

A5 - Políticas Generales de Seguridad Informática y de Infraestructura de Sistemas GAF

GAF

Contenido

1	Introducción	10
2	Objetivo	10
3	Alcance	10
4	Beneficios	11
5	Políticas de Seguridad de la Información (A5)	12
5.1	Políticas de Seguridad de la Información	12
5.2	Revisión de las Políticas de Seguridad de la Información	12
6	Organización de la Seguridad de la Información (A6).....	12
6.1	Organización Interna	12
6.1.1	Funciones y responsabilidades de la Seguridad de la Información.....	12
6.1.2	Separación de las Funciones	13
6.1.3	Contacto con Autoridades	15
6.1.4	Contacto con grupos de Interés especial	15
6.1.5	Seguridad de la Información en la gestión de proyectos.....	15
6.2	Dispositivos Móviles y Teletrabajo.....	16
6.2.1	Política de Dispositivos Móviles	16
6.2.2	Teletrabajo	16
7	Seguridad Relativa a los Recursos (A7).....	16
7.1	Previo al empleo	17
7.1.1	Selección	17
7.1.2	Términos y condiciones del empleo	17
7.2	Durante la relación laboral	18
7.2.1	Responsabilidades de las Direcciones.....	18
7.2.2	Concientización, educación y formación en la seguridad de la Información	19
7.2.3	Proceso disciplinario	20
7.3	Finalización de la Relación laboral.....	21
7.3.1	Responsabilidades en la desvinculación.....	21
8	Gestión de Activos (A8)	23
8.1	Responsabilidad de los activos.....	23
8.1.1	Inventario de activos	23
8.1.2	Propiedad de los activos	24

8.1.3	Uso aceptable de activos	24
8.1.4	Devolución de los activos	26
8.2	Clasificación de la Información	27
8.2.1	Clasificación de la Información	27
8.2.2	Etiquetado de la información	29
8.3	Manejo de los activos	30
8.3.1	Manejo de los Soportes	30
8.3.2	Gestión de Soporte Extraíble	31
8.3.3	Eliminación de Soportes	31
8.3.4	Traslado de Soportes Físicos	32
9	Control de Acceso (A9)	32
9.1	Requisitos del negocio para el control de acceso	32
9.1.1	Política de control de acceso	32
9.1.2	Acceso a las redes y a los servicios de red	34
9.2	Gestión del acceso de usuarios	35
9.2.1	Registro de usuarios y cancelación del registro	35
9.2.2	Gestión de acceso a los usuarios	36
9.2.3	Gestión de derechos de acceso privilegiados	37
9.2.4	Gestión de la información de autenticación secreta de los usuarios	37
9.2.5	Revisión de derechos de acceso de usuario	38
9.2.6	Remoción o ajuste de los derechos de acceso	39
9.3	Responsabilidades del usuario	39
9.3.1	Uso de la información de autenticación secreta	39
9.3.2	Restricción de acceso a la información	40
9.3.3	Procedimientos de conexión (log-on) seguros	41
9.3.4	Sistema de gestión de contraseñas	41
9.3.5	Uso de programas de utilidad privilegiados	42
9.3.6	Control de acceso al código de programas fuente	42
10	Criptografía (A10)	43
10.1	Controles criptográficos	43
10.1.1	Política sobre el empleo de controles criptográficos	43
10.1.2	Gestión de claves	44
11	Seguridad física y del entorno (A11)	45
11.1	Áreas seguras	45
11.1.1	Perímetro de seguridad física	45
11.1.2	Controles de acceso físico	46
11.1.3	Seguridad de oficinas, despachos e instalaciones	47

