quito en sucursal mayor y la sucursal de la ciudad de Guayaquil en nueva matriz, por esta razón se requiere la IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA LA ENTIDAD FINANCIERA, CON EL PROPÓSITO DE MITIGAR LOS RIESGOS QUE PODRÍAN PRESENTARSE A CAUSA DE ATAQUES CIBERNÉTICOS, INTERNOS O EXTERNOS Y SALVAGUARDAR LA INTEGRIDAD DE LA INFORMACIÓN, BASADOS EN EL ESTÁNDAR ISO 27001, los cuales deben estar acorde a la realidad de la nueva dirección de la matriz.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

A raíz del inicio de la era digital las empresas y compañías en general han ido con el paso del tiempo implementando medidas de seguridad direccionadas a proteger la información que poseen para el correcto desempeño de sus funciones en todos sus ámbitos, teniendo que ser cada vez más exigentes en las seguridades para este fin cada vez que los ataques de delincuentes informáticos han ido evolucionando y haciéndose más frecuentes y eficientes.

Se tiene entonces la necesidad de crear el departamento de seguridad informática, el cual está a cargo de la implementación de un esquema de seguridad informática para la entidad financiera, con el propósito de mitigar los riesgos que podrían presentarse a causa de ataques cibernéticos, internos o externos y salvaguardar la integridad de la información, basados en el estándar ISO 27001. Aprovechando el cambio de Matriz de la ciudad de Quito a la ciudad de Guayaquil., para de esta manera poder realizar la implementación del nuevo esquema de seguridad en toda su extensión y lograr alcanzar el 100% de efectividad.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

Los ataques cibernéticos son una realidad que amenaza la información de varios sistemas de diversas características y funciones y los sistemas financieros no son un excepción, al realizar el cambio de domicilio de la Matriz la compañía se ve en la obligación de implementar las políticas y procedimientos de seguridad para salvaguardar la información de nuestros clientes y de esa manera asegurar la confidencialidad, integridad y disponibilidad de la información ofreciendo fluidez de las operaciones y transparencia.

Desde la creación de la empresa se ha tenido reportes e informes generados por los diferentes sistemas de seguridad informática que nos advierten y protegen de ataques perpetrados provenientes no solo de

orígenes locales sino incluso ataques provenientes de orígenes externos, entiéndase hackers nacionales e internacionales, ataques a nuestros sistemas de correos, ataques cibernéticos a nuestros servidores, intentos de robo de información por parte de empleados activos en nómina y también por parte de ex empleados.

Por esta razón directorio financiero solicita la implementación de un esquema de seguridad informática basado en las normas ISO 27001 para la nueva matriz en la ciudad de Guayaquil.

En vista de que el esquema actual fue creado y generado en el pasado por personal de sistemas no expertos en asuntos de seguridad, se da luz verde a la creación de este nuevo esquema esta vez contando con el asesoramiento de personal calificado, los cuales son expertos en seguridad de la información y con experiencia en los temas requeridos por la empresa.

1.2. Descripción del problema

Actualmente la entidad financiera tiene la mayor parte de su infraestructura informática en la ciudad de Quito, pero por orden de la directiva se ha decidido que la sucursal mayor de la ciudad de Guayaquil, pase a ser la nueva matriz, por lo que se debe dotar a la sucursal mayor de equipos, software e infraestructura necesaria para

dicho cambio, así como actualizar sus normativas y definir nuevas políticas de seguridad de la información con el fin de que La sucursal Guayaquil pueda operar ahora como matriz, quedando Quito como sitio alterno. Al momento la nueva matriz Guayaquil no cuenta con políticas y normativas actualizadas para la situación real actual, se necesita definir nuevas normativas de seguridad informática, políticas y procedimientos que establezcan controles de seguridad en cuanto a accesos y uso de los recursos informáticos, así como un adecuado uso del data center, Se requiere mejorar la seguridad física, estableciendo políticas de accesos al centro de cómputo, ya que se han presentado incidentes como fuga o pérdida de información, ingresos no autorizados, entre otros problemas de seguridad que afectan a la información. Se debe mantener controles de seguridad para garantizar la disponibilidad, confidencialidad e integridad de los activos de información.

El no mantener una política de seguridad, aumenta el riesgo de que ocurran pérdidas de información o de recursos informáticos, que afecten los procesos críticos de la entidad, impidiendo a su vez la correcta continuidad del negocio.

Los índices estadísticos de incidentes que afectan a la seguridad de la información han aumentado notablemente en nuestro país en los

últimos años, haciendo imperativo que se actualicen las normas y se creen mecanismos preventivos y disuasivos para de esta manera se pueda evitar que la nueva matriz sea víctima de ataques tanto a nivel físico dentro de sus instalaciones como a nivel virtual a través de sus portales de atención al cliente, al momento en la Entidad financiera en su sucursal Guayaquil, La sucursal mayor de Guayaquil ha mantenido un nivel nulo de ataques e incidentes de seguridad registrados hasta el momento pero existe la posibilidad de que en el momento en que tome el lugar de la central de Quito como Matriz dicho índice se incremente ya que en el caso de Quito como matriz si se detectan frecuentemente intentos de ataques cibernéticos a la seguridad de los servidores , tales como ataques de negación de servicios a nuestros portales a través de códigos maliciosos, ataques de INYECCIÓN DE CÓDIGO SQL detección de virus en las redes informáticas, pero hasta ahora dichos ataques se han podido mantener bajo control gracias a la aplicación de ciertas políticas de seguridad gestionadas por el área de Sistemas y que son destinadas a prevenir y mitigar sus posibles efectos.

Ninguna de las dos agencias tanto Quito como Guayaquil cuentan con normativas claras y correctamente difundidas para asegurar la integridad de la infraestructura y de la información.

1.3. Solución propuesta

De acuerdo a lo anteriormente planteado es necesaria la emisión oficial e implementación de normativas y procedimientos para este fin basándose en estándares como el ISO 27001.

Elaborar, implantar y difundir un esquema en el cual se definan las normativas de seguridad informática soportada en procedimientos que ayuden a garantizar la seguridad de la información, recursos informáticos, Servidores críticos y usuarios, haciendo uso de los servicios e infraestructura tecnológica que ofrece la Entidad financiera, basados en el estándar ISO 27001, aplicando los controles necesarios de los dominios de aspectos organizativos de la seguridad de la información, gestión de activos, control de accesos, seguridad física y ambiental y control de las operaciones.

Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos quienes estén interesados y sean responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información; preservando la confidencialidad, integridad y disponibilidad de la misma. Es decir que es un código de buenas prácticas (un documento interno) y no es una

especificación formal, como la norma ISO 27001, lo que hace que se adapte a la necesidades o requerimientos de una organización.

Al hacer uso de esta norma se evaluarán las vulnerabilidades de los activos, a través de una identificación, análisis y tratamiento de riesgos, se identificara los procesos críticos de la empresa, y luego se definirá y aplicarán controles u otras formas para el tratamiento de los mismos.

Servirá como guía para la implementación de controles y de las prácticas más eficaces para gestionar la seguridad de la información. Al final se reforzará con la debida divulgación y capacitación a todo el personal de la Entidad para garantizar su aplicación, seguimiento y eficacia.

Se iniciará por un proceso de levantamiento de la información, revisión de estadísticas y comparación de las mismas entre las dos sucursales, se procederá a coordinar diálogos entre las áreas afectadas por las nuevas normativas, se identificará los respectivos alcances por cada área o departamento, se realizarán visitas físicas en ambas sucursales para poder estandarizar las medidas de seguridad de la información y la seguridad perimetral entre ellas, se evaluara los tiempos de respuesta

en casos de ataques, tanto para el sitio principal como para el sitio alterno.

Una vez se cuente con toda la información requerida se procederá a realizar el respectivo análisis para la actualización y creación de las normativas de seguridad de la información, apegándose a la estandarización de la ISO 27001.

Se iniciará de esta manera con el levantamiento de la información, recopilando los antecedentes requeridos para la identificación del problema o requerimiento de la institución.

Se empieza a definir el marco teórico visualizando objetivos generales y específicos para de esta forma trabajar en las propuestas. Se define la metodología con la cual se va a trabajar, desde el levantamiento de la información requerida, pasando por el proceso de desarrollo del proyecto hasta la implementación del esquema de seguridad.

Se inicia un proceso de culturización y capacitación en el personal en general sobre temas relacionados a seguridad informática preparando al personal para los cambios que están por realizarse y para que se familiaricen con los nuevos estándares a ser aplicados.

Se procede a la implementación de los programas propuestos para salvaguardar la seguridad informática, ANTIVIRUS CORPORATIVO “MCAFEE CORPORATIVO”, SISTEMA DE SEGURIDAD PERIMETRAL “JUNIPER”, SISTEMA DE ESCANEO DE SOFTWARE LOCAL “SNAT”.

Se procede a la implementación de las medidas de seguridad físicas para el centro de datos en la Matriz Guayaquil y en el sitio alterno Quito, así como de las sucursales a nivel nacional.

Se definen lineamientos para el manejo del software especializado y controles para el monitoreo de las seguridades de los centros de datos.
Con la correcta y oportuna implementación del nuevo esquema de Seguridad Informática, se lograra estandarizar medidas preventivas y correctivas en el manejo y cuidado de la información en todos los ámbitos, así como se evitara que dicha información caiga en manos de terceros pudiendo ser usada de manera ilegal, perjudicando a los clientes que mantienen negocios con la entidad financiera, se previene también filtración de información por parte del personal que labora en la entidad financiera quienes podrían hacer mal uso de información privilegiada para favorecer a ciertos inversionistas.

Otro beneficio que se logra con la implementación del esquema de seguridad será el de mantener los servicios en línea brindados por la entidad siempre operativos y seguros.

Las políticas de Seguridad de la Información serán definidas bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento.

Para clasificar un activo de Información, se evaluarán los criterios de confidencialidad, integridad y disponibilidad como se detalla a continuación:

- **Confidencialidad:**

✓ Baja: Información de tipo pública, disponible para todos en general.

✓ Media: Información que puede ser conocida y utilizada por los funcionarios de la Entidad al interior de la misma.

✓ Alta: Información que no puede ser divulgada, es de conocimiento limitado a las personas del manejo de la misma, considerada como reservada o confidencial.

- **Integridad:**

✓ Baja: Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatividad de la Entidad financiera.

✓ Media: Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la Entidad financiera, el Sector Público Nacional o terceros.

✓ Alta: Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas o graves para la entidad o terceros.

- **Disponibilidad:**

✓ Baja: Información cuya inaccesibilidad no afecta la operatividad.

✓ Media: Información cuya inaccesibilidad durante 1 día podría ocasionar pérdidas materiales, de imagen, de valor estratégico de la información, de obligaciones contractuales o públicas, de disposiciones legales, etc. significativas para la Entidad o terceros.

✓ Alta: Información cuya inaccesibilidad durante 4 horas podría ocasionar pérdidas significativas o graves a la Entidad o a terceros.

De esta manera se trabajará en garantizar la completa y segura administración de la información que se maneja en la Entidad Financiera, así como implementar la correcta clasificación y etiquetado de la información la cual solo podrá cambiar el propietario de la misma según los criterios antes mencionados.

1.4. Objetivo General

Implementar un esquema de seguridad Informática para una entidad financiera, con el propósito de mitigar los riesgos informáticos e implementar mecanismos de prevención de ataques cibernéticos a los servidores de la entidad sean estos internos o externos.

1.5. Objetivos Específicos

- Analizar la situación actual del Departamento de Sistemas de la entidad financiera y las políticas actuales para identificar los problemas actuales y posibles vulnerabilidades.

- Verificar los temas correspondientes al marco teórico considerando las necesidades de la entidad, identificación de riesgos, definición de estándares aplicados a la seguridad de la información.

- Identificar los activos de información que administra la entidad, verificación del alcance de las políticas de seguridad informática para con el departamento de sistemas, coordinación entre departamentos en pos de preservar la seguridad, definición de responsabilidades y alcance de las políticas según el área o departamento.

- Diseñar un esquema de seguridad, tomando como base la norma ISO 27001, definiendo las políticas y los procedimientos necesarios para salvaguardar la seguridad física y la integridad de la información.

- Analizar los resultados obtenidos a través de los diferentes sistemas de control con la finalidad de llevar estadísticas que permitan prevenir situaciones de riesgo futuro.

1.6. Alcance

Este esquema se aplica a todos los empleados de la institución Financiera, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o convenios con terceros, en resumen todo aquel que tenga de manera directa o indirecta acceso a la información de la empresa.

1.7. Metodología

Para el desarrollo e implementación del esquema de seguridad, la institución financiera ha tomado como referencia la Norma ISO 27001 adaptando dicha normativa a su realidad operativa.

Se realizará el respectivo levantamiento de información para el desarrollo del nuevo esquema tomando en cuenta la variedad de nuevas amenazas que existen en el nuevo ámbito digital priorizando la protección de la información tratando de no perder agilidad en los procesos.

El Comité de Administración Integral de Riesgos de la Corporación, será responsable de evaluar las políticas de seguridad de la información y someterlas a aprobación del Directorio; proponer al Directorio modificaciones a la Política de Seguridad de la Información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación de incidentes relativos a la seguridad; recomendar la aplicación de las principales iniciativas, estrategias y metodologías para incrementar la seguridad de la información.

Por su lado el área de Informática será responsable de implementar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Corporación Financiera Nacional. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y

que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Seguridad Informática

Es el Área que cumple la función de supervisar el cumplimiento de la presente política y de asesorar en materia de seguridad de la información a los integrantes de la Institución [5].

Parte de seguridad informática comprende la preservación de la información cumpliendo las siguientes características [6]:

- ✓ Confidencialidad: garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- ✓ Integridad: salvaguardar la totalidad y exactitud de la información, así como, los métodos de procesamiento.

- ✓ Disponibilidad: garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, siempre que lo requieran.

Adicionalmente, para la seguridad de la información en sistemas de transferencia electrónica deben considerarse las siguientes características [7]:

- ✓ Autenticación: garantizar el origen de la transacción, validando al emisor para evitar suplantación de identidades.
- ✓ Autorización: asegurar que la transacción sea ejecutada por quién está legalmente facultado.
- ✓ No repudio: garantizar que el uso y/o modificación de la información por parte de un usuario sea irrefutable, es decir, que el usuario no pueda negar dicha acción.
- ✓ Confiabilidad: asegurar que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las funciones.

2.2. Normas y estándares aplicables a la seguridad informática según el ISO 27001

La normativa de las políticas de Seguridad de la Información de la entidad financiera está orientada a cumplir los lineamientos de los

estándares internacionalmente aceptados para la práctica de seguridad de la información tales como [1]:

- ✓ Constitución de la República del Ecuador.
- ✓ Ley de Comercio Electrónico.
- ✓ Ley General de Instituciones del Sistema Financiero, Riesgo Operativo - Tecnológico, Resolución No. JB-2005-834 del octubre 20 del 2005.
- ✓ Ley Institucional de Transparencia y Acceso a la Información.
- ✓ Código de Ética de la entidad.
- ✓ NORMA ISO/IEC 27.001 Sistemas de Gestión de Seguridad de la Información – Requerimientos.

