ANEXO 5:

CONTROLES DE LOS ESTÁNDARES ISO/IEC 17799 E ISO/IEC 27001, SECCIONES 5 A 15

CONTROLES DEL ESTÁNDAR ISO / IEC 17799, SECCIONES 5 A 15

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- 5.1 Política de Seguridad de la información
  - 5.1.1 Documentación de la política de seguridad
  - 5.1.2 Revisión y Evaluación

6. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

- 6.1 Comité de gestión de seguridad de la información
  - 6.1.1 Comité de gestión de seguridad de la información
  - 6.1.2 Coordinación de la seguridad de la información
  - 6.1.3 Asignación de responsabilidades sobre seguridad de información
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información
  - 6.1.5 Acuerdos de confidencialidad
  - 6.1.6 Contacto con autoridades
  - 6.1.7 Contacto con grupos de interés especial
  - 6.1.8 Revisión independiente de la seguridad de la información
- 6.2 Seguridad en los accesos de terceras partes
  - 6.2.1 Identificación de riesgos por el acceso de terceros
  - 6.2.2 Requisitos de seguridad cuando sea trata con clientes
  - 6.2.3 Requisitos de seguridad en contratos de outsourcing

7. CLASIFICACIÓN Y CONTROL DE ACTIVOS

- 7.1 Responsabilidad sobre los activos
  - 7.1.1 Inventario de activos
  - 7.1.2 Propiedad de los activos
  - 7.1.3 Uso adecuado de los activos
- 7.2 Clasificación de la información
  - 7.2.1 Guías de clasificación
  - 7.2.2 Marcado y tratamiento de la información

8. SEGURIDAD EN RECURSOS HUMANOS

- 8.1 Seguridad antes del empleo
  - 8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales
  - 8.1.2 Selección y política de personal
  - 8.1.3 Acuerdos de confidencialidad
- 8.2 Durante el empleo
  - 8.2.1 Responsabilidades de la gerencia
  - 8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información
  - 8.2.3 Proceso disciplinario
- 8.3 Finalización o cambio del empleo
  - 8.3.1 Responsabilidades de finalización
  - 8.3.2 Retorno de activos
  - 8.3.3 Retiro de los derechos de acceso

9. SEGURIDAD FÍSICA Y DEL ENTORNO

- 9.1 Áreas seguras
  - 9.1.1 Perímetro de seguridad física
  - 9.1.2 Controles físicos de entradas
  - 9.1.3 Seguridad de oficinas, despachos y recursos
  - 9.1.4 Protección contra amenazas externas y ambientales
  - 9.1.5 El trabajo en las áreas seguras
  - 9.1.6 Acceso publico, áreas de carga y descarga
- 9.2 Seguridad de los equipos
  - 9.2.1 Instalación y protección de equipos
  - 9.2.2 Suministro eléctrico
  - 9.2.3 Seguridad del cableado
  - 9.2.4 Mantenimiento de equipos
  - 9.2.5 Seguridad de equipos fuera de los locales de la organización
  - 9.2.6 Seguridad en el rehúso o eliminación de equipos
  - 9.2.7 Retiro de la propiedad

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

- 10.1 Procedimientos y responsabilidades de operación
  - 10.1.1 Documentación de procedimientos operativos
  - 10.1.2 Gestión de Cambios
  - 10.1.3 Segregación de tareas
  - 10.1.4 Separación de los recursos para desarrollo y para producción
- 10.2 Gestión de servicios externos
  - 10.2.1 Servicio de entrega
  - 10.2.2 Monitoreo y revisión de los servicios externos
  - 10.2.3 Gestionando cambios para los servicios externos
- 10.3 Planificación y aceptación del sistema
  - 10.3.1 Planificación de la capacidad
  - 10.3.2 Aceptación del sistema
- 10.4 Protección contra software malicioso
  - 10.4.1 Medidas y controles contra software malicioso
  - 10.4.2 Medidas y controles contra código móvil
- 10.5 Gestión de respaldo y recuperación
  - 10.5.1 Recuperación de la información
- 10.6 Gestión de seguridad en redes
  - 10.6.1 Controles de red
  - 10.6.2 Seguridad en los servicios de redes
- 10.7 Utilización de los medios de información
  - 10.7.1 Gestión de medios removibles
  - 10.7.2 Eliminación de medios
  - 10.7.3 Procedimientos de manipulación de la información
  - 10.7.4 Seguridad de la documentación de sistemas
- 10.8 Intercambio de información
  - 10.8.1 Políticas y procedimientos para el intercambio de información y software
  - 10.8.2 Acuerdos de Intercambio
  - 10.8.3 Medios físicos en tránsito
  - 10.8.4 Seguridad en la mensajería electrónica
  - 10.8.5 Sistemas de Información de Negocios
- 10.9 Servicios de correo electrónico
  - 10.9.1 Comercio Electrónico
  - 10.9.2 Transacciones en línea
  - 10.9.3 Información publica disponible
- 10.10 Monitoreo
  - 10.10.1 Registro de la auditoría
  - 10.10.2 Monitoreando el uso del sistema
  - 10.10.3 Protección de la información de registro
  - 10.10.4 Registro de administradores y operadores
  - 10.10.5 Registro de la avería
  - 10.10.6 Sincronización del reloj