11.1.4	Protección contra amenazas externas y del ambiente	48
11.1.5	El trabajo en las áreas seguras	49
11.2	Equipamiento	50
11.2.1	Ubicación y protección del equipamiento	50
11.2.2	Elementos de soporte.....	51
11.2.3	Seguridad en el cableado	52
11.2.4	Mantenimiento del equipamiento.....	53
11.2.5	Retiro de bienes	53
11.2.6	Seguridad del equipamiento y de los activos fuera de las instalaciones	54
11.2.7	Seguridad en la reutilización o eliminación de equipos	55
11.2.8	Equipamiento desatendido por el usuario	55
11.2.9	Política de escritorio y pantalla limpios.....	55
12	Seguridad de las Operaciones (A12).....	56
12.1	Procedimientos operacionales y responsabilidades	57
12.1.1	Procedimientos documentados de operación.....	57
12.1.2	Gestión de cambios.....	57
12.1.3	Gestión de la capacidad	58
12.1.4	Separación de los ambientes para desarrollo, prueba y operación	58
12.2	Protección ante software malicioso	59
12.2.1	Controles ante software malicioso	59
12.3	Respaldo	61
12.3.1	Respaldo de la información	61
12.4	Registros y supervisión	62
12.4.1	Registro de eventos.....	62
12.4.2	Protección de la información de registros (logs).....	63
12.4.3	Registros del administrador y operador.....	64
12.4.4	Sincronización de relojes.....	64
12.5	Control de software en la producción.....	65
12.5.1	Instalación de software en los sistemas operativos.....	65
12.6	Gestión de vulnerabilidad técnica	65
12.6.1	Gestión de vulnerabilidades técnicas	65
12.6.2	Restricciones en la instalación de software	66
12.7	Consideraciones sobre la auditoría de sistemas de información....	66
12.7.1	Controles de auditoría de sistemas de información.....	66
13	Seguridad en las Comunicaciones (A13)	66
13.1	Gestión de la seguridad de red.....	67

13.1.1	Controles de Red.....	67
13.1.2	Seguridad de los servicios de red.....	67
13.1.3	Separación en redes	69
13.2	Intercambio de información	70
13.2.1	Políticas y procedimientos de intercambio de información	70
13.2.2	Acuerdos de intercambio de información	71
13.2.3	Mensajería electrónica	72
13.2.4	Acuerdos de confidencialidad y de no divulgación	73
14	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información (A14)	74
14.1	Requisitos de seguridad de los Sistemas de información	74
14.1.1	Análisis y especificación de los requisitos de seguridad	74
14.1.2	Aseguramiento de los servicios de aplicación en las redes públicas.....	74
14.1.3	Protección de transacciones de los servicios de aplicación	75
14.2	Seguridad den los procesos de desarrollo y soporte	76
14.2.1	Política de desarrollo seguro	76
14.2.2	Procedimiento de control de cambios del sistema.....	76
14.2.3	Revisión técnica de aplicaciones después de cambios de las plataformas operativas	77
14.2.4	Restricciones a los cambios en los paquetes de software	77
14.2.5	Principios de la ingeniería de Sistemas Seguros.....	78
14.2.6	Ambiente de desarrollo seguro.....	78
14.2.7	Desarrollo subcontratado	79
14.2.8	Pruebas de seguridad del sistema	79
14.2.9	Pruebas de aceptación del sistema.....	80
14.3	Datos de prueba.....	80
14.3.1	Protección de datos de prueba.....	80
15	Relación con proveedores (A15)	80
15.1	Seguridad de la información en las relaciones con los proveedores	80
15.1.1	Política de seguridad de la información para las relaciones con los proveedores	80
15.1.2	Tener en cuenta la seguridad en los acuerdos con proveedores	81
15.1.3	Cadena de suministro de tecnologías de la información y las comunicaciones .	82
15.2	Gestión de la entrega del servicio por terceras partes	82
15.2.1	Seguimiento y revisión de los servicios de proveedores	82
15.2.2	Gestión de cambios en los servicios de los proveedores	82
16	Gestión de Incidentes de la Seguridad de la Información (A16)	82
16.1	Gestión de incidentes y mejoras de seguridad de la información.....	83

17 Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio (A17)	89
17.1 Continuidad de la seguridad de la información.....	89
17.1.1 Planificación de la continuidad de la seguridad de la información.....	89
17.1.2 Implementación de la continuidad de seguridad de la información	90
17.1.3 Verificar, revisar y evaluar la continuidad de la seguridad de la información	90
17.2 Redundancia	90
17.2.1 Disponibilidad de las instalaciones de procesamiento de información	90
18 Cumplimiento (A18)	90
18.1 Cumplimiento de los requisitos legales y contractuales	91
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	91
18.1.2 Derechos de propiedad intelectual	91
18.1.3 Protección de los registros	91
18.1.4 Protección de los datos y privacidad de la información personal	92
18.1.5 Regulación de los controles criptográficos	92
18.2 Revisiones de seguridad de la información	92
18.2.1 Revisión independiente de la seguridad de la información.....	92
18.2.2 Cumplimiento de la política y las normas de seguridad.....	93
18.2.3 Revisión del cumplimiento técnico.....	93
19 Políticas y/o Procedimientos Relacionados	94
20 Definiciones	95