En base a lo antes expuesto, las normas y estándares que se aplicaran en la institución son las siguientes [1]:

2.2.1. Normas y estándares del control de accesos

- ✓ Se entiende por control de accesos, a las políticas y normas emitidas para garantizar que el acceso a los sistemas y servicios de información se realiza en forma ordenada, con una clara definición de roles, sustentada en las funciones y actividades del cargo de los funcionarios.

- ✓ Existen tres actividades ligadas en el control de accesos: la autenticación (quién soy), la autorización (qué puedo hacer) y el registro de auditoria (qué he hecho).
- ✓ Sistemas base.- Es el software que controla el equipo de computación (hardware) y administra los servicios y sus funciones (ejecución de otros programas compatibles con éste).
- ✓ Personal Alterno.- Backup, hace referencia al funcionario que está en la capacidad de asumir las funciones de otro funcionario (principal) cuando este se ausenta.

ESTÁNDARES

1.- Cuentas de usuario de sistemas de información:

- ✓ Nombre de cuenta de usuario: se debe crear la cuenta con letras mayúsculas (siempre que el sistema lo permita), y deberá estar conformado por la primera letra del nombre seguido del apellido paterno, en caso de ya existir otro usuario con este mismo nombre de cuenta, se deberá registrar la primera letra del segundo nombre más el apellido paterno o se podrá hacer combinaciones con las letras de los nombres más el apellido paterno.
- ✓ Cada funcionario tendrá una única cuenta de acceso por sistema requerido.
- ✓ Bloqueo o eliminación lógica, luego de 91 días de no uso.

- ✓ Depuración de perfiles (roles) y cuentas de usuario: al menos cada 12 meses.

2.- Contraseñas:

- ✓ Bloqueo: luego de 3 intentos fallidos.
- ✓ Caducidad de contraseña hasta 60 días.
- ✓ Longitud mínima: 8 caracteres.
- ✓ Contraseña alfanumérica (números y letras).
- ✓ Cierre automático de sesión por inactividad, hasta en 60 minutos.

3.- Carpetas compartidas:

- ✓ Creación de carpetas: en servidor de archivos.
- ✓ Nombre: letras mayúsculas.
- ✓ Tamaño máximo: 1.00 GB.

2.2.2. Normas y estándares de la gestión de activos

Se entiende por Gestión de Activos a las políticas, normas y estándares emitidos para inventariar, clasificar, custodiar y mantener los activos de información en forma adecuada, que garantice su protección en un nivel aceptable, minimizando los

riesgos inherentes a la confidencialidad, reserva, integridad y disponibilidad de los activos de información.

Se deben tomar en cuenta lo siguiente:

- ✓ Responsabilidad sobre los Activos (Inventario y Propiedad).
- ✓ Clasificación de la información (Criterios y Etiquetado).
- ✓ Uso aceptable de los activos.
- ✓ Uso inaceptable de los activos.

ESTÁNDARES

1. Criterios de clasificación de activos:
   a. Confidencialidad.
   b. Integridad.
   c. Disponibilidad.
2. Etiquetado:
   a. Pública.
   b. De uso interno.
   c. Reservada o confidencialidad.
3. Período de actualización: al menos cada 12 meses.
4. Modificación: solo propietario de la información.

5. Correo electrónico:
   a. Dirección e-mail: usuariodered@fin.ec.
   b. El envío de la información desde la cuenta de correo electrónico puede ser externa como interna.
   c. Nombre en Address Book: primer nombre más apellido paterno.
   d. Short Name / UserID: usuario de red.

2.2.3. Normas y estándares de la adquisición, desarrollo y mantenimiento de los sistemas de información

Se entiende por normas de adquisición, desarrollo y mantenimiento de los sistemas de información, al conjunto de normas y lineamientos enmarcados en el ámbito jurídico y administrativo de la Institución, para garantizar que la seguridad está integrada en los sistemas de información, así como, asegurar un tratamiento correcto de las aplicaciones informáticas y sus datos en todo su ciclo de vida, es to encierra los siguientes conceptos:

- ✓ Requisitos de seguridad de los sistemas de información.
- ✓ Tratamiento correcto de las aplicaciones.
- ✓ Controles Criptográficos.
- ✓ Seguridad de los archivos de sistema.

- ✓ Seguridad en los procesos de desarrollo y soporte.

ESTÁNDARES

1. Administración de usuarios y contraseñas:
   a. Creación, mantenimiento, eliminación lógica de usuarios.
   b. Manejo de estados de la cuenta: vigente, bloqueado, eliminado, expirado.
   c. Bloqueo de cuenta por n intentos fallidos parametrizable.
   d. Encriptación de contraseñas.
   e. Cambio de contraseña en forma automática, cada 30 días parametrizables.
   f. Recordar las últimas 6 contraseñas en los sistemas del core del negocio.
2. Administración de roles:
   a. Creación, mantenimiento, eliminación lógica.
   b. Personalización del rol en forma gráfica.
   c. Opciones de menú por defecto: deshabilitadas.
3. Pistas de auditoría: Los sistemas informáticos deben dejar rastro de las acciones realizadas en el mismo.
4. Aplicaciones Web: Permitir el protocolo Secure Socket Layer
5. (SSL).

2.2.4. Normas y estándares de la gestión de comunicaciones y operaciones

Se refiere al control del ciclo de vida de todo cambio en los sistemas de información, el mismo que debe ser llevado a cabo asegurando la continuidad del servicio.

Ambiente de procesamiento de información, se refiere a todos los controles, sistemas, procedimientos, infraestructura (hardware y software) que soporta el procesamiento de información, se debe tomar en cuenta los siguientes parámetros:

- ✓ Responsabilidades y procedimientos de operación.
- ✓ Gestión de la provisión de servicios por terceros.
- ✓ Protección contra código malicioso y descargable.
- ✓ Copias de Seguridad.
- ✓ Gestión de la Seguridad de las Redes.
- ✓ Manipulación de los soportes.
- ✓ Intercambio de Información.

ESTANDARES

1. Periodicidad de revisión de logs:
   a. Acciones realizadas por servidores (personal) de la GDI: al menos cuatrimestral.
   b. Acciones de usuarios finales: al menos semestral.

2. Periodicidad de revisión de existencia de información en pistas de auditoria: al menos semestral.
3. Redes de información:
   a. Separación lógica o física.
   b. Aplicación de mecanismos que garanticen la confidencialidad en el tránsito de la información.
4. Administración y soporte de equipos:
   a. Administración remota de equipos: restringida por IP's/roles al personal de competencia.
   b. Control remoto de equipos: con la autorización explícita del dueño del equipo.
5. Sincronización de relojes en equipos de procesamiento.

2.2.5. Normas y estándares de la gestión de incidentes de seguridad de la información

Se entiende por Gestión de Incidentes a la identificación de los eventos o sucesos relacionados con la vulnerabilidad de la seguridad de la información y el tratamiento para hallar su causa y remediación a fin de evitar que se vuelva a producir.

Vulnerabilidad, es la debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

- ✓Protección contra código malicioso y descargable
- ✓Copias de Seguridad
- ✓Gestión de la Seguridad de las Redes
- ✓Manipulación de los soportes
- ✓Intercambio de Información
- ✓Servicios de Comercio Electrónico

ESTANDARES

Para detectar incidentes de seguridad de la información adicionalmente se revisará:

- ✓ Logs de seguridad.
- ✓ Pistas de auditoria.
- ✓ Alertas en sistemas o herramientas de monitoreo.
- ✓ Análisis de vulnerabilidades.

2.2.6. Normas y estándares de la seguridad de información

Se entiende por Organización de la Seguridad de la Información a las políticas y normas emitidas para garantizar que dentro de la entidad financiera existe una logística humana adecuada para gestionar la seguridad de la información, así como, el asegurar que las responsabilidades frente a la Seguridad de la Información fueran delegadas oportuna y correctamente.

- ✓ Funciones y responsabilidades del Analista de Seguridad de la Información.
- ✓ Funciones y responsabilidades del Encargado de Seguridad del Área de Tecnologías de la Información.
- ✓ Proceso de autorización para los medios de procesamiento de información.
- ✓ Acuerdos de confidencialidad.
- ✓ Revisión Independiente de la Seguridad de la Información.
- ✓ Identificación de riesgos relacionados con entidades externas.
- ✓ Tratamiento de la Seguridad en contratos con terceras personas.

ESTÁNDARES

- ✓ Actividades relativas de seguridad coordinadas con diferentes áreas de la Institución.
- ✓ Propietarios de la información designado por la Gerencia General.
- ✓ Revisiones periódicas independientes.

2.2.7. Normas y estándares de la seguridad de los recursos humanos

Se entiende por Seguridad de los Recursos Humanos a las políticas y normas emitidas para asegurar que los empleados,

contratistas y terceros entiendan sus responsabilidades y que sean adecuados para los roles que se les considera, reduciendo el riesgo de robo, fraude o mal uso de las instalaciones.

Contempla:

- ✓ Funciones y Responsabilidades.
- ✓ Selección.
- ✓ Términos y condiciones laborales.
- ✓ Gestión de Responsabilidades.
- ✓ Capacitación y Educación en Seguridad de la información.
- ✓ Proceso disciplinario.
- ✓ Responsabilidades y Terminación del contrato.
- ✓ Devolución de activos.
- ✓ Eliminación de derechos de acceso.

ESTÁNDARES

- ✓ Comprobar antecedentes de los candidatos a los puestos de trabajo.
- ✓ Cláusulas de seguridad de la información en los contratos elaborados por la institución.
- ✓ Concientización sobre actualizaciones en la Política de Seguridad de la Información.
- ✓ Eliminación de accesos a la información cuando el empleado finaliza su contrato.

2.2.8. Normas y estándares de la seguridad física y del entorno

Se entiende por Seguridad Física y del Entorno al cuidado de la integridad de los equipos, recursos informáticos y áreas de la Institución, de la correcta ubicación de los mismos para asegurar que no sean afectados por variaciones ambientales que podrían causar su mal funcionamiento, accesos físicos no autorizados, de tal forma que se garantice la seguridad de la información en la organización.

Es de mucha importancia tomar en cuenta las situaciones de riesgo para los activos fijos por lo que se trabaja políticas para proteger:

- ✓ Perímetro de seguridad física.
- ✓ Controles de ingreso físico.
- ✓ Seguridad de oficinas, recintos e instalaciones.
- ✓ Protección contra amenazas externas e internas.
- ✓ Trabajo en áreas seguras (Data Centers, cuartos de redes, entre otros).
- ✓ Áreas de carga, despacho y acceso público.
- ✓ Seguridad del equipo.

ESTÁNDARES

Procedimientos de Administración de la Seguridad Física.

2.2.9. Normas y estándares de la gestión de la continuidad del negocio

Se entiende por Gestión de la Continuidad del Negocio a las políticas, normas y procedimientos utilizados para asegurar a la institución ante una situación de emergencia y que pueda reanudar de forma oportuna los sistemas catalogados como críticos, de tal forma que se garantice la operatividad del negocio sin interrupciones.

Comprende normas para:

- ✓ Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
- ✓ Evaluación de riesgo del Plan de Continuidad del Negocio.
- ✓ Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.
- ✓ Estructura para la planificación de la continuidad del negocio.
- ✓ Pruebas, mantenimiento y revisión del Plan de Continuidad del Negocio.

ESTÁNDARES

- ✓ Metodología, estrategias para elaborar y mantener el plan de continuidad del negocio y recuperación de desastres.
- ✓ Análisis de la información.
- ✓ Pruebas del plan de continuidad del negocio:
  1. Simulaciones.
  2. Intentos de restauración.
- ✓ Documentación y preparación de informes.

2.3. Metodología de análisis y gestión de riesgo bajo la normativa ISO 27001

En el marco normativo de los estándares relacionados con la seguridad informática y de la información, está incluida normas específicas para la gestión de seguridad de la información y pueden ser aplicables a cualquier organización, independientemente de su tamaño o actividad.

Para realizar el control de seguridad de la información, el proceso se dividió en etapas sucesivas y sistemáticas; en cada una de ellas se trata de establecer objetivos y metas claras con productos entregables, donde los productos resultado de la primera etapa servirán para adelantar la segunda y los de las segunda servirán para proseguir con la tercera etapa y así sucesivamente, ya que se plantea que el control

debe ser periódico o permanente dependiendo de los cambios en la tecnología de información usada en el tratamiento y procesamiento de la información [2].

Una vez que se han establecido los procesos y se han obtenido los resultados se hace el estudio de las causas que originan los hallazgos. Una vez confirmados, se define los controles apropiados de acuerdo a la norma ISO 27001 se establece su tratamiento, y finalmente, se diseñan las políticas. Confirmados los hallazgos, se establecen los controles de seguridad como políticas y procedimientos de acuerdo a la norma ISO 27001, se definen los más apropiados para mitigar los riesgos y se adaptan para la organización. Luego se determina el tratamiento de los riesgos para aceptarlos o aplicar los controles y posteriormente éstos se integran a las políticas y a los procedimientos institucionales. Al culminar, se elabora el informe final que servirá para el diseño de actividades que ayuden a mantener una mejora continua y fortalecer todos los procesos y servicios dentro de la organización [3].

2.4. Estadística actual de ataques e incidentes registrados

Los datos arrojados por las herramientas de control y de seguridad periférica de la institución han brindado información precisa de los tipos de ataques informáticos más comunes a los que nos enfrentamos en la

región, entres estos ataques tipificados y reconocidos por las principales empresas desarrolladoras de soluciones de seguridad como la empresa JUNIPER tenemos los siguientes [4]:

- ✓ DNS: BIND OPT DoS
- ✓ SSL: Invalid Content Type
- ✓ DNS: Unassigned Opcode
- ✓ DNS: BIND Version Query

Las estadísticas actuales de incidentes registrados al momento en la institución se detallan en la siguiente figura:

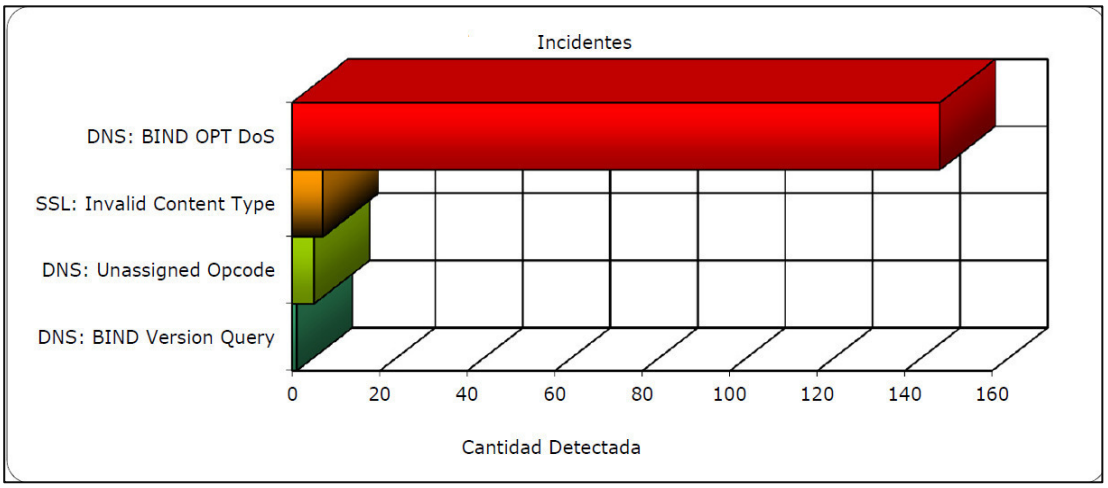

Figura 2.1: Ataques e incidentes registrados ordenados por cantidad
Fuente: Reporte de amenazas de seguridad perimetral emitido en base a las lecturas de los equipos Juniper.

