

**ESCUELA DE POSGRADO**

**PROGRAMA DE ESPECIALIZACIÓN EN CIBERSEGURIDAD**

**TRABAJO FINAL**

**GESTIÓN INTEGRAL DE RIESGOS**

**DOCENTE : Ing. Nicanor Sachahuaman Martinez**

**PRESENTADO POR :**

* **Pozo Cajahuanca George Francis**
* **Quispe Ramos Ada**
* **Ricse Pahuacho Francis Carolay**
* **Rojas Ponce Edwin Ronald**

**2020**

**INFORME GENERAL**

1. **ANTECEDENTES**

Las entidades financieras se han consolidado en nuestro medio de forma rápida, que permite realizar operaciones de intermediación financiera como son préstamos, créditos, inversión de capital, seguros, entre otros.

Su principal labor está enmarcada en la captación de fondos y la posterior colocación de dichos fondos para así obtener un beneficio.

1. **DESCRIPCION DE LA ORGANIZACIÓN:**

FORTALEZA, institución financiera que desde el inicio de sus operaciones se encuentra comprometido con la inclusión financiera, tal es así que brinda atención especial a los sectores marginados por la banca tradicional. Siendo el socio más querido de sus clientes, colaboradores y comunidades, que acompañan su progreso, es el principal promotor de evolución de la micro-finanzas de la región.

**Misión**

“Brindar servicios financieros, comprometidos con la inclusión y desarrollo de los emprendedores y sus familias, incrementando el valor de nuestra empresa y el bienestar de nuestros colaboradores”.

**Visión**

"Ser el Banco ético preferido por los emprendedores de la micro y pequeña empresa, sus familias y colaboradores".

**Valores**

* Orientación al cliente
* Innovación
* Trabajo en equipo
* Transparencia
* Orientación a la persona

1. **ORGANIGRAMA DEL ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Para el desarrollo del trabajo el equipo se centró en la Gerencia de Tecnologías de la Información.

**Gráfico N° 01**

1. **RESULTADO DEL INVENTARIO DE ACTIVO**
   1. **Resultado del Inventario de Activos de Infraestructura Tecnológica**

En el área de TI se ha identificado los activos de los cuales 6 son de carácter confidencial y 4 de carácter restringido. Los activos cuyo valor (promedio) sea Relevante (3), Alto (4) o Crítico (5) pasarán a la fase de Análisis del Riesgo

| **Nro.** | **Nombre de Activo** | **Descripción de Activo** | **Categoría del Activo** | **Propietario Responsable** | **Tipo de información** | **Sensibles** | **Categoría de Seguridad** | **Confidencialidad** | **Integridad** | **Disponibilidad** | **Valor** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|
| 1 | Formato Check List | Formato check List que sirve para supervisar las configuraciones realizadas a los servidores | D1 | Dpto. IT | Documento | SI | Restringida | 2 | 3 | 3 | 3 |
| 2 | Formato de ingreso | Formato donde se registra el ingreso de un personal al centro de cómputo | D2 | Dpto. IT | Documento | SI | Restringida | 2 | 3 | 3 | 3 |
| 3 | Switch Core | Dispositivo de interconexión utilizado para conectar equipos en red | D3 | Dpto. IT | Hardware | SI | Confidencial | 3 | 3 | 5 | 4 |
| 4 | Equipo biométrico | Es un dispositivo que permite la identificación biométrica y verifica automáticamente la identidad de la persona mediante la medición de alguna de sus características físicas (huella) | D4 | Dpto. IT | Hardware | SI | Confidencial | 4 | 3 | 3 | 3 |
| 5 | Servidor Windows | Servidor donde se aloja el rol del active directory, se almacena el catálogo de usuarios, grupos. | D5 | Dpto. IT | Hardware | SI | Confidencial | 5 | 5 | 5 | 5 |
| 6 | Sistema operativo Microsoft Windows server 2012 R2 Estándar | Sistema operativo instalado en los servidores de la empresa | D6 | Dpto. IT | Software | NO | Restringida | 2 | 4 | 5 | 4 |
| 7 | Firewall WAF | Aplicación WAF permite proteger las aplicaciones web ante ataques informáticos de tipo sql injection, denegación de servicio | D7 | Dpto. IT | Software | SI | Confidencial | 4 | 4 | 4 | 4 |
| 8 | Gabinetes de comunicación | Contenedor de los equipos de conectividad, donde se resguarda los switches, el cableado restructurado y los servidores | D8 | Dpto. IT | Infraestructura | NO | Pública | 1 | 1 | 1 | 1 |
| 9 | Equipo Antimalware | Equipo que permite inspeccionar el trafico HTTP Y HTPPS para bloquear la descarga de páginas con algún tipo de malware | D9 | Dpto. IT | Hardware | SI | Confidencial | 4 | 4 | 4 | 4 |
| 10 | Centro de Control de la Red (NOC) | Ambiente donde se efectúa el control (televisores o monitores) donde se puede monitorear las redes, enlaces satelitales entre otros | D10 | Dpto. IT | Infraestructura | SI | CONFIDENCIAL | 3 | 3 | 3 | 3 |

1. **RESULTADOS DEL ANALISIS DE RIESGOS:**

Para el análisis de riesgos se ha desarrollado el catálogo de amenazas vs las vulnerabilidades para todos los activos cuyo valor fueron mayor o igual a 3.