11. CONTROL DE ACCESOS

- 11.1 Requisitos de negocio para el control de accesos
  - 11.1.1 Política de control de accesos
- 11.2 Gestión de acceso de usuarios
  - 11.2.1 Registro de usuarios
  - 11.2.2 Gestión de privilegios
  - 11.2.3 Gestión de contraseñas de usuario
  - 11.2.4 Revisión de los derechos de acceso de los usuarios
- 11.3 Responsabilidades de los usuarios
  - 11.3.1 Uso de contraseñas
  - 11.3.2 Equipo informático de usuario desatendido
  - 11.3.3 Política de pantalla y escritorio limpio
- 11.4 Control de acceso a la red
  - 11.4.1 Política de uso de los servicios de la red
  - 11.4.2 Autentificación de usuario para conexiones externas
  - 11.4.3 Identificación de equipos en las redes
  - 11.4.4 Diagnostico remoto y configuración de protección de puertos
  - 11.4.5 Segregación en las redes
  - 11.4.6 Control de conexión a las redes
  - 11.4.7 Control de enrutamiento en la red
- 11.5 Control de acceso al sistema operativo
  - 11.5.1 Procedimientos de conexión de terminales
  - 11.5.2 Identificación y autenticación del usuario
  - 11.5.3 Sistema de gestión de contraseñas
  - 11.5.4 Utilización de las facilidades del sistema
  - 11.5.5 Desconexión automática de sesiones
  - 11.5.6 Limitación del tiempo de conexión
- 11.6 Control de acceso a las aplicaciones y la información
  - 11.6.1 Restricción de acceso a la información
  - 11.6.2 Aislamiento de sistemas sensibles
- 11.7 Informática móvil y teletrabajo
  - 11.7.1 Informática móvil y comunicaciones
  - 11.7.2 Teletrabajo

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- 12.1 Requisitos de seguridad de los sistemas
  - 12.1.1 Análisis y especificación de los requisitos de seguridad
- 12.2 Seguridad de las aplicaciones del sistema
  - 12.2.1 Validación de los datos de entrada
  - 12.2.2 Control del proceso interno
  - 12.2.3 Integridad de mensajes
  - 12.2.4 Validación de los datos de salida
- 12.3 Controles criptográficos
  - 12.3.1 Política de uso de los controles criptográficos
  - 12.3.2 Gestión de claves
- 12.4 Seguridad de los archivos del sistema
  - 12.4.1 Control del software en producción
  - 12.4.2 Protección de los datos de prueba del sistema
  - 12.4.3 Control de acceso a los códigos de programas fuente
- 12.5 Seguridad en los procesos de desarrollo y soporte
  - 12.5.1 Procedimientos de control de cambios
  - 12.5.2 Revisión técnica de los cambios en el sistema operativo
  - 12.5.3 Restricciones en los cambios a los paquetes de software
  - 12.5.4 Fuga de Información
  - 12.5.5 Desarrollo externo del software
- 12.6 Control de las vulnerabilidades técnicas