Categoría	Origen	Destino	Hits
DNS: BIND OPT DoS	89.248.168.136	186.46.112.146	11
DNS: BIND OPT DoS	198.206.14.130	186.46.112.146	9
DNS: BIND OPT DoS	80.82.64.231	186.46.112.146	8
DNS: BIND OPT DoS	80.82.64.8	186.46.112.146	8
DNS: BIND OPT DoS	89.248.172.121	186.46.112.146	7
DNS: BIND OPT DoS	94.102.56.234	186.46.112.146	7
DNS: BIND OPT DoS	94.102.49.90	186.46.112.146	6
DNS: BIND OPT DoS	93.174.93.176	186.46.112.146	6
DNS: BIND OPT DoS	78.110.166.164	186.46.112.146	5
DNS: BIND OPT DoS	94.102.52.44	186.46.112.146	5
DNS: BIND OPT DoS	192.198.206.251	186.46.112.146	5
DNS: BIND OPT DoS	94.102.49.221	186.46.112.146	5
DNS: BIND OPT DoS	80.82.65.123	186.46.112.146	5
DNS: BIND OPT DoS	89.248.162.212	186.46.112.146	4
SSL: Invalid Content Type	151.236.13.163	186.46.112.144	4
DNS: BIND OPT DoS	142.0.41.10	186.46.112.146	4
DNS: BIND OPT DoS	94.102.49.37	186.46.112.146	3
DNS: BIND OPT DoS	94.102.56.237	186.46.112.146	3
TOTAL			**105**

Figura 2.2: Relación entre orígenes, destinos y firmas de los incidentes
Fuente: Reporte de amenazas de seguridad perimetral emitido en base a las lecturas de los equipos Juniper.

También se han reportado por parte de los analistas de seguridad informática de la institución falencias en el manejo de la información por parte de las personas designadas, lo cual podría conllevar a fuga de información en algunos casos o perdida de información en otros, por esta razón se necesita actualizar el esquema de seguridad informática con el fin de mejorar y eliminar dichas falencias en la nueva Matriz Guayaquil.

CAPÍTULO 3

ANÁLISIS DEL DEPARTAMENTO DE SISTEMA

3.1. Situación actual

La información brindada por el departamento de seguridad informática de la actual Matriz nos indica que existe un aumento en el número de ataques externos generados hacia los diferentes servidores de la institución los cuales al momento se encuentran protegidos por equipos de seguridad perimetral.

Los ataques externos según el portal de la empresa Juniper son de severidad Crítica, Media y Alta.

La mayoría de ataques registrados va dirigidos al protocolo DNS debido a que las aplicaciones de la Institución son de tipo web y tienen

implementado un certificado digital para asegurar el tráfico de información con el protocolo HTTPS.

Se presenta ataques de tipo DNS hacia el servicio de DNS externo de la Institución, así como también ataques al servicio de correo en la sucursal de Guayaquil, el firewall de Guayaquil ha realizado los bloqueos de los eventos generados en los equipos de seguridad perimetral correctamente y los mismos están siendo reportados mensualmente.

La mayoría de los ataques hacia el protocolo de DNS es de tipo BIND que es el servicio más común usado en Internet, a pesar que dicho aumento puede deberse a las pruebas de vulnerabilidad que realiza el proveedor de Servicios de Seguridad informática como parte del contrato establecido.

Las direcciones IPS públicas responsables de la mayoría de estos ataques en los equipos de seguridad perimetral pertenecen a países como EEUU, Holanda, Rep. Checa y Ecuador según la herramienta online Netwoork-Tools.

Al momento y gracias a las políticas de seguridad implementados en la matriz Quito, dichos ataques no han ocasionado problemas en la

disponibilidad de nuestros servicios a clientes. No se ha reportado ningún incidente en los equipos internos sean estaciones de trabajo o servidores mencionados en el reporte.

Este análisis hace necesario la implementación del mismo esquema de seguridad o una versión mejorada en la sucursal mayor de Guayaquil la cual será la nueva matriz.

3.2. Identificación de activos de información

Los responsables de los activos de información (propietario de la información) serán designados por la Gerencia General, los mismos que podrán delegar y/o revocar sus actividades. Los activos de información y sus designados están descritos en la Tabla 1:

Tabla 1: Descripción de los activos de información

Fuente: Gerencia de División de Informática

ACTIVOS DE INFORMACIÓN Y SUS DESIGNADOS		
COBIS: Manejo de información de crédito y contable		
ACTIVO DE INFORMACIÓN	**UNIDAD**	**UNIDAD SUC. MAYOR**
ADMINISTRACIÓN CRÉDITO 1ER PISO, GESTIÓN, EXPEDIENTES Y TRÁMITES	GERENTE GENERAL DE CRÉDITO DE PRIMER PISO	SUPERVISOR DE CREDITO DE PRIMER PISO
ADMINISTRACIÓN CRÉDITO 2DO PISO, GESTIÓN Y TRÁMITES	GERENTE GENERAL DE CREDITO DE SEGUNDO PISO	SUPERVISOR DE CREDITO DE SEGUNDO PISO
CARTERA, INFORMES, COBRANZAS	GERENTE GENERAL DE CARTERA	SUPERVISOR REGIONAL DE CARTERA
CONTABILIDAD	GERENTE GENERAL DE CONTABILIDAD	SUPERVISOR DE CONTABILIDAD
CENTRAL DE RIESGOS	GERENTE DE CALIFICACIÓN DE RIESGOS	EJECUTIVOS DE CALIFICACION DE RIESGOS
ADMIN UNICO	GERENCIA DE DIVISIÓN INFORMÁTICA	SUBGERENCIA REGIONAL DE SOPORTE TÉCNICO DE INFORMATICA

Tabla 2: Módulos adquiridos del sistema gerencial PCIE

Fuente: Gerencia de División de Informática

PCIE (Módulos adquiridos del sistema gerencial PCIE)		
MODULO	**UNIDAD**	**UNIDAD SUC. MAYOR**
PCIE ADMINISTRATIVO PCIE CLASIFICACIÓN Y VALORACIÓN	SUBGERENTE NACIONAL DE REC. HUMANOS	SUBGERENTE REG. DE RECURSOS HUMANOS
PCIE ADMINISTRATIVO 5 (CONTROL Y PAGADURÍA)	SUBGERENCIA NAL. DE CONTROL Y PAGADURÍA	SUBGERENTE REGIONAL DE CONTROL Y PAGADURÍA
PCIE CORPORATIVO 5	SUBGERENTE NACIONAL DE CARTERA	SUBGERENTE REG. DE CARTERA
PCIE FINANCIERO 5	SUBGERENTE REG. DE CONTABILIDAD	SUBGERENTE NACIONAL DE CONTABILIDAD
PCIE FINANCIERO 6	SUBGERENTE REG. DE TESORERÍA Y ADM. DE RECURSOS	SUBGERENTE NACIONAL DE TESORERÍA
PCIE PRESUPUESTO	SUBGERENTE NACIONAL DE PRESUPUESTO Y CONTROL	GERENTE REGIONAL DE FINANZAS Y ADM. CREDITO

PCIE (Módulos adquiridos del sistema gerencial PCIE)		
MODULO	**UNIDAD**	**UNIDAD SUC. MAYOR**
PCIE RIESGOS	SUBGERENTE NACIONAL DE CALIFICACIÓN DE RIESGOS	GERENTE NACIONAL DE RIESGOS
PCIE ADMINISTRATIVO V12 VIÁTICOS	SUBGERENTE NAL. DE SERVICIOS GENERALES	SUBGERENCIA REGIONAL DE SERVICIOS GENERALES Y ADM. DE BIENES.
PCIE ADMINISTRATIVO V5 – MATERIALES Y SUMINISTROS – GASTOS ADMINISTRATIVOS.	SUBGENTE NAL. DE ADMINISTRACIÓN DE BIENES	SUBGERENTE REGIONAL DE SERVICIOS GENERALES Y ADMIN. DE BIENES
OTROS		
ACTIVO DE INFORMACIÓN	**UNIDAD**	**UNIDAD SUC. MAYOR**
RED, CORREO ELECTRÓNICO, HP SERVICE MANAGER, INTRANET, QLICKVIEW	GERENTE DE DIVISIÓN DE INFORMATICA	SUBGERENTE REG. DE SOPORTE TECNICO DE INFORMATICA

PCIE (Módulos adquiridos del sistema gerencial PCIE)		
MODULO	**UNIDAD**	**UNIDAD SUC. MAYOR**
SITIO WEB, REDES SOCIALES INSTITUCIONAL	GERENTE DE MERCADEO Y PROMOCIÓN	EJECUTIVOS DE MERCADEO Y PROMOCIÓN
SISTEMA IDENTITY MANAGER	GERENCIA DE DIVISIÓN INFORMÁTICA	N/A
INVESTIGACIÓN, DISEÑO DE PRODUCTOS	JEFE DE SUPERVISIÓN DEL PROCESO DE INVETSIGACIÓN Y DESARROLLO	N/A
AUDITORIA INTERNA	AUDITOR INTERNO	N/A
SISTEMA DE GESTIÓN DE RIESGO OPERATIVO	GERENTE DE CALIFICACIÓN DE RIESGOS	EJECUTIVO DE RIESGOS

3.3. Definición de amenazas

Las amenazas son las situaciones que desencadenan en un incidente en la empresa, causando como consecuencia un daño material o pérdidas inmateriales de sus activos de información.

Las normas de referencia nos permiten la identificación de riesgos de seguridad de la información, tomando como base los procesos cubiertos por el Sistema de Gestión de Seguridad de la Información de la institución, para poder identificar las fuentes de riesgo, vulnerabilidades y las posibles consecuencias con sus efectos o nivel de impacto para la entidad.

Una vez que hemos identificado los riesgos podemos presentar las opciones para el Plan de Tratamiento con base en el estándar ISO27001.

En base a lo anteriormente detallado se ha procedido a identificar los riesgos que enfrentan los activos de información de la institución en un trabajo conjunto del departamento de Sistemas, analistas de seguridad informática y demás personal técnico involucrados en el manejo de los activos de información se procedió a identificar los posibles riesgos y amenazas que enfrenta la institución, una vez identificados los riesgos se podrán definir con mayor efectividad las políticas y procedimientos de seguridad de la información con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la institución:

- ✓ Amenaza de Vulnerabilidad técnica.
- ✓ Amenaza de código malicioso y descargable en aplicaciones.
- ✓ Amenaza de Fuga de Información.
- ✓ Amenazas a la infraestructura de redes.
- ✓ Amenazas de ataques perimetrales, externas e internas.

3.4. Análisis y valoración de riesgo

Se entiende por evaluación de riesgos al análisis de las amenazas y vulnerabilidades relativas a la información, a las instalaciones de procesamiento (centro de cómputo) y estaciones de trabajo la probabilidad de que ocurran y su potencial impacto en la operatividad de la entidad.

Tabla 3: Realización de análisis y valoración de riesgo

AMENAZA	ACTIVO AFECTADO	PROBABILIDAD DE OCURRENCIA	VULNERABILIDAD	POSIBLE EXPLOTACION DE VULNERABILIDAD	VALOR DE ACTIVO	POSIBLE OCURRENCIA	TOTAL
Vulnerabilidad técnica	Estaciones personales, Servidores, Información	Medio	- Mala Practica en mantenimientos físicos. - Manipulación de equipos por personal inexperto.	Alto Medio	Alto	Medio	Medio
Código malicioso y descargable en aplicaciones	Estaciones personales, Información	Alta	- Mal uso del internet por parte de empleados. - Correos electrónicos no seguros.	Alto Alto	Alto	Alto	Alto
Fuga de Información	Información	Alta	- Robo de información por parte de empleados internos o separados de la institución. - Robo de información por parte de personas externas vía remota (Pishing).	Medio Medio	Alto	Bajo	Medio
Infraestructura de redes	Servidores, Switches, Información.	Medio	- Falta de seguridad física en data center. - Falta de seguridad en estaciones de trabajo por parte de usuarios.	Alto Alto	Alto	Medio	Medio
Ataques perimetrales, externas e internas	Servidores, Estaciones personales, Switches, Información	Alta	- Ataques remotos por parte de personas externas con software especializado. - Falta de actualización de software de control perimetral (Equipos Juniper).	Medio Medio	Medio	Bajo	Medio

3.5. Tratamiento de riesgo

Alineándonos con la normativa ISO 27001, los objetivos de control se basan en resultados y conclusiones de los procesos dedicados a medir el riesgo y los procesos para el tratamiento de dichos riesgos tales como las obligaciones de contratos y requerimientos comerciales de la institución para la seguridad de la información.

Por lo antes descrito es necesario la existencia de unos factores y condiciones que garanticen el éxito tales como: el apoyo incondicional por parte de la dirección general, la alineación de los objetivos de seguridad con los objetivos de la Institución, la compatibilidad de los controles con la cultura organizacional, el conocimiento de los requerimientos de seguridad, el conocimiento de la administración de los riesgos, los canales de comunicación con los empleados para dar a conocer los aspectos de seguridad, la disposición de las políticas y procedimientos de seguridad, y los mecanismos para la medición de efectividad del programa de seguridad de la información, las políticas, los controles y planes para el tratamiento del riesgo, con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de la misma, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

CAPÍTULO 4

DISEÑO

4.1. Selección de controles basados en la Norma ISO 27001

Se detallan los controles de la seguridad de la información de acuerdo a las necesidades de la Institución:

- ✓ Responsabilidades del Usuario.
- ✓ Control de Accesos a la Red y Sistemas Operativos.
- ✓ Control de Acceso a las aplicaciones y a la información.
- ✓ Monitoreo de Accesos.
- ✓ Control para acceso de computadores Portátiles y de Escritorio.
- ✓ Control de Redes Inalámbricas.
- ✓ Control para Trabajo remoto.

