**Índice**

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **INTRODUCCIÓN.....................................................................................S** | |  |
| **1.1.** | **Alcance............................................................................................................................S** | |  |
| **2** | **TÉRMINOS Y DEFINICIONES................................................................G** | |  |
| **2.1.** | **Seguridad de la Información .........................................................................................G** | |  |
| **2.2.** | **Evaluación de Riesgos ................................................................................................D** | |  |
| **2.3.** | **Administración de Riesgos .........................................................................................D** | |  |
| **2.4.** | **Comité de Seguridad de la Información ....................................................................G** | |  |
| **2.5.** | **Responsable de Seguridad Informática.....................................................................G** | |  |
| **2.6.** | **Incidente de Seguridad................................................................................................G** | |  |
| **3** | **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ...........................G** | |  |
| **3.1.** | **Objetivo y Aspectos Generales...................................................................................G** | |  |
| **3.2.** | **Sanciones Previstas por Incumplimiento..................................................................G** | |  |
| **4** | **ORGANIZACIÓN DE LA SEGURIDAD ................................................S** | |  |
| **4.1.** | **Infraestructura de la Seguridad de la Información ...................................................S** | |  |
| 4.1.1. | | Comité de Seguridad de la Información ...............................................................S. |  |
| 4.1.2. | | Asignación de Responsabilidades en Materia de Seguridad de la Información ...S |  |
| 4.1.3. | | Proceso de Autorización para Instalaciones de Procesamiento de Información ..S |  |
| 4.1.4. | | Asesoramiento Especializado en Materia de Seguridad de la Información ..........S |  |
| **5** | **RELACIONES CON TERCEROS .................................................D** | |  |
| 5.1. | | Identificación de Riesgos del Acceso de Terceras Partes ....................................D |  |
| 5.2. | | Requerimientos de Seguridad en Contratos o Acuerdos con Terceros................D |  |
| **5.3.** | **Tercerización ................................................................................................................D** | |  |
| 5.3.1. | | Requerimientos de Seguridad en Contratos de Tercerización .............................D |  |
| **6** | **CLASIFICACIÓN Y CONTROL DE ACTIVOS......................................G** | |  |
| **6.1.** | **Inventario de activos....................................................................................................G** | |  |
| **6.2.** | **Clasificación de la información ..................................................................................G** | |  |
| **6.3.** | **Rotulado de la Información .........................................................................................G** | |  |
|  |  | |  |
| **7** | **SEGURIDAD LIGADA A LOS RECURSOS HUMANOS ..............................................S** | |  |

**7.1.** **Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos …S**

|  |  |  |
| --- | --- | --- |
| 7.1.1. | Control y Política del Personal .....................................................S |  |
| 7.1.2. | Compromiso de Confidencialidad...................................................S |  |
| 7.1.3. | Términos y Condiciones de Empleo................................................S |  |
| **7.2. Capacitación del Usuario .......................................................................S** | |  |
| 7.2.1. | Formación y Capacitación en Materia de Seguridad de la Información....S. |  |
| **8 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN...D** | |  |
| 8.1 | Comunicación de Incidentes Relativos a la Seguridad .........................D |  |
| 8.2 | Comunicación de Debilidades en Materia de Seguridad .......................D |  |
| 8.3 | Comunicación de Anomalías del Software........................................D |  |
| 8.4 | Procesos Disciplinarios ....................................................................D |  |