Se ha determinado el valor de degradación, valor de impacto, determinación de la probabilidad, la matriz de valor de riesgo, el riesgo de servicio de TI y finalmente el resultado se ha evaluado de acuerdo a la escala PENTA. Los detalles se especifican en el archivo Excel.

**Análisis de Riesgos**

| **N°** | **Servicio** | **Activo** | **Valor** | **Categoría** | **Amenaza** | **Vulnerabilidad** | **Controles Existentes** | **Degradación** | **Riesgo Efectivo** | | | **Riesgo Servicio** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **D** | **Impacto** | **Probabilidad** | **Riesgo** |
| 1 | SERVICIO DE RED Y COMUNICACIÓN | Switch Core | 4 | Tecnológica | Caída de la red | Falta de redundancia de equipos de comunicación (switches) y falta de mantenimiento preventivo | Ninguno | 5 | 4.5 | 3 | 13.5 | 4 |
| SERVICIO DE SOFTWARE | Servidor Windows | 5 | Tecnológica | Fallo de servicios de Aplicaciones, correos electrónico | No hay Servidores Tier 3, ni Mantenimiento Preventivos. | Revisión de logs del Sistema | 5 | 5 | 3 | 15 | 4 |
| Sistema operativo Microsoft Windows server 2012 R2 Estándar | 4 | Tecnológica | Falla del Sistema Operativo del servidor en Producción | Incumplimiento de políticas de despliegue de parches y actualizaciones | Revisión de logs del Sistema | 4 | 4 | 3 | 12 |
| SERVICIO DE SEGURIDAD PERIMETRAL | Firewall WAF | 4 | Tecnológica | Ataques externos | Hay ciertos datos que son invisibles para el WAF | Ninguno | 4 | 4 | 4 | 16 | 4 |
| Equipo Antimalware | 4 | Tecnológica | Equipos con virus | No hay redundancia Equipo Antimalware | Ninguno | 3 | 3.5 | 4 | 14 |

1. **RESULTADOS DE LA EVALUACIÓN DE RIESGOS:**

En ésta fase se ha determinado las matrices de nivel de operación, nivel de disponibilidad, nivel de preparación. Del mismo modo se ha calculado el nivel de tratamiento de acuerdo a la formula (NIVEL DE TRATAMIENTO = (Valor del Riesgo del Servicio \* Valor del Nivel de Preparación) / 2). Finalmente se estableció el nivel de prioridad de los riesgos. Los destalles en el archivo Excel.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Criterios de Nivel de Preparación de los Servicios de TI** | | | |  |  |  |  |  |  |
| **N°** | **Servicios** | **Medición de Operaciones** | | **Medición de Disponibilidad de:** | | **Nivel de la operación** | **Nivel de la Disponibilidad** | **Valor del nivel de preparación** | **Valor del riesgo del servicio** | **Nivel de Tratamiento** | **Nivel de Prioridad** |
| **Tiempo Promedio para la solución de incidentes de producción (HORAS)** | **Número de incidentes de producción de gravedad alta** | **% de cumplimiento o del nivel de disponibilidad** | **Duración total de las interrupciones del servicio (HORAS)** |
| 1 | SERVICIO DE RED Y COMUNICACIÓN | 2 horas | 4 | 98% | 3 | 2 | 3 | 3 | 4 | 6 | 3 |
| 2 | SERVICIO DE SOFTWARE | 2 horas | 2 | 95% | 3 | 2 | 4 | 3 | 4 | 6 | 3 |
| 3 | SERVICIO DE SEGURIDAD PERIMETRAL | 1 hora | 2 | 95% | 2 | 2 | 4 | 3 | 4 | 6 | 3 |

1. **TRATAMIENTO DE LA EVALUACION DE RIESGOS**

Finalmente se ha desarrollado la matriz de tratamiento de riesgos, en donde se ha identificado el tratamiento del riesgo (Evitar, Reducir, Transferir, Retener) para cada servicio de TI identificado. Se evaluó los controles, actividades y tareas a aplicar de acuerdo al riesgo presentado (amenaza y vulnerabilidad). Así como se ha considerado los costos de inversión que amerita cada control con sus plazos de ejecución.



1. **CONCLUSIONES**

* En el presente trabajo final fueron descritos los conceptos e importancia de los términos relacionados con la gestión del riesgo desarrollados en clases y que están presentes en la seguridad de la información que es administrada mediante los diversos equipos, servicios y personal del área de TI; además de conocer los estándares, metodologías y herramientas que posibilitan el desarrollo del análisis de riesgo en una organización.
* MAGERIT fue la metodología implementada en el caso de estudio realizado, para conocer las vulnerabilidades a las cuales se encuentran expuestos los activos que forman parte del departamento de informática de la entidad financiera, mediante un análisis de riesgos de orden cualitativo permitió conocer el nivel de madurez en la seguridad aplicada en la institución para finalmente sugerir las salvaguardas necesarias para reducir los niveles de riesgo e impacto.