4.2. Definición de la Política de seguridad

Se entiende por Política de Seguridad de la Información, al conjunto de reglas obligatorias que deben observar todos los funcionarios de la Institución, siendo responsabilidad de la Gerencia General, a través de la función de Seguridad Informática, vigilar su estricta observancia en el ámbito nacional.

La Institución al ser una entidad financiera, que genera, utiliza, procesa, comparte y almacena información en medio electrónico o escrito, clasificada como confidencial, reservada y no reservada, deberá aplicar el Esquema de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que se requiera, tomando las medidas preventivas y correctivas para que se cumpla con la planificación y la mejora continua del Sistema de Gestión de la Calidad, a fin de:

- ✓ Proteger la inversión de la infraestructura tecnológica y sistemas de información.
- ✓ Asegurar la información contenida en los sistemas.
- ✓ Reducir los riesgos tecnológicos, legales y comerciales de la Institución.
- ✓ Proteger el buen nombre de la institución.

4.2.1. Importancia

La información es un recurso que, como el resto de los activos, tiene valor importante y estratégico para la entidad y por consiguiente debe ser debidamente protegida.

Las Políticas y Procedimientos de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Corporación.

4.2.2. Objetivos Específicos

Proteger los recursos de información de la y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información, así como, contribuir a la continuidad del negocio.

Asegurar la consecución de los objetivos de seguridad contemplados en esta Política mediante la implementación de un Sistema de Gestión de Seguridad de la Información.

Mantener la Política de Seguridad de la Información de la Institución actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

4.2.3. Alcance

Esta Política se aplica en todo el ámbito de la Institución, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o convenios con terceros.

4.2.4. Principios

a. Las políticas de Seguridad de la Información serán definidas bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento.

b. Las políticas, procedimientos y normas de seguridad serán elaboradas, revisadas y evaluadas periódicamente; en especial, ante cambios significativos en la tecnología de información institucional o procesos que puedan afectar la base original de evaluación de riesgos.

4.2.5. Niveles de Revisión y Aprobación

a. El Comité de Gestión de la Seguridad de la Información (CSI) deberá evaluar las políticas, normas y procedimientos recomendadas por el Área de Seguridad Informática, y proponer su aprobación a las instancias competentes.
b. La Gerencia General aprobará los procedimientos y normas de Seguridad de la Información.
c. El Directorio de la Institución aprobará las políticas de Seguridad de la Información.

4.3. Definición de los Procedimientos mitigación de riesgos

4.3.1. Responsabilidades del Usuario

a. El usuario de los recursos informáticos es responsable por el uso que dé a su cuenta, está obligado a mantener la

confidencialidad y reserva de su contraseña y a cambiarla periódicamente.

b. Los usuarios de las diferentes aplicaciones y de la red serán los únicos responsables del ingreso, actualización y calidad de los datos, controlados por las aplicaciones informáticas en producción.

c. Todas las transacciones en los sistemas de información realizados con una cuenta de usuario y contraseña, son de responsabilidad del usuario propietario de la cuenta.

d. La contraseña inicial otorgada por el Departamento Nacional de Seguridad Informática, deberá ser cambiada inmediatamente por una contraseña personalizada por el usuario. Las contraseñas caducarán en 30 días.

e. Las contraseñas son de uso personal e intransferible en todo momento; manejadas por el funcionario como información confidencial, en caso de compartir o divulgar las claves se considerará como falta grave.

f. Los usuarios de los recursos informáticos deberán utilizar contraseñas fuertes, que no puedan ser violentadas por otros. Se recomienda que al especificar una contraseña deba:
   - ✓ Tener una longitud mínima de 8 caracteres.
   - ✓ Ser una combinación de dígitos, letras y caracteres especiales, si el sistema lo permite.
   - ✓ No ser una palabra o combinación de palabras comunes, sean estas del idioma español o de otros idiomas.
   - ✓ No estar relacionada con nombres de familiares, ciudad o fecha de nacimiento, número de cédula, números de cuentas bancarias, etc.
   - ✓ No seguir una secuencia de teclado.

g. Es responsabilidad del usuario si considera que su clave ha perdido confidencialidad, cambiar su contraseña o solicitar al área de Seguridad Informática la asignación de una nueva clave.

h. Las contraseñas no deberán ser escritas o registradas en documentos o lugares donde puedan ser observadas por otras personas.

i. Una vez concluida la jornada laboral, es obligación de los usuarios apagar su computadora y equipos informáticos a su cargo.

j. El ambiente de escritorio de las computadoras deberá estar estandarizado con un solo papel tapiz y protector de pantalla, en los que constará el logo de la Institución.

k. El usuario está prohibido de cambiar cualquier tipo de configuración de la computadora.

l. Las aplicaciones y/o utilitarios deben ser utilizados solo por los usuarios autorizados y para realizar funciones inherentes a su cargo.

m. El usuario deberá asegurarse de respaldar frecuentemente la información considerada como crítica para el cumplimiento de sus labores y garantizar la supervivencia de la misma, por la cual responde ante la institución. Dichos respaldos y copias de seguridad deberán ser efectuados con el mecanismo y procedimiento que defina la Gerencia de División Informática,

para lo cual esta Gerencia deberá tomar en cuenta la disponibilidad de la información, tanto en las oficinas locales como en el sitio alterno definido en el Plan de Continuidad del Negocio.

n. La información considerada como crítica será la definida por el Plan de Continuidad del Negocio y la Clasificación de la Información, deberá estar estrictamente relacionada con las tareas institucionales asignadas al usuario. Los usuarios están expresamente prohibidos de colocar información que no tenga que ver con el trabajo y/o respaldarla en cualquier medio de almacenamiento. En particular, cualquier tipo de información multimedios como audio (formato mp3, wav, y otros), imágenes (formatos jpg, bmp y otros) y video (formato avi, mpg y otros), no debe ser respaldada.

o. Todo usuario de los servicios informáticos, deberá suscribir el Acta de Usuario RPRH-15 - Acuerdo de Confidencialidad y reserva de la Información (Ver Anexo 2).

p. Se podrá bloquear automáticamente la sesión de red del usuario del equipo si se detecta inactividad durante un lapso de hasta 10 minutos, y se desbloqueará únicamente si el usuario ingresa nuevamente su clave.

q. La Institución adoptará la política de escritorios y pantallas limpias para los documentos, medios de almacenamientos removibles y para los medios de procesamiento de la información, se deberá considerar las siguientes directrices para el cumplimiento de esta política:

   - ✓ El Departamento de Seguridad Informática a través del analista de Seguridad de la Información revisará de acuerdo a la planificación operativa del área el contenido de las pantallas de los equipos, con el fin de que no se encuentren íconos y accesos innecesarios; carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.
   - ✓ Para proteger la información de accesos no autorizados, los funcionarios deben retirar información sensible de copiadoras, impresoras, fax, entre otros, así mismo no deben tener claves pegadas en sus escritorios y/o pantallas.

- ✓ Cada funcionario es responsable de retirar los dispositivos removibles una vez que se hayan dejado de utilizar.

r. Es responsabilidad del Superior Jerárquico notificar a la Gerencia de División de Informática y al Departamento Nacional de Seguridad Informática cuando el personal a su cargo haga uso de sus vacaciones y solicitar vía correo electrónico la inhabilitación de los accesos otorgados, así como indicar el nombre de su backup para proceder a la habilitación temporal de los roles necesarios.

s. Es responsabilidad del usuario activar en su correo institucional la opción “Ausente de la Oficina” con la finalidad de mantener informados al resto de usuarios que requieran comunicarse por esta vía.

4.3.2. Control de Accesos a la Red y Sistemas Operativos

a. El uso de la infraestructura y servicios de red por parte de los usuarios informáticos, deberá ser consecuente con los propósitos de la institución.

b. El usuario deberá utilizar la infraestructura de red para el intercambio de información, cuyo contenido únicamente sea laboral.

c. El usuario deberá utilizar eficientemente la red, con el fin de evitar en la medida de lo posible la congestión y degradación de los servicios asociados o que dependen de la infraestructura de red.

d. Todo usuario al encender o reiniciar su computador deberá ingresar a la red con su cuenta de usuario y contraseña asignadas, no en modo estación de trabajo.

Se considerará falta grave:

- ✓ Instalar software no licenciado o no autorizado por la Gerencia de División Informática.
- ✓ Cambiar las configuraciones estándar de los equipos de procesamiento.
- ✓ Obtener la información de los sistemas de la institución para uso y provecho personal.
- ✓ Ejecutar programas de escaneo de puertos TCP/UDP, uso de técnicas de enumeración, obtención de información interna de la configuración de la red, ataques de negación de servicio (DoS), obtención de contraseñas vía ataques de fuerza bruta, entre otros.

e. En el caso de requerir la creación de una carpeta compartida en equipos centralizados, el área requirente deberá solicitar mediante correo electrónico u otra vía al Departamento de Seguridad Informática solicitando el servicio.

f. El Departamento de Seguridad Informática podrá supervisar el tráfico de la red y el uso del servicio de todos los usuarios con

el propósito de verificar su apropiado uso, operación correcta del sistema o distribución justa de los recursos de red.

g. La Departamento de sistemas deberá asegurar y mantener los sistemas operativos actualizados con los últimos parches de seguridad tanto en los PC como en servidores, de acuerdo a los estándares definidos.

h. El Departamento de Seguridad Informática y el Departamento de sistemas podrán usar los programas necesarios para proteger a la Institución contra software malicioso, como antivirus, anti-spyware, anti-phishing y otros.

i. Es responsabilidad del Departamento de sistemas mantener actualizado y estandarizado las herramientas y utilitarios informáticos, incluyendo el antivirus.

j. Únicamente la Departamento de sistemas podrá usar programas de tipo firewall en los PC o servidores de la institución.

k. Todas las estaciones de trabajo deberán disponer de un firewall local activo con el fin de evitar ataques, intrusiones y aplicaciones maliciosas que intenten establecer conexiones remotas.

l. Se otorgará acceso al Internet a todos los funcionarios de la Institución con contrato fijo, contrato de servicios ocasionales, honorarios profesionales o en comisión de servicios, pasantes o terceros.

m. Durante el horario habitual de labores y fuera del horario de trabajo, el acceso a Internet será únicamente con fines laborales relacionados con la Institución.

4.3.3. Monitoreo de Accesos

a. El Departamento de Seguridad Informática evaluará en forma permanente el uso adecuado de las cuentas de usuario, contraseñas, roles/perfiles y otros recursos informáticos asignados.

b. El Departamento de Seguridad Informática, realizará revisiones periódicas a la configuración de las computadoras, equipos del centro de cómputo y seguridad perimetral para evaluar la correcta aplicación de las políticas.

4.3.4. Control de Redes Inalámbricas

a. Acceso inalámbrico será accesible solo para empleados de la Institución que cumplan con los siguientes requisitos:
   - ✓ El dispositivo autorizado para esta conexión son computadores portátiles institucionales.
   - ✓ Acceso por dirección física (MAC).
   - ✓ Se habilitarán servicios de acceso a la red LAN e Internet.
   - ✓ Los funcionarios mantendrán los mismos accesos que poseen en la red LAN.

b. No se permitirá acceso de equipos de invitados a la red inalámbrica por atentar contra la seguridad de nuestras redes internas.

c. El servicio para dispositivos móviles (teléfonos inteligentes y tablets) será de uso exclusivo de Gerentes, Subgerentes y Asesores autorizados por el Gerente General.
   - ✓ Se permite el acceso de dispositivos móviles personales.
   - ✓ Acceso por dirección física (MAC).
   - ✓ Se permitirá el acceso a la red LAN de institución para los servicios de Internet, correo electrónico institucional, sistema de video conferencia y/o comunicaciones unificadas.
   - ✓ Servicio de Internet controlado.

4.3.5. Trabajo remoto

a. La Gerencia de División de Informática autorizará el uso del servicio de "conexión remota" únicamente al personal técnico de su área y del Departamento Nacional de Seguridad Informática. Por requerimientos excepcionales, el Departamento Nacional de Seguridad Informática será quien autorice el uso de este servicio a funcionarios independientes a estas áreas, previa justificación otorgada por el respectivo superior jerárquico.

b. El funcionario deberá observar la seguridad física de la edificación y del entorno local existente en el sitio de trabajo remoto, protegiéndolo contra cualquier contingencia o accidente.

c. Cada funcionario es responsable de evitar la conexión remota a través de redes inalámbricas desconocidas/expuestas, que no presten la seguridad de acceso y autenticación adecuada.

d. En todo trabajo remoto deberá aplicarse la confidencialidad de la información que se conserva, los sistemas y servicios internos para los cuales está autorizado.

e. El usuario al establecer una conexión remota, será el responsable de considerar la protección de antivirus con el fin de evitar ataques e intrusiones.

f. Es responsabilidad del usuario que realiza el trabajo remoto el correcto uso de este servicio.

4.4. Difusión de la Política

La Política de Seguridad debe ser parte de la cultura organizacional, es por ello que existe el compromiso manifiesto de las máximas Autoridades y de los Gerentes, Subgerentes, Jefes y Designados de las Áreas para la difusión, capacitación, consolidación y cumplimiento de la presente Política.

La etapa de difusión consiste en propagar, divulgar y difundir las políticas de seguridad informática, así como sus objetivos, metas y beneficios con el fin de crear conciencia en todo el personal de la organización acerca de lo importante que es que se sigan y se respeten aun cuando el personal no se encuentre dentro de la organización.

Los resultados y la efectividad dependen en gran manera de la participación y capacitación adecuada de todo el personal que conforma la organización ya que en la manera en que cada individuo entienda la importancia de la información que le fue confiada para la realización de su trabajo, así como la propia, estará directamente relacionada con el nivel de seguridad, es decir, entre mejor capacitación y participación del personal haya, el nivel de seguridad será mucho más alto.

En nuestro caso la institución ha optado por tres mecanismos de difusión del esquema actualizado para la nueva sucursal en Guayaquil, y para toda la institución en general:

Publicidad interna

Se hará uso de publicidad que contenga información concreta acerca de las políticas de seguridad actualizadas, esta información puede ser difundida a través de correos electrónicos, publicada en la página web de la institución, el mail o publicidad en la página web debe contener un comunicado resumido de las políticas de seguridad, así como alguna ilustración acorde con el tema que pueda dar una idea y atrape la atención del usuario.

Boletines diarios

Los boletines diarios se enviaran a todas las estaciones de trabajo a manera de pantallazos donde se recordara las políticas más importantes para el manejo correcto de la información y de los equipos asignados a cada usuario, así como recalcar la importancia del cumplimiento de las mismas, de la misma manera se procederá a realizar publicaciones sobre estos temas en áreas comunes dentro de la institución, Este tipo de publicidad debe ser puesta en lugares donde

exista una gran afluencia de usuarios, es decir, en lugares donde exista un tránsito abundante o en lugares establecidos para la difusión de otro tipo de publicidad donde normalmente los usuarios acudan en busca de información de algún otro tipo.