|  |  |  |
| --- | --- | --- |
| **9** | **SEGURIDAD FÍSICA Y AMBIENTAL ..............................................G** |  |
| **9.1** | **Perímetro de Seguridad Física .................................................G** |  |
| **9.2** | **Controles de Acceso Físico ...................................................G** |  |
| **9.3.** | **Protección de Oficinas, Recintos e Instalaciones ................................G** |  |
| **9.4.** | **Desarrollo de Tareas en Áreas Protegidas.............................................G** |  |
| **9.5.** | **Aislamiento de las Áreas de Recepción y Distribución .......................G** |  |
| **9.6.** | **Suministros de Energía....................................................S** |  |
| **9.7.** | **Seguridad del Cableado .......................................................................S** |  |
| **9.8.** | **Mantenimiento de Equipos....................................................................S** |  |
| **9.9.** | **Retiro de los Bienes ........................................................................S** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **10** | **GESTIÓN DE COMUNICACIONES Y OPERACIONES ....................D** | |  |
| **10.1. Procedimientos y Responsabilidades Operativas.........................................D** | | |  |
|  | 10.1.1. | Documentación de los Procedimientos Operativos................................D |  |
|  | 10.1.2. | Control de Cambios en las Operaciones.......................................D |  |
|  | 10.1.3. | Procedimientos de Manejo de Incidentes ................................D |  |
|  | 10.1.4. | Separación de Funciones e Instalaciones..............................................D |  |
| **10.2. Planificación y Aprobación de Sistemas ..................................G** | | |  |
|  | 10.2.1. | Planificación de la Capacidad ...........................G |  |
|  | 10.2.2. | Aprobación del Sistema........................................S |  |

|  |  |  |
| --- | --- | --- |
| **10.3. Protección Contra Software Malicioso ...........................S** | |  |
| 10.3.1 | Controles Contra Software Malicioso ..........................S |  |
| **10.4. Mantenimiento .................................................................D** | |  |
| 10.4.1 | Resguardo de la Información ...........................................D |  |
| 10.4.2 | Registro de Actividades del Personal Operativo ........................D |  |
| 10.4.3 | Registro de Fallas.....................................................................D |  |
| **10.5. Administración de la Red .................................................................S** | |  |
| 10.5.1 | Controles de Red.....................................................S |  |
| **10.6. Administración y Seguridad de los Medios de Almacenamiento ...........S** | |  |
| 10.6.1 | Procedimientos de Manejo de la Información .....................................S |  |
| 10.6.2 | Seguridad de la Documentación del Sistema .......................................S |  |
| **10.7. Intercambios de Información y Software....................................S** | |  |
| 10.7.1 | Acuerdos de Intercambio de Información y Software............................S |  |
| 10.7.4 | Seguridad del Correo Electrónico........................................................D |  |
| 10.7.4.2. | Política de Correo Electrónico............................................D |  |
| 10.7.5 | Seguridad de los Sistemas Electrónicos de Oficina....................D |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **11.** | **CONTROL DE ACCESOS ....................................................................G** | |  |
| **11.1. Requerimientos para el Control de Acceso................................................G** | | |  |
| 11.1.1. | | Política de Control de Accesos.................................................................G |  |
| 11.1.2. | | Reglas de Control de Acceso .................................................................G |  |
| **11.2. Administración de Accesos de Usuarios ..................................G** | | |  |
| 11.2.1. | | Registración de Usuarios ....................................................................G |  |
| 11.2.2. | | Administración de Privilegios...................................................................G. |  |
| 11.2.3. | | Administración de Contraseñas de Usuario .............................................G |  |
| 11.2.5. | | Revisión de Derechos de Acceso de Usuarios .........................................S |  |
| **11.3.** | **Responsabilidades del Usuario....................................................................S** | |  |
| 11.3.1. | | Equipos Desatendidos en Áreas de Usuarios...................................S |  |
| **11.4. Control de Acceso a la Red..............................................................................S** | | |  |
| 11.4.1. | | Política de Utilización de los Servicios de Red ......................................S |  |
| 11.4.2. | | Autenticación de Usuarios para Conexiones Externas ............................S |  |
| 11.4.3. | | Autenticación de Nodos...................................................... |  |
| 11.4.4. | | Protección de los Puertos (Ports) de Diagnóstico Remoto ........................D |  |
| 11.4.5. | | Subdivisión de Redes...........................................................................D |  |
| 11.4.6. | | Acceso a Internet.............................................................................D |  |
| 11.4.7. | | Control de Conexión a la Red ...................................................D |  |
| 11.4.8. | | Seguridad de los Servicios de Red .................................................S |  |
| **11.5. Control de Acceso al Sistema Operativo........................................................D** | | |  |
| 11.5.1. | | Identificación Automática de Terminales...................................................D |  |