Talleres de capacitación al personal

Es necesario que en cualquier organización exista una capacitación la cual depende en gran parte de que exista un programa de difusión que tenga el objetivo de acercar al usuario a las políticas de seguridad informática, el usuario Bien capacitado tiene una clara idea de lo importante que es la información. Sabe cómo proteger los activos o bienes tanto propios como los que la Institución.

Para este fin se contará con la ayuda de los analistas de seguridad informática quienes se encargaran de dar charlas informativas, talleres, y reuniones con el personal de los distintos departamentos de la institución para poder explicar de manera más específica y dependiendo del área o cargo del usuario las políticas que serían la más importantes para cada caso.

Figura 4.1: Ejemplos de boletines
Fuente: Departamento de Seguridad Informática de la institución.

CAPÍTULO 5

IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD

5.1. Instalación e implementación de software especializado

Para el correcto monitoreo y prevención de ataques que puedan dañar severamente los equipos, servidores, o que puedan causar perdida de información crítica para la Institución, se ha realizado evaluación de méritos de varios proveedores tanto locales como extranjeros para la instalación de equipos y software especializado para la protección de los sistemas, hardware e información de la compañía.

De todas las propuestas se escogieron los siguientes por ser los que mejor equilibrio mostraban entre precio, funcionalidad y experiencia.

5.1.1. Equipos y software para seguridad perimetral

Equipos Marca JUNIPER una de las más conocidas en el mercado de la seguridad Informática, el contrato contempla informes mensuales emitidos por la herramienta y acceso a la consola que el fabricante pone a disposición de sus clientes para monitorizar en tiempo real los accesos y cantidad de requisiciones a servidores de la institución, al ser el proveedor personal de habla inglesa los Analistas de seguridad informática serán los encargados de traducir y elaborar un nuevo informe basado en el informe original emitido por el proveedor, destacando los puntos de mayor relevancia y explicando las posibles causas de dichos resultados.

5.1.2. Antivirus Corporativo McAfee

Antivirus corporativo que ofrece protección y actualización constante, ofrece protección de antivirus para el mail corporativo.

Emite alarmas cada vez que detecta una descarga que contiene algún material peligroso que pueda dañar la integridad de los equipos o información así mismo brinda protección web para las páginas de la institución.

5.1.3. Software de Monitoreo de red SNAT

Software que permite a los analistas de seguridad informática, monitorear lo que los usuarios ven en sus pantallas, así como también graba logs de los accesos a los equipos, y actividades diarias, también controla el tráfico de red permitiendo definir anchos de banda personalizados por áreas y usuarios, permite visualizar el software instalado en todo los equipos de computación, ayuda en el control y prevención de ataques provenientes de fuentes internas de la institución, casos como el de empleados despedidos que pueden intentar llevarse información.

5.2. Pruebas y control de calidad del Software Especializado

De manera periódica mensual, el departamento de seguridad informática, a través de sus analistas de seguridad informática, realizaran pruebas y simulaciones que ayuden a comprobar el buen desempeño de los programas especializados de control, adicional a estas pruebas, los proveedores de los equipos JUNIPER, así como los proveedores del antivirus corporativo McAfee, estipulan dentro de los contratos celebrados con la institución pruebas periódicas y reportes mensuales con el análisis y recomendaciones derivadas de dichas pruebas, así mismo incluye dichos contratos las actualizaciones

periódicas necesarias para mantener los productos contratados con ellos en óptimo funcionamiento.

5.3. Estandarización de reportes

La institución tomando en cuenta el esquema de Seguridad Informática para la nueva matriz ha implementado y estandarizado reportes que facilitaran el análisis de los resultados de las herramientas de control, con la ayuda de dichos reportes será más fácil poder tomar decisiones que ayuden a mejorar el control y proteger más eficientemente los Activos informáticos de la Institución.

A continuación se presenta los 3 tipos de reportes periódicos que los analistas de seguridad informática revisaran como producto de nuestras herramientas de control, protección y monitoreo.

5.3.1. Informe equipo Juniper seguridad perimetral (Anexo 3)

Informe emitido basado en el reporte del proveedor internacional que nos brinda el servicio de seguridad perimetral para protección de los activos informáticos de la institución, tales como servidores hosts de nuestros servicios en línea, servidores

de respaldo, el informe es realizado por el analista de seguridad informática encargado y es entregado a la Gerencia de Riesgos.

5.3.2. Informe de revisión y monitoreo de logs para sistema COBIS (Anexo 4)

El sistema COBIS es el sistema de administración gerencial y financiera, al contener información crítica de la Institución debe ser monitoreado constantemente y se debe mantener el control de los usuarios que accedan al sistema y que requerimientos solicitaron del mismo, para este fin se emite el informe de los accesos y actividades (LOGS) de los usuarios durante el mes que han ingresado al sistema COBIS.

5.3.3. Informe de gestión de incidentes de seguridad de información (Anexo 5)

Basados en todos los reportes e informes de las herramientas de control con los que dispone la institución, se procede una vez al mes a emitir el informe de gestión de incidentes de seguridad de la información, donde se incluyen eventos detectados por el sistema de monitoreo de red SNAT y eventos detectados por el antivirus corporativo McAfee, en caso de haber existido, se

incluye los detalles de los mismos, así como las acciones tomadas para corregir, mitigar o restaurar las consecuencias de dichos eventos, y se incluye también las recomendaciones para evitar que dichos eventos vuelvan a suceder.

5.4. Controles de seguridad de los centros de datos

5.4.1. Objetivo

Salvaguardar la integridad física del personar ya sea externo o interno que se encuentren realizando laborando dentro del centro de cómputo al momento de presentarse una situación de emergencia.

Para este fin, el departamento de sistemas en conjunto con el departamento de Seguridad Informática, realizaran visitas periódicas mensuales a las agencias de Guayaquil y Quito, en dichas visitas se revisara el cumplimiento de las políticas de seguridad tanto en las estaciones de trabajo como en los centros de datos y se emitirá el informe correspondiente con las novedades encontradas en la revisión de los equipos (Anexo 6) y se adjuntará el registro de la revisión de los accesos al centro de Cómputo (Ver Anexo 7).

5.4.2. Alcance

Procedimiento a realizar en caso de siniestro y situaciones de emergencia al interior del centro de cómputo, las áreas implicadas en esta fase serian:

- ✓ Gerencia de División de Riesgos.
- ✓ Departamento de Seguridad de la Información.
- ✓ Subgerencia de Recursos Humanos.
- ✓ Superiores jerárquicos.
- ✓ Servidores de la Institución.

5.4.3. Medidas de seguridad emergencias al interior del Data Center

- ✓ El personal Interno o externo que se encuentre en el interior del centro de cómputo deberá informar al Administrador inmediatamente en caso de presenciar alguna anomalía en las conexiones eléctricas que puedan causar cortes de energía o corto circuitos que atenten contra la integridad física de los equipos y personas dentro del Data Center.

- ✓ En caso de que un incendio este en su fase de inicio y de encontrarse personal ya sea externo o interno de la institución dentro del centro de cómputo, estos deberán dar la voz de

alarma, y el administrador del Data center procederá a activar la alarma manualmente en caso de que la misma no se haya disparado de manera automática a través del sistema de detección y extinción de incendios.

- ✓ En caso de que una vez iniciado el siniestro y personal haya quedado atrapado dentro del área del centro de cómputo, estos deberán activar inmediatamente la alarma para que personal que se encuentre fuera del área pueda ayudar a la evacuación para esto pueden ayudarse con el extintor de CO2 que se encuentra en la parte exterior del centro de cómputo cercano a la puerta de ingreso, la evacuación debe hacerse previniendo de preferencia que no quede personal dentro del área al momento de la activación automática del sistema dispensador del extintor fijo FM -200 instalado dentro del data center.

- ✓ Se recomienda al personal en el interior del centro de cómputo que no se exponga a peligros mayores debiendo desalojar el área de manera ordenada y guiándose por las señalética de seguridad las cuales se han recomendado aumentar e instalar

para que quede de manera visible en toda el área del data center.

5.4.4. Procedimiento para el uso de extintores de CO2

- ✓ En caso de extintores de CO2 estos se diferencian de los demás por contar de una corneta color negro al final de la manguera dispensadora del producto.

- ✓ Tomar el Extintor y retirar la bincha de seguridad de la manija para poder disparar el compuesto de CO2.

- ✓ Antes de usar el extintor se debe primero GOLPEAR LEVEMENTE la base del extintor contra una superficie plana para asegurar su correcto funcionamiento.

- ✓ Agitar la corneta del extintor haciendo movimientos uniformes sobre el área en llamas.

5.4.5. Procedimiento para la activación del extintor fijo FM-200

- ✓ El extintor fijo de gas ecológico FM-200 forma parte del sistema automático de detección y extinción de incendios, por lo cual este va conectado a los dos detectores de humo existentes en el área los cuales disparan el gas a través de un dispensador ubicado en la parte central del techo al momento de detectar humo dentro del data center.

- ✓ En caso de no activarse automáticamente por fallas en los detectores de humo se puede activar el mismo de manera manual, retirando la bincha de seguridad y desplazando la palanca de activación en dirección hacia uno mismo y hacia abajo tal como lo indica la señalética del extintor, al realizar este procedimiento se disparara automáticamente una señal de alarma seguida de la liberación del producto de contención en toda el área del centro de cómputo.

- ✓ Al tratarse de gas Ecológico el producto no resulta toxico y puede ser utilizado en casos de que se encuentre personal atrapado dentro del data center.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1. Evaluación de estadísticas

La implementación del nuevo esquema de seguridad Informática para la nueva matriz Guayaquil permite que unto con los controles periódicos a través de las herramientas y dispositivos de control se pueda llevar cifras y estadísticas de los diferentes eventos detectados por los equipos de seguridad informática, la generación de informes con dicha información permite a los analistas de seguridad informática poder evaluar y dar soluciones así como también permite crear historiales para tomar medidas preventivas más efectivas contra dichos ataques y mitigar riesgos.

En este caso la institución cuenta con herramientas de control y prevención de eventos que nos brindan estadísticas actualizadas con el

índice de frecuencia de ataques a nuestros activos de información, Servidores, portales web, etc. La información detallada es emitida por la herramienta Juniper y que son remitidos al departamento de seguridad informática desde el Security Operation Center (SOC), los especialistas monitorean toda actividad en su red a través de una consola centralizada de administración. Desde ahí, se administra, controla y reportan todos los eventos que se puede observar en dicho informe.

Adicionalmente el SOC ofrece un usuario de lectura para que un analista de nuestro departamento de Seguridad informática pueda acceder a la consola del proveedor y obtener detalle de cualquier actividad en particular.

6.2. Evaluación de los dispositivos de control

Los dispositivos de control como los equipos JUNIPER, el antivirus corporativo McAfee, la herramienta de barrido y monitoreo de RED local SNAT son las que nos brindan la seguridad requerida para las normales operaciones de la Institución, el uso periódico de estas herramientas junto con los procedimientos definidos por las normas y políticas de seguridad Informática facilitan la protección de la información crítica y

de vital importancia para la empresa, por esta razón se ha definido la efectividad de las herramientas de control según las características de protección que poseen.

6.2.1. Características de las protecciones Juniper*Deep Inspection*

Se denomina de esta forma, al módulo IDP de los productos Juniper. Es el encargado de analizar las capas superiores de los paquetes recibidos por el dispositivo, en busca de amenazas, integrándose con el módulo de firewall para cumplir su misión.

Screening

Es una protección adicional a la del Deep Inspection, mas relacionada con el comportamiento de la Red, que con la comparativa de firmas. Trabaja en las capas inferiores conjuntamente con el firewall y sirve de primer filtro antes de enviar el paquete al módulo de Deep Inspection.

6.2.2. Características de las protecciones del antivirus corporativo McAfee

La principal característica de esta herramienta es que posea encriptación de correo de ambos lados (emisor y receptor) para

que la información viaje segura por los canales de comunicación y que pueda ser visualizada únicamente por el destinatario final, para este efecto deberá contar con adecuados mecanismos criptográficos.

También se requiere de esta herramienta que posea filtros potentes para correos no deseados así como también servicio de actualización en línea de sus listas de virus.

6.2.3. Características de las protecciones del software de monitoreo de RED SNAT

De entre varias opciones en el mercado se escogió el sistema de monitoreo y barrido de redes SNAT por su interfaz amigable y su rapidez y estabilidad en los procesos.

Las principales características de este software es que nos permite hacer los controles de manera remota si causar molestias a los usuarios, permite ver las pantallas de usuario en tiempo real, permite de manera sigilosa revisar que software tienen instalados los usuarios en sus estaciones de trabajo, así como permite realizar desinstalaciones en red.

También nos da la opción de revisar en línea logs de instalaciones que hayan hecho los usuarios durante un tiempo determinado, y nos muestra una alerta cuando se está realizando alguna falla de seguridad por parte de los usuarios que haya sido configurada previamente como por ejemplo que el usuario haya dejado el equipo encendido luego de la jornada de trabajo.

Gracias a la información obtenida de esta herramienta los analistas de seguridad informática pueden hacer mayor énfasis en hacer cumplir las políticas de seguridad realizando llamados de atención o notificando a los jefes de área para que se apliquen sanciones a los usuarios que hayan cometido faltas o descuidado la información de sus equipos.

6.3. Análisis de resultados emitidos por el sistema

El departamento de seguridad informática, en conjunto con el departamento de riesgos, son quienes revisan, evalúan y emiten criterios sobre los resultados emitidos por los sistemas de control, de dichos análisis se definen acciones correctivas o preventivas según sea el caso.

El departamento de seguridad informática tiene también la tarea de traducir y elaborar informes sobre dichos resultados que sean fáciles de comprender por parte de la gerencia del departamento de Riesgos.

En el caso de los equipos de seguridad perimetral JUNIPER, los análisis de los resultados de los eventos detectados se analizaran según su origen, cantidad por cada tipo de evento y por destinos atacados.

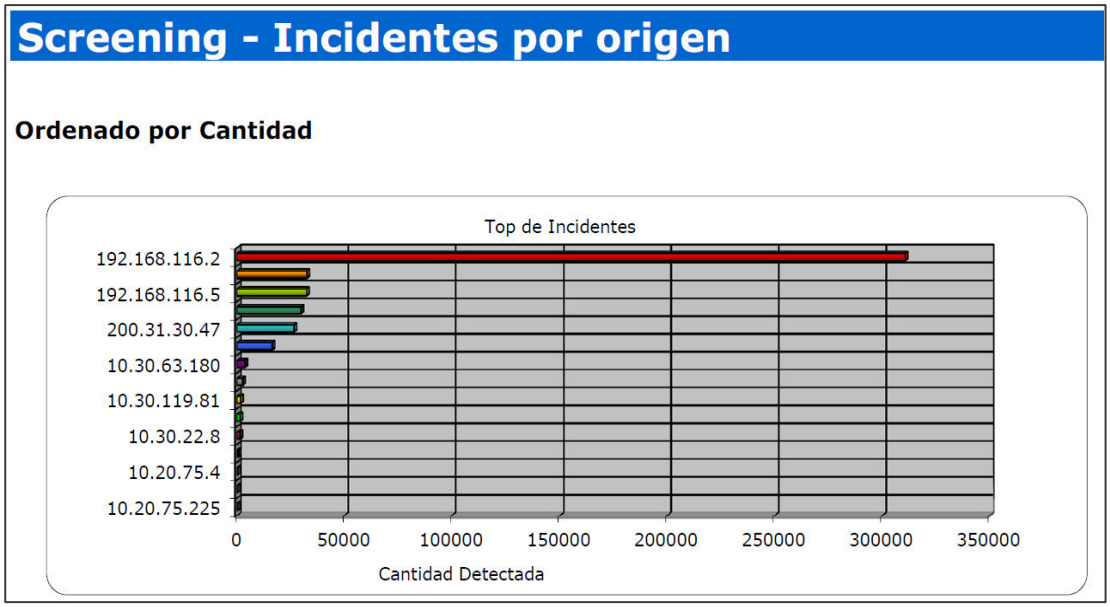

Figura 6.1: Ejemplo de reporte de incidentes agrupados por su origen emitido por equipo de seguridad perimetral Juniper
Fuente: Departamento de Seguridad Informática de la institución.

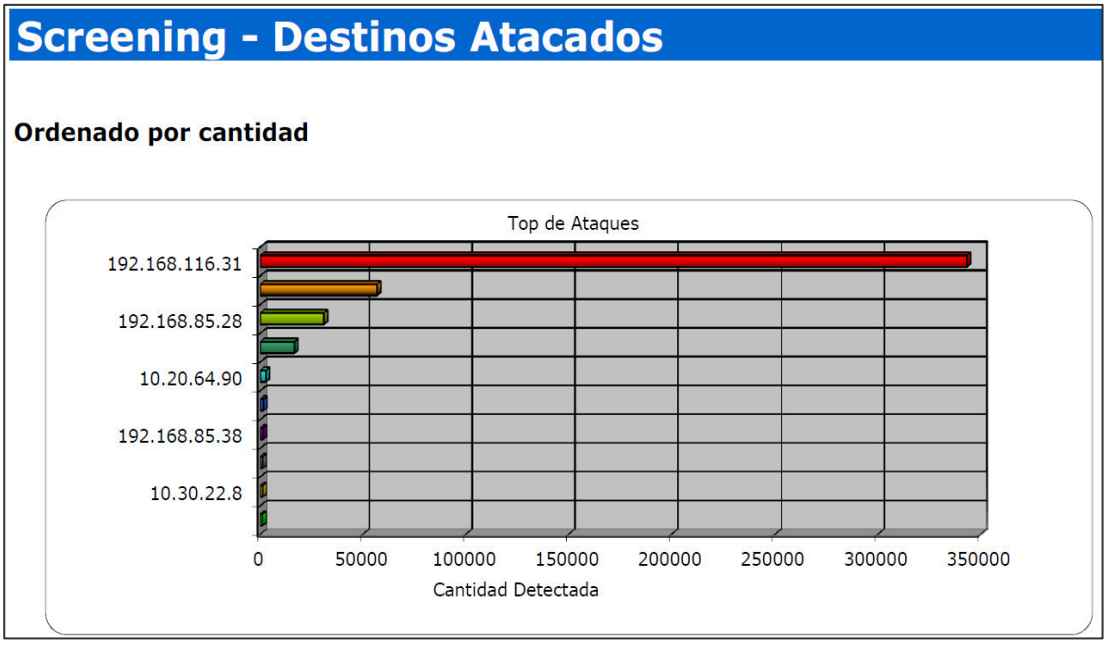

Figura 6.2: Ejemplo de reporte de incidentes agrupados por los destinos afectados dentro de la institución, emitido por equipo de seguridad perimetral Juniper
Fuente: Departamento de Seguridad Informática de la institución.

Los análisis de los resultados emitidos por el software del antivirus corporativo se realizan a través de la consola proporcionada por el proveedor, y se emite informes de los eventos detectados solo cuando estos suceden, pero lo más importante que se logra con esta herramienta es la detección, identificación y bloqueo de correos considerados SPAMS y que podrían contener adjuntos archivos conteniendo códigos maliciosos.

El análisis de los resultados obtenidos con el sistema de monitoreo de red y estaciones de trabajo SNAT, se centra en la frecuencia con la que

los usuarios realizan actividades que puedan vulnerar o descuidar la seguridad de la información que se encuentra a su cuidado, actividades no autorizadas como instalar software no licenciado, o ejecutar archivos EXE desde pendrives son consideradas faltas graves, para evitar estas acciones peligrosas por parte de los usuarios se realizan talleres y capacitaciones para concientizar a los usuarios sobre los peligros que pueden tener las acciones realizadas por ellos sin autorización, gracias a la herramienta SNAT dichas charlas pueden ser direccionadas a los usuarios específicos que más reinciden en dichas faltas y que pueda llegarse a un llamado de atención al usuario como factor disuasivo.

Los resultados de la herramienta SNAT son incluidos en el informe de visita a las agencias de la institución en este caso Quito y Guayaquil, y se hace un escaneo de la situación actual de cada equipo entre estaciones de trabajo y servidores.

Tabla 4: Resultados Guayaquil (Nueva matriz)

Parámetros revisados	Estado	Usuarios	Porcentaje
Nombre del PC	Correcto	18	100,00%
	Incorrecto	0	0,00%
NAC administrable	Correcto	18	79,17%
	Incorrecto	0	20,83 %
Fondo de Pantalla	Correcto	7	83,33%
	Incorrecto	11	16,67%
Bloqueo Regedit	Correcto	17	95,83%
	Incorrecto	1	4,17%
Bloqueo Agregar/Quitar programas	Correcto	14	95,83%
	Incorrecto	4	4,17%
Antivirus	Correcto	16	83,33%
	Incorrecto	2	16,67%
Protector de Pantalla	Correcto	14	95,83%
	Incorrecto	4	4,17%
Office	Correcto	24	100,00%
	Incorrecto	0	0,00%

Se detalla la accesibilidad de cada estación de trabajo y servidores desde los equipos de control.

Detalle de resultados

Grupo de Trabajo, PC's que se encuentran en otro grupo de trabajo:

No se encontraron Equipos en grupos de trabajo ajenos a la institución.

Administrable NAC / SNAT, PC's que NO son administrables:

Guayaquil

Herrera María

Rodas Susana

Quito

Vargas Johanna

Torres Tamara

Game Xavier

Puerto USB desbloqueado al reiniciar equipo, Usuarios conectan dispositivo USB y reinician el equipo para poder acceder (solo pasa con equipos IBM):

Guayaquil

Valarezo Christian

Aguilar Mariana

Quito

Mayorga Paulina

Torres Tamara

Game Xavier

Software sin licencia instalado, Usuarios instalan software para actividades ajenas a la institución:

Guayaquil

Michael Ruperto

Pérez Santiago

Zambrano Wendy

Quito

Castro Mónica

Heymann Romina

González Jorge

Cevallos Katherine (Pasante)

Lascano Luis

Como se muestra en los resultados del SNAT, se puede tener datos verídicos de la situación de cada estación de trabajo para de esa manera ejercer un mayor control para salvaguardar la información.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Una vez realizado el análisis de los resultados de las herramientas de control el departamento de seguridad informática puede emitir sus conclusiones y recomendaciones para su posterior implementación.

1. Se separa las recomendaciones por dispositivos y por áreas para hacer más fácil la identificación de los mismos.

2. Teniendo identificados los riegos y vulnerabilidades se debe proceder a actualizar las políticas de seguridad de la institución y se las adapta a la nueva matriz de acuerdo al análisis de la situación actual del Departamento de Sistemas de la entidad financiera y tomando también en cuenta las políticas vigentes, la actualización estará a cargo de los departamentos de

sistemas y de seguridad informática, quienes estarán a cargo del levantamiento de la información, la creación de nuevas normativas e implementación del nuevo esquema de seguridad informática de la institución.

3. Una vez identificados los activos de información que administra la entidad, se determina que las nuevas políticas de seguridad de información tendrán un alcance total entre personal, áreas, mandos medios y mandos altos de la institución y se debe definir sanciones realistas a su incumplimiento con el fin de promover su aplicación integra por todos los colaboradores internos y externos de la institución, las normativas y políticas de seguridad así como sus sanciones por incumplirlas serán definidas de acuerdo al área y de acuerdo al nivel de importancia de la información en cuestión y definiendo responsabilidades y custodios de información.

En base de los análisis de los resultados obtenidos a través de los diferentes sistemas de control se dispone al departamento de seguridad informática la creación de informes que incluyan estadísticas de los riesgos y amenazas con la finalidad de prevenir situaciones de riesgo futuro.

RECOMENDACIONES

1. Manejo de Racks

Gestionar los medios necesarios para la instalación del Rack que se encuentra en cada sucursal siguiendo las siguientes recomendaciones.

- ✓ En el Rack se deberá alojar solo los equipos de comunicaciones e independizarlos de otros equipos que no tengan los fines de interconectar a las sucursales con las oficinas principales.

- ✓ Las centrales telefónicas y el cableado telefónico no deben formar parte del Rack de Comunicaciones.

- ✓ El Rack deberá tener el ambiente adecuado ya que, todos los equipos de comunicación generan algo de calor y reducen el rendimiento del equipo.

- ✓ El Rack debe estar protegido en su parte superior si se llegare a encontrar debajo de alguna amenaza de humedad o fuga de líquido cercano al equipo de comunicación.

- ✓ Se deberá implementar en el Rack las debidas seguridades en cuanto al acceso, como: apertura de puerta controlada mediante “tarjeta de aproximación” y “circuito cerrado de tv”.

- ✓ El Rack deberá estar en un sitio estratégico de las sucursales, de tal manera que no se encuentre accesible a los funcionarios y a las personas ajenas a la Institución.

- ✓ El rack no debe compartir el espacio físico con otros objetos como: archivadores, escritorios, equipos de limpieza y demás.

- ✓ Los puntos de red no utilizados en las sucursales, no deben estar conectados a un punto activo en los Switches del Rack de Comunicaciones; a menos que estos sean administrables.

2. Wireless

- ✓ Las Claves de accesos de los dispositivos inalámbricos no pueden ser proporcionadas a todos los funcionarios, para así evitar el uso ajeno a la funcionalidad para la que fue instalado.

3. UPS online

- ✓ Todos los Computadores deben estar conectados a la red eléctrica independiente con soporte Ups online para que, en caso de apagones de luz, puedan seguir trabajando.

- ✓ Las Impresoras u otro equipo independiente que no trabaje con almacenamiento de información, no deben formar parte de la red eléctrica independiente para Computadores porque, extraen energía que puede ser asignada a la red de computadores en caso de apagones.

- ✓ Los Ups deben de tener un mantenimiento preventivo para su correcto funcionamiento y así cumpla con el efecto de respaldo de energía a la red independiente de Computadores, y no tengan inconvenientes.

4. Redes

- ✓ El cableado estructurado de las sucursales debe de cumplir con las normativas y estándares de instalación, las cuales incluyen protección física en todas las rutas para que no sufran atenuación.

- ✓ Se debe actualizar toda la infraestructura de Networking para que se viabilicen los proyectos de seguridad, tales como: IPS-Sistema de prevención de intrusos e IDS-Sistema de detección de intrusos.

- ✓ Integrar la solución NAC-Control de acceso a red en las sucursales, con la finalidad de controlar los puntos de acceso a la red y bloquear las conexiones no autorizadas.

5. Generales

- ✓ Colocar la señalética adecuada de prohibición de acceso, en los espacios físicos donde se encuentre el Rack de comunicaciones de las sucursales.

6. Gestión de Responsabilidades

- ✓ El departamento de sistemas deberá explicar y definir las funciones, responsabilidades respecto a la seguridad de la información a los funcionarios de la Institución, antes de otorgar el acceso a la información, contraseñas o sistemas de la información sensibles.

- ✓ El Departamento de Seguridad Informática debe lograr la concienciación del funcionario sobre la Seguridad de la Información

correspondiente a sus funciones y responsabilidades dentro de la institución.

- ✓ La Gerencia Administrativa deberá exigir a los empleados, contratistas y terceros que apliquen aspectos de seguridad de acuerdo con la Política de Seguridad de la Información y procedimientos establecidos en la institución.

- ✓ El Departamento de Seguridad Informática deberá verificar el cumplimiento de las funciones y responsabilidades respecto a la Seguridad de la Información mediante la utilización de reportes e informes.

7. Capacitación y Educación en Seguridad de la información

La Subgerencia de Recursos Humanos en coordinación con el Departamento de Seguridad Informática, deberán emplear mecanismos adecuados para que los empleados y cuando corresponda contratistas y terceros, conforme a las funciones laborales de cada uno, reciban el conocimiento y actualizaciones necesarias de las Políticas de Seguridad de la Información.

8. Proceso disciplinario

- ✓ La Subgerencia de Recursos Humanos debe desarrollar un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la Política de Seguridad de la Información.

- ✓ La Subgerencia de Recursos Humanos debe considerar sanciones graduales, dependiendo de factores tales como naturaleza, cantidad y la gravedad de la violación, así como su impacto en el negocio, el nivel de la capacitación del personal, la legislación correspondiente (Ley de Comercio Electrónico, formas electrónicas, mensajes de datos, entre otros) y demás factores existente en los procedimientos propios de la Institución financiera.

9. Finalización de empleo o cambio de puesto de trabajo

- **Responsabilidades y Terminación del contrato**
  - ✓ La Subgerencia de Recursos Humanos debe comunicar oficialmente al personal las responsabilidades para la terminación de su relación laboral, lo cual debe incluir los requisitos permanentes para la seguridad de la información y las responsabilidades legales o contenidas en cualquier acuerdo de confidencialidad.

- ✓ Los cambios en la responsabilidad o en el contrato laboral de un funcionario deberán ser gestionados por la Subgerencia de Recursos Humanos y Desarrollo Organizacional como la terminación de la responsabilidad o el contrato laboral respectivo, dentro de la nueva responsabilidad o contrato laboral se deberá instaurar en el contrato de confidencial.

- ✓ Previo a la terminación de un contrato es obligación del funcionario realizar la transferencia de la documentación e información de la que fue responsable al nuevo funcionario a cargo, jefe inmediato y/o responsable del área; en caso de ausencia, al Oficial de Seguridad de la información.