|  |  |  |
| --- | --- | --- |
| 11.5.2 | Procedimientos de Conexión de Terminales.......................................G |  |
| 11.5.3 | Identificación y Autenticación de los Usuarios .................................G |  |
| 11.5.4 | Sistema de Administración de Contraseñas .......................................D |  |
| 11.5.5 | Limitación del Horario de Conexión..................................D |  |
|  | |  |
| **12. SEGURIDAD EN LAS TELECOMUNICACIONES...................................S** | |  |
| 12.1 | Registro y Revisión de Eventos.....................................................S |  |
| 12.2 | Monitoreo del Uso de los Sistemas ...............................................S |  |
| 12.3 | Sincronización de Relojes .............................................................D |  |
| **12.4 Trabajo Remoto....................................................D** | |  |
| 12.5 | Trabajo Remoto ......................................................................D |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **13.** | **DESARROLLO Y MANTENIMIENTO DE SISTEMAS..........................G** | |  |
| **13.1.** |  | **Requerimientos de Seguridad de los Sistemas.................G** |  |
| 13.1.1. | | Análisis y Especificaciones de los Requerimientos de Seguridad ..................G |  |
| **13.2.** |  | **Seguridad de los Archivos del Sistema ..........................D** |  |
| 13.2.1. | | Control del Software Operativo ..........................................................S |  |
| 13.2.2. | | Control de Cambios a Datos Operativos......................................D |  |
| **13.3.** |  | **Seguridad de los Procesos de Desarrollo y Soporte............................G** |  |
| 13.3.1. | | Procedimiento de Control de Cambios.......................................G |  |
| 13.3.2. | | Desarrollo Externo de Software...................................................G |  |

|  |  |  |
| --- | --- | --- |
| **14** |  | **CIFRADO………………………………..D** |
| 14.1. | | Política de Utilización de Controles Criptográficos.......................D |
| 14.2. | | Cifrado ..........................................................................D |
| 14.3. | | Firma Digital.............................................................................S |
| 14.4 | | Normas, Procedimientos y Métodos ........................................................S |

**15.** **ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES**

**DEL ORGANISMO**...............................................................................................................................G

**15.1.** **Proceso de la Administración de la Continuidad del Organismo**............................. G

**15.2.** **Continuidad de las Actividades y Análisis de los Impactos**....................................... G

**15.3. Marco para la Planificación de la Continuidad de las Actividades del Organismo…………………….G**

**15.4.** **Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del**

|  |  |
| --- | --- |
| **Organismo …….G** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **16** | **CUMPLIMIENTO ...................................................................................S** | |  |
| **16.1.** | | **Cumplimiento de Requisitos Legales.................................S** |  |
| 16.1.1. | | Identificación de la Legislación Aplicable ..........................................S |  |
| 16.1.2. | | Derechos de Propiedad Intelectual..............................................S |  |
|  | 16.1.2.1. Derecho de Propiedad Intelectual del Software.............................D | |  |
| 16.1.3. | | Protección de los Registros del Organismo ..................D |  |
| 16.1.4. | | Protección de Datos y Privacidad de la Información Personal ...................D |  |

**16.2.** **Revisiones de la Política de Seguridad y la Compatibilidad Técnica**.....................D

16.2.1. Cumplimiento de la Política de Seguridad........................................................................... D

**16.3.** **Consideraciones de Auditorías de Sistemas**.....................................................................G.

16.3.1. Controles de Auditoría de Sistemas...................................................................................... G

**16.4.** **Sanciones Previstas por Incumplimiento**............................................................................G