- ✓ La Gerencia de División Administrativa y/o Subgerencia de Recursos Humanos deberá garantizar que los contratos del empleado, el contratista o el usuario de terceras partes, incluyan las responsabilidades válidas aún después de la terminación del contrato laboral.

- **Devolución de activos**
  - ✓ La Subgerencia de Recursos Humanos debe garantizar que los empleados devuelvan todos los activos (dispositivos de cómputo móviles, tarjetas de acceso, token usb con certificados de electrónicos, pendrive, entre otros) de la organización que estén inventariados, al finalizar su empleo, contrato o acuerdo.

  - ✓ El departamento de sistemas en coordinación con la Subgerencia de Recurso Humanos deberán aplicar los debidos procesos para garantizar que toda la información generada por el empleado, contratista o usuario de terceras partes dentro de la institución, sea transferida, archivada o eliminada con seguridad.

  - ✓ La Subgerencia de Recursos Humanos deberá solicitar al jefe inmediato del funcionario saliente que certifique que se ha realizado el proceso de traspaso de conocimientos por parte del empleado, contratistas o terceras partes al nuevo funcionario, y en caso de ausencia se podrá realizar dicha transferencia a un funcionario delegado para esta actividad, de tal forma que se asegure la continuación de las operaciones importantes dentro de la institución.

- **Eliminación de derechos de acceso**
  - ✓ La Subgerencia de Recursos Humanos debe notificar al Departamento de Seguridad Informática y a la Gerencia de División Informática cuando un empleado finaliza el contrato o cambia de puesto con el objetivo de retirar los accesos a la información y los recursos de tratamiento de la información o asignar los nuevos accesos de acuerdo a los cambios producidos de ser el caso.

10. Normas de la seguridad física y del entorno

- **Áreas seguras**
  - ✓ La Gerencia de División Administrativa deberá garantizar que los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

- **Perímetro de seguridad física**

  Es responsabilidad de la Gerencia de División Administrativa establecer en la Institución el uso de perímetros de seguridad controlados por personal de seguridad, tarjetas de ingreso o sistemas biométricos para

proteger las áreas que contienen información y medios de procesamiento de información y centros de cómputo (Data centers), para tal efecto deberá considerar lo siguiente:

- ✓ Definir y documentar claramente los perímetros de seguridad (barreras, paredes, puertas de acceso controladas con tarjeta, etc.), con una ubicación y fortaleza adecuadas).
- ✓ Definir un área de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio.
- ✓ Los perímetros de seguridad de los Data Centers deberán estar claramente definidos con respecto a su ubicación y funcionalidad para con el resto del edificio, contarán con atención especial para los requerimientos de seguridad de los mismos, garantizando que no existan brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado.
- ✓ Cualquier funcionario de la Institución estará habilitado para reportar de forma inmediata a la Gerencia de División Informática o administrador de red cuando se detecte la existencia de riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio, cableado eléctrico en mal estado u otros.

- ✓ Se debe elaborar las barreras físicas para prevenir el acceso físico no autorizado y la contaminación ambiental a las áreas donde exista información crítica y de primordial importancia para la institución.
- ✓ Disponer de alarmas de incendio y puertas de evacuación debidamente monitoreadas que cumplan normas nacionales e internacionales.
- ✓ Disponer de un sistema de vigilancia mediante el uso de circuitos cerrados de televisión.
- ✓ Aislar los ambientes de procesamiento de información de los ambientes proporcionados por terceros.

- **Controles de ingreso físico**
  - ✓ Registrar la fecha y la hora de entrada y salida de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida, en el caso del Data Center sólo se permitirá el acceso para propósitos específicos y autorizados.

  - ✓ Controlar y limitar el acceso, exclusivamente a personal autorizado a la información clasificada y a las instalaciones de procesamiento de información. Se debe utilizar controles de autenticación como tarjetas de control de acceso más el número de identificación personal.

- ✓ Exigir que todos los empleados de la Institución, pasantes, contratistas, terceras personas y todos los visitantes usen alguna forma de identificación visible, así como es responsabilidad de todos los funcionarios de la Institución notificar inmediatamente al personal de seguridad si se encuentra a un visitante que no esté usando una identificación visible.

- ✓ Los visitantes que se dirijan a áreas restringidas deberán ser escoltados o a su vez supervisados por el servicio de guardianía de la Institución.

- ✓ Revisar y actualizar periódicamente los derechos de acceso a las áreas restringidas, mismos que serán documentados y firmados por el responsable así como revocados cuando sea necesario.

- **Seguridad de oficinas, recintos e instalaciones**

  La Gerencia de División Administrativa debe controlar y gestionar el diseño y aplicación de seguridad física en las oficinas, habitaciones y medios, para tal efecto deberá considerar lo siguiente:

- ✓ Aplicar los reglamentos y las normas en materia de sanidad y seguridad.

- ✓ Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas tanto en matriz como en el resto de oficinas y sucursales sólo a personas autorizadas, para salvaguardar los equipos de cómputo y de comunicaciones.

- ✓ Los edificios, bodegas o cuartos donde se guarde información importante y de índole confidencial (Centros de Cómputo) deben ser discretos y dar una indicación mínima de su propósito, sin carteles obvios dentro y fuera del edificio que indiquen la presencia de actividades de procesamiento de información.

- ✓ Ubicar las impresoras, copiadoras, entre otros, en un área protegida.

- ✓ Disponer que las puertas y ventanas permanezcan cerradas, especialmente cuando no haya vigilancia.

- **Protección contra amenazas externas e internas**

  La Gerencia de División Administrativa debe controlar, diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre, por lo que deberá considerar lo siguiente:

  - ✓ Adoptar controles para minimizar el riesgo de amenazas físicas potenciales como robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, interferencia del suministro eléctrico e interferencia de las comunicaciones.

  - ✓ Se deberá prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

  - ✓ Realizar mantenimiento de las instalaciones eléctricas y UPS.

  - ✓ Realizar mantenimientos en los sistemas de climatización y ductos de ventilación.

- ✓ Se deberá considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

1. Los materiales peligrosos o combustibles deben ser almacenados en un lugar seguro preparado para almacenar este tipo de materiales y a distancia considerable de áreas donde se archive documentos e información importante. Documentos, papelería y archivos no deben almacenarse en el área asegurada destinada almacenar productos inflamables.
2. El sitio alterno y todo lo que este comprende, equipos de reemplazo y los medios de respaldo deben ubicarse a una distancia segura de la matriz principal para evitar el daño de un desastre que afecte el local principal.
3. Se debe suministrar el equipo apropiado contra-incendios (Extintores, detectores de humo, entre otros) y ubicarlos adecuadamente.

- **Trabajo en áreas seguras (Data Centers, cuartos de redes, entre otros)**

  La Gerencia de División Administrativa en coordinación con las áreas afines deberá controlar el diseño, aplicación de la protección física y lineamientos para trabajar en áreas seguras, para tal efecto deberá considerar lo siguiente:

  - ✓ El Centro de Cómputo de la institución es un área restringida, por lo que sólo el personal previamente autorizado podrá acceder al mismo, su responsable es el Administrador del mismo.

  - ✓ Dar a conocer al personal, la existencia de un área segura.

  - ✓ El personal debe conocer solo lo estrictamente necesario sobre existencia o las actividades dentro de estas áreas.

  - ✓ Se deberá evitar el trabajo no-supervisado para evitar actividades maliciosas.

  - ✓ Revisar periódicamente y disponer de un bloqueo físico de las áreas seguras vacías.

- ✓ No se deberá permitir equipo fotográfico, de vídeo, audio y otro equipo de grabación, como cámaras en equipos móviles dentro de los centros de cómputo; a no ser que tenga previa autorización; su responsable y/o persona autorizada por éste deberá hacer cumplir esta buena práctica.

- ✓ Se deberá proteger el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte, implementando sistemas de suministro de energía ininterrumpido UPS.

BIBLIOGRAFÍA

[1] Estándar Internacional, ISO / IEC 27001, Edición 2005.

[2] Comité de Administración Integral de Riesgos del 20 de octubre de 2011, Acta No. 07-2011, Actualización 07/2012, Edición 19 de marzo de 2012.

[3] Comité de Administración Integral de Riesgos, Acta No. 05-2012, Publicación del 20 marzo de 2012.

[4] Comité de Administración Integral de Riesgos, Acta No. 15-2012, Publicación del 13 noviembre de 2012.

[5] Miro C., Seguridad de la Información., http://www.kelssiler.com/, I (2005), fecha de consulta Marzo del 2016.

[6] Palavicini, Seguridad Informática, http://seguridadinformatica.cl/empresa.php.

[7] Carballo Pariñas, Auditoria de Sistemas. Universidad Iberoamericana, México, R. Edición (1981).

[8] Fine H.L., Seguridad en centros de cómputo. México: Editorial Trillas, Edición 1999.

GLOSARIO

Código malicioso, es un tipo de software o programa que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

Los virus informáticos, son los programas diseñados para realizar cambios o dañar sin autorización, los programas y datos, por consiguiente, los virus pueden causar la destrucción de los recursos corporativos.

Copia de seguridad, es la copia total o parcial de información de discos duros, CD's, bases de datos u otros medios de almacenamiento, de forma que estén disponibles en caso de requerir su recuperación.

Mecanismos Criptográficos, es la aplicación de un algoritmo específico a los datos a fin de alterar su apariencia y volverlos incomprensibles para quienes no están autorizados a ver la información.

Certificado digital, es un documento digital otorgado por una autoridad de certificación de confianza que garantiza la asociación de una persona física con una firma digital.

Doble factor de autenticación, es la combinación de dos mecanismos diferentes que permitan comprobar la identidad de un usuario con el fin de autorizar su ingreso a un sistema de información.

Registros o pistas de auditoria, datos relativos a la actividad de usuarios en las aplicaciones de negocio.

Log's de seguridad, datos relativos a los eventos generados en herramientas tecnológicas como sistemas operativos, motor de bases de datos, etc.

ANEXOS

ANEXO 1

REGISTRO ELECTRÓNICO

SOLICITUD DE CREACION, CAMBIO O MANTENIMIENTO DE ACCESOS INFORMATICOS
USUARIOS ESPECIALES

FECHA DE SOLICITUD: 28 / 12 / 2012 (dd/mm/aaaa)

INFORMACION A SER LLENADA POR EL SOLICITANTE

1. DATOS GENERALES DEL USUARIO ESPECIAL:

DESCRIPCIÓN DEL SERVICIO : _____

_____

CÓDIGO DE USUARIO (Sugerido): _____

DIRECCION DE CORREO (si aplica): _____

2. CARACTERÍSTICAS GENERALES

TIEMPO DE VIGENCIA : ☐ Num. días ó ☐ Ilimitado

CAMBIA CLAVE CADA: ☐ Num. días ó ☐ Nunca cambia

PERMISOS SOBRE EL ARBOL - LDAP

☐ Lectura ☐ Escritura ☐ Comparación ☐ Ninguno

PERMISOS SOBRE EL SISTEMA DE ARCHIVOS NOVELL

☐ Lectura ☐ Escritura ☐ Creación ☐ Borrado ☐ Modificación ☐ Exploración de archivos ☐ Ninguno

DESCRIPCIÓN DE RECURSOS A LOS QUE DEBE ACCEDER (Usuarios, Grupos, BDD, Tablas, Campos, Servidores - SO, etc)

_____

_____

_____

3. RESPONSABILIDAD - DATOS DEL FUNCIONARIO RESPONSABLE DE LA CUENTA

APELLIDOS Y NOMBRES : _____

CEDULA DE IDENTIDAD : _____

AREA: _____

CARGO: _____

FIRMA: _____

INFORMACION A SER LLENADA POR EL JEFE INMEDIATO

4. AUTORIZACIÓN - DATOS DE LA JEFATURA AUTORIZANTE

APELLIDOS Y NOMBRES : _____

CEDULA DE IDENTIDAD : _____

AREA: _____

CARGO: _____

FIRMA: _____

5. ASIGNACION DE CLAVES

Fecha ejecución: ___/___/_____ (dd/mm/aaaa)

Ejecutado por: _____ Firma: _____

8. ACUSE DE RECIBO DE CLAVES - USUARIO RESPONSABLE

Recibí las claves de acceso: SI___ NO___ Motivo: _____

Fecha recepción: ___/___/_____	Nombre: _____	Firma: _____

ANEXO 2

COMPROMISO DE CONFIDENCIALIDAD INDIVIDUAL

Yo,....., con cédula de ciudadanía No. ....., mayor de edad, quien participa como parte del equipo de trabajo de la empresa ……..……. con la que la Corporación Financiera Nacional ha suscrito un contrato/convenio para la provisión de ……....., me obligo al cumplimiento total de las siguientes disposiciones:

PRIMERO:

El presente compromiso se anexa y forma parte integral del Contrato/Convenio suscrito entre las partes mencionadas.

SEGUNDO:

Reconozco y acepto que toda la información que se me proporcione de la Corporación Financiera Nacional es propia de la entidad y por tanto valiosa, especialmente para los negocios desarrollados por ésta y en consecuencia es **Información Confidencial, Privilegiada y goza del carácter de reservada**. Para estos efectos se entiende por Información Confidencial, aquella propia de la entidad, incluyendo toda la información técnica, contable, comercial, legal etc., suministrada al suscrito obligado para los fines indicados en este acuerdo. Esta información tendrá carácter confidencial cualquiera sea el medio bajo el cual haya sido facilitada, comprendiendo la información vertida en software de computador o en medios de almacenamiento electrónico, así como la que consiste en datos, testimonios, noticias, documentos, figuras, referencias orales, visuales o escritas.

Por lo tanto me obligo a:

- Mantener la reserva de la información que me sea entregada por cualquiera de los medios antes descritos o cualquier otro medio, para efectos del desarrollo del trabajo a mi encomendado.
- No divulgar o hacer uso indebido de la información entregada por la Corporación Financiera Nacional.
- No copiar, ni reproducir, parcial o totalmente, por ningún medio la INFORMACION CONFIDENCIAL.

- Devolver todos los documentos que me hayan sido entregados y mantener la reserva de la información recibida, inmediatamente durante y después de finalizada la actividad.
- Responder por daños y perjuicios, en caso de incumplimiento al deber de mantener la confidencialidad y guardar la información, así como también por los costos y gastos que se generen en caso que medie algún reclamo o demanda por violación del deber de confidencialidad.

TERCERO:

Declaro conocer, entender y aceptar el sigilo de información que se derive del trabajo encomendado, así como todas las normas de reserva de la información constantes en las leyes pertinentes, especialmente lo dispuesto en el artículo 46 de la Ley Orgánica de la institución, la ley de propiedad intelectual, así como los convenios internacionales aplicables y sus implicaciones penales que podrían derivar de su incumplimiento.

Se firma como aceptación de lo acordado a los..... Días del mes de..... de 20.....

_____

Nombre:
CI:

ANEXO 3

INFORME DE REVISION Y MONITOREO DE EQUIPOS JUNIPER REGISTRO RSI-06			
DEPARTAMENTO NACIONAL DE SEGURIDAD INFORMATICA			
1. DATOS GENERALES			
Fecha de ejecución:		Período evaluado:	
Componente objeto de revisión/monitoreo:	Equipos de seguridad perimetral Juniper GYE		
Eventos evaluados:	Informes de eventos registrados en los equipos de seguridad perimetral.		
2. RESULTADOS DE LOG.			

Juniper GYE

a.- Resultado Externo

Ataques Septiembre: 161 distribuidos de la siguiente manera: 22 sin importancia, 15 mayores y 134 críticos.

Origen de ataques - Direcciones IP externas

80.82.65.204 – Pertenece a Holanda
186.4.241.130- Pertenece a Ecuador
69.31.134.30 – Pertenece a EEUU
89.248.168.224 - Pertenece a Holanda
94.102.49.150 - Pertenece a Holanda
172.245.6.113 - Pertenece a EEUU
199.168.99.130 - Pertenece a EEUU
46.167.245.133 – Pertenece a Rep. Checa
190.131.3.86 - Pertenece a Ecuador

Equipos con ataques reportados:

186.46.112.146– DNS Externo
186.46.112.144 - Correo Electrónico GYE

Tipos de ataques externos:

DNS: BIND OPT DoS
DI - TOP de Incidentes Detectados
DNS: BIND Version Query
DNS: Unassigned Opcode
SSL: Invalid Content Type

Puertos: 443 y 53

b.- Resultado Interno

Ataques internos: 669358

Origen de ataques - Direcciones IP internas

10.30.2.13 – Forescot Inventarios
10.30.63.14 – GYEE0310
10.30.63.180 - GYEE0304
157.100.75.140 – Switch Core Cisco

Tipos de ataques internos:

IDS IP Spoofing
Block IP fragment traffic
IDS UDP Flood
IDS Address Sweep
IDS ICMP Flood
IDS TCP FIN No ACK
IDS TCP SYN FIN

IDS Port Scan
Source IP session limit
IDS TCP No Flag

Destino de ataques - Direcciones IP internas
10.20.2.50 UIO
10.30.182.5 NO EXISTE YA EN RED
157.100.102.132 Equipo Espectrum OneClick

El informe completo “GYE-Septiembre-2013” se encuentra en la siguiente dirección: G:\USERS\RIESGOS\Seguridad Informática\Aplicaciones\SEGURIDAD PERIMETRAL\Monitoreo y Revisión\Reportes SOC\2013

3. ANALISIS DE RESULTADOS / IDENTIFICACION DE CAUSAS
- Han aumentado el número de ataques externos generados hacia los diferentes servicios expuestos mediante el equipo de seguridad perimetral. - Los ataques externos según el portal de la empresa Juniper son de severidad Crítica, Media y Alta, de acuerdo al portal Juniper. - La mayoría de ataques registrados son hacia el protocolo DNS debido a que las aplicaciones de la Institución son de tipo web y tienen implementado un certificado digital para asegurar el tráfico de información con el protocolo HTTPS. - Se presenta ataques de tipo DNS hacia el servicio de DNS externo de la Institución, así como también ataques al servicio de correo en GYE. - Los ataques hacia el protocolo de DNS es de tipo BIND que es el servicio más común usado en Internet.
4. CONCLUSIONES
- El aumento de registros puede originarse a las pruebas de vulnerabilidad que realiza el proveedor de Servicios de Seguridad Gerenciados como parte del contrato establecido. - El firewall de Guayaquil ha realizado los bloqueos de los eventos generados en los equipos de seguridad perimetral correctamente y los mismos están siendo reportados mensualmente. - Las direcciones ips públicas que han generado el ataques en los equipos de seguridad perimetral pertenecen a EEUU, Holanda, Rep. Checa y Ecuador según la herramienta online Networok-Tools. - Los ataques internos o externos registrados en el equipo de seguridad perimetral no han ocasionado problemas en la disponibilidad de los servicios. - No se ha reportado ningún incidente en los equipos internos sean estaciones de trabajo o servidores mencionados en el reporte.
5. ESTRATEGIAS A APLICAR (recomendaciones)
Revisar los informes generados por el SOC mensualmente para monitorear la actividad que se genera en los equipos de Seguridad Perimetral.

Elaborado por:	**Revisado por:**
Nombre:	Nombre:
Fecha:	Fecha:
GERENCIA DE RIESGOS	
6. APROBACION / SELECCIÓN DE ESTRATEGICAS DE EJECUCION	
	Aprobado por:
	Nombre:

		Fecha:
DEPARTAMENTO DE SEGURIDAD INFORMATICA		
7. REGISTRO DE APLICACIONES DE LA APROBACION Y SEGUIMIENTO.		
Fecha de aplicación	Documento adjunto	Registrado por

ANEXO 4

INFORME DE REVISION Y MONITOREO DE LOGS
REGISTRO RSI-06

DEPARTAMENTO NACIONAL DE SEGURIDAD INFORMATICA

1. DATOS GENERALES

Fecha de ejecución:		Período evaluado:	
Componente objeto de revisión/monitoreo:	Sistema Cobis Quito y R1		
Eventos evaluados:	Logs de acceso al sistema COBIS		

2. RESULTADOS DE LOG.

Se ejecuta el siguiente script

```
select fu_nombre, in_login, count(*) IntentosFallidos, of_nombre
from in_intento, cl_funcionario, cl_oficina
where in_fecha between '20130924' and '20131024'
and fu_login = in_login
and of_oficina = fu_oficina
and fu_oficina in (1, 11, 9, 8, 5, 13)
group by in_login, fu_nombre, of_nombre
having count(1)> 15
order by of_nombre
```

3. ANALISIS DE RESULTADOS / IDENTIFICACION DE CAUSAS

Log de Accesos Fallidos COBIS			
Fecha:			
Funcionario	**Cod. Usuario**	**IntentosFallidos**	**Oficina**
VINTIMILLA BRAVO ADRIAN ESTUARDO	avintimi	57	QUITO
PAEZ TACO LUZ SORAYA	spaez	44	QUITO
CEDENO CORRAL OLGA DEL PILAR	ocedeno	41	QUITO
CACHIMUEL MALES MARIA VICTORIA	vcachimu	37	QUITO
JIMENEZ PAUCAR KATTY GISSELE	kjimenez	36	GUAYAQUIL
ZAPATA MERINO KATYA	kzapata	28	GUAYAQUIL
REINOSO GOYES VERONICA MARGARITA	vreinoso	27	QUITO
ROSERO MARIA CRISTINA	mrosero	26	QUITO
SEGOVIA LARREA JUAN FRANCISCO	jsegovia	25	QUITO

SANDOVAL TABANGO MARIA GABRIELA	msandova	21	QUITO
ALVAREZ VILLACIS JORGE ANIBAL	jalvarez	20	QUITO
HIDALGO ONATE DIEGO FERNANDO	dihidalg	18	QUITO
LLUMIQUINCA CAIZA JOHANA MIREYA	jllumiqu	17	QUITO
BASTIDAS BORJA KATY LORENA	kbastida	16	GUAYAQUIL

4. CONCLUSIONES

- En el periodo analizado comprendido de 30 días se han generado 14 usuarios que han ingresado incorrectamente la clave en el sistema COBIS.
- De 255 usuarios vigentes en el sistema COBIS a nivel de Región 1 se puede evidenciar que alrededor del 5.49% se equivocan al ingresar su clave.

5. ESTRATEGIAS A APLICAR (recomendaciones)

- Hacer un llamado de atención vía mail a las personas que registraron conexiones fallidas.
- Continuar con las revisiones de acuerdo al cronograma de trabajo de actividades del Departamento.

Elaborado por:	**Revisado por:**
Nombre:	Nombre:
Fecha:	Fecha:

GERENCIA NACIONAL DE RIESGOS

6. APROBACION / SELECCIÓN DE ESTRATEGICAS DE EJECUCION

	Aprobado por:
	Nombre: Mauricio Flores
	Fecha:

DEPARTAMENTO NACIONAL DE SEGURIDAD INFORMATICA

7. REGISTRO DE APLICACIONES DE LA APROBACION Y SEGUIMIENTO.

Fecha de aplicación	Documento adjunto	Registrado por

ANEXO 5

INFORME DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (RSI-07)			
GERENCIA NACIONAL DE RIESGOS DEPARTAMENTO NACIONAL DE SEGURIDAD INFORMATICA			
1. REPORTE / NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
Fecha de reporte:		Medio de reporte:	
Nombre del usuario reportante:			
Descripción del reporte:			
2. ANÁLISIS E IDENTIFICACIÓN INICIAL DE CAUSAS (Descripción del impacto, patrones y síntomas, causa raíz, herramientas utilizadas, etc.)			
3. COMUNICACIÓN INICIAL			
4. RECOLECCIÓN DE PISTAS DE AUDITORIA O LOG'S DE SEGURIDAD (EVIDENCIA)			
5. PLANIFICACIÓN E IMPLEMENTACIÓN DE SOLUCIÓN(ES)			

6. COMUNICACIÓN CON LAS PERSONAS AFECTADAS	
7. NOTIFICACIÓN A ORGANISMOS EXTERNOS	
8. NOTIFICACIÓN DE LA ACCIÓN A LA AUTORIDAD PERTINENTE	
9. SEGUIMIENTO DE IMPLEMENTACIÓN DE SOLUCIÓN DEFINITIVA	
10. FIRMAS DEL EQUIPO DE TRABAJO	
Nombre:	Nombre:
Área:	Área:
Fecha:	Fecha:
Nombre:	Nombre:
Área:	Área:
Fecha:	Fecha:
Nombre:	Nombre:
Área:	Área:
Fecha:	Fecha:
11. APROBACIÓN	
Nombre:	
Área:	
Fecha:	

ANEXO 6

INFORME REVISION EQUIPOS DE AGENCIAS Y CENTROS DE DATOS

SR – SM

PARA:

Subgerente Regional de Informática (S)

DE:

Subgerente Regional de Riesgos

FECHA:

Con fecha del _____del 20 se procedió a realizar una revisión a los computadores de los funcionarios y al rack de comunicaciones de las agencias de Guayaquil (Nueva Matriz) y Quito.; Esta actividad se la efectuó con la finalidad de validar que los mismos se encuentren configurados de acuerdo a los estándares de la Institución y en cuanto al rack de comunicaciones que en éstos se encuentren implementados aspectos de seguridad.

A continuación sírvase encontrar los resultados de la ejecución de dicho trabajo:

Objetivo

Garantizar la correcta estandarización de configuración básica en las estaciones de trabajo, la misma que se realiza mediante el utilitario Zenworks de Novell.

Validar el correcto funcionamiento del utilitario Zenworks de Novell, debido a que mediante esta herramienta se realizan otras actualizaciones en los computadores, como por ejemplo: distribución de versiones de los aplicativos del Core Bancario.

Validar los aspectos de seguridad en el rack de comunicaciones.

Dar Cumplimiento a las Políticas de Seguridad de la Información, y al cronograma de actividades del Departamento Nacional de Seguridad Informática.

Parámetros revisados

- Revisión del grupo de trabajo de los Computadores
- Revisión del nombre de los Computadores.
- Revisión de fondo y protector de pantalla institucional
- Validación del bloqueo: Registro de Windows, Propiedades de pantalla, Agregar/Quitar programas.
- Revisión de versión de Antivirus.
- Revisión de versión del software de oficina – Microsoft Office.
- Aspectos de seguridad en los equipos de comunicación

Resumen de Resultados

Estaciones de trabajo por Sucursal:

Guayaquil

Parámetros revisados	Estado	Usuarios	Porcentaje
Nombre del PC	Correcto	3	100,00%
	Incorrecto	0	0,00%
NAC administrable	Correcto	3	100,00%
	Incorrecto	0	0,00%
Fondo de Pantalla	Correcto	2	66,67%
	Incorrecto	1	33,33%
Bloqueo Regedit	Correcto	2	66,67%
	Incorrecto	1	33,33%
Bloqueo Agregar/Quitar programas	Correcto	2	66,67%
	Incorrecto	1	33,33%
Antivirus	Correcto	3	100,00%
	Incorrecto	0	0,00%
Protector de Pantalla	Correcto	2	66,67%
	Incorrecto	1	33,33%
Office	Correcto	0	100,00%
	Incorrecto	3	0,00%

Quito

Parámetros revisados	Estado	Usuarios	Porcentaje
Nombre del PC	Correcto	14	100,00%
	Incorrecto	0	0,00%
NAC administrable	Correcto	10	83,33%
	Incorrecto	2	16,67%
Fondo de Pantalla	Correcto	13	91,67%
	Incorrecto	1	8,33%
Bloqueo Regedit	Correcto	12	83,33%
	Incorrecto	2	16,67%
Bloqueo Agregar/Quitar programas	Correcto	12	83,33%
	Incorrecto	2	16,67%
Antivirus	Correcto	11	83,33%
	Incorrecto	3	16,67%
Protector de Pantalla	Correcto	2	16.67%
	Incorrecto	12	83.33%
Office	Correcto	11	83,33%
	Incorrecto	3	16,67%

Detalle de resultados

Características de Seguridad	Agencia Guayaquil (Nueva Matriz)	Agencia Quito (Sucursal Mayor)
Independencia de equipos de comunicación	El equipo de la central telefónica se encuentra fuera del rack.	El equipo de la central telefónica se encuentra fuera del rack.
Seguridad en los Racks	El acceso a los equipos de comunicación del rack	Fácil acceso a los equipos de comunicación en el

	está correctamente asegurado en un cuarto con llave para el acceso, sin embargo una vez dentro el rack colgante que contiene los equipos de redes no tiene seguridad ya que está abierto todo el tiempo, el cableado no está correctamente organizado y el servidor se encuentra encima del UPS de la agencia.	rack.
Sitio Estratégico	Se encuentra en un cuarto con la debida seguridad y bien ubicado	Se encuentra muy accesible a cualquier Clientes, y a los funcionarios.
Compartición de espacio físico	Comparte espacio físico con cartones.	Comparte espacio físico con archivadores de información y con materiales de limpieza.
Cableado estructurado	Cableado protegido mediante canaletas.	Cableado protegido mediante

		canaletas.
Señal-ética	No existe señal-ética sobre el acceso restringido.	No existe señal ética sobre el acceso restringido.
UPS	UPS implementado, no funciona por falta de revisión.	UPS implementado y funcionando.
RECOMENDACIONES		
Atentamente,		**Conforme,**
Jefe Seguridad Informática		**Subgerente de Riesgos**

ANEXO 7

REGISTRO DE REVISION ACCESO CENTROS DE COMPUTO RSI-02						
Fecha	Mes Evaluado	No. Accesos	No. Novedades	Observaciones novedades	Nombre responsable	Firma responsable