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

13.1 Reportando eventos y debilidades de la seguridad de información

13.1.1 Reportando los eventos en la seguridad de información

13.1.2 Reportando debilidades en la seguridad de información

13.2 Gestión de las mejoras e incidentes en la seguridad de información

13.2.1 Responsabilidades y procedimientos

13.2.2 Aprendiendo de los incidentes en la seguridad de información

13.2.3 Recolección de evidencia

14. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

14.1 Aspectos de la gestión de continuidad del negocio

14.1.1 Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio

14.1.2 Continuidad del negocio y evaluación de riesgos

14.1.3 Redacción e implantación de planes de continuidad que incluyen la seguridad de información

14.1.4 Marco de planificación para la continuidad del negocio

14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

15. CUMPLIMIENTO

15.1 Cumplimiento con los requisitos legales

15.1.1 Identificación de la legislación aplicable

15.1.2 Derechos de propiedad intelectual (DPI)

15.1.3 Salvaguarda de los registros de la organización

15.1.4 Protección de los datos y de la privacidad de la información personal

15.1.5 Prevención en el mal uso de los recursos de tratamiento de la información

15.1.6 Regulación de los controles criptográficos

15.2 Revisiones de la política de seguridad y de la conformidad técnica

15.2.1 Conformidad con la política de seguridad y los estándares

15.2.2 Comprobación de la conformidad técnica

15.3 Consideraciones sobre la auditoría de sistemas

15.3.1 Controles de auditoría de sistemas

15.3.2 Protección de las herramientas de auditoría de sistemas

CONTROLES DEL ESTÁNDAR ISO / IEC 27001, SECCIONES 5 A 15

A.5	Security policy	
A.5.1	Information security policy Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	
A.5.1.1	Information security policy document	Control An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
A.5.1.2	Review of the information security policy	Control The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6	Organization of information security	
A.6.1	Internal organization Objective: To manage information security within the organization.	
A.6.1.1	Management commitment to information security	Control Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
A.6.1.2	Information security co-ordination	Control Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
A.6.1.3	Allocation of information security responsibilities	Control All information security responsibilities shall be clearly defined.
A.6.1.4	Authorization process for information processing facilities	Control A management authorization process for new information processing facilities shall be defined and implemented.
A.6.1.5	Confidentiality agreements	Control Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
A.6.1.6	Contact with authorities	Control Appropriate contacts with relevant authorities shall be maintained.
A.6.1.7	Contact with special interest groups	Control Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.1.8	Independent review of information security	Control The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
A.6.2 External parties Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.		
A.6.2.1	Identification of risks related to external parties	Control The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A.6.2.2	Addressing security when dealing with customers	Control All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
A.6.2.3	Addressing security in third party agreements	Control Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.
A.7 Asset management		
A.7.1 Responsibility for assets		
A.7.1.1	Inventory of assets	Control All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
A.7.1.2	Ownership of assets	Control All information and assets associated with information processing facilities shall be "owned" by a designated part of the organization.
A.7.1.3	Acceptable use of assets	Control Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
A.7.2 Information classification Objective: To ensure that information receives an appropriate level of protection.		
A.7.2.1	Classification guidelines	Control Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
A.7.2.2	Information labelling and handling	Control An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.

A.8 Human resources security		
A.8.1 Prior to employment [4)] Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.		
A.8.1.1	Roles and responsibilities	Control Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.
A.8.1.2	Screening	Control Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
A.8.1.3	Terms and conditions of employment	Control As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.
A.8.2 During employment Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.		
A.8.2.1	Management responsibilities	Control Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
A.8.2.2	Information security awareness, education and training	Control All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
A.8.2.3	Disciplinary process	Control There shall be a formal disciplinary process for employees who have committed a security breach.
A.8.3 Termination or change of employment Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.		
A.8.3.1	Termination responsibilities	Control Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

A.8.3.2	Return of assets	Control All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
A.8.3.3	Removal of access rights	Control The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9 Physical and environmental security		
A.9.1 Secure areas Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.		
A.9.1.1	Physical security perimeter	Control Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	Control Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.9.1.3	Securing offices, rooms and facilities	Control Physical security for offices, rooms, and facilities shall be designed and applied.
A.9.1.4	Protecting against external and environmental threats	Control Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
A.9.1.5	Working in secure areas	Control Physical protection and guidelines for working in secure areas shall be designed and applied.
A.9.1.6	Public access, delivery and loading areas	Control Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
A.9.2 Equipment security Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.		
A.9.2.1	Equipment siting and protection	Control Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

A.9.2.2	Supporting utilities	Control Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.9.2.3	Cabling security	Control Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
A.9.2.4	Equipment maintenance	Control Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.9.2.5	Security of equipment off-premises	Control Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
A.9.2.6	Secure disposal or re-use of equipment	Control All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
A.9.2.7	Removal of property	Control Equipment, information or software shall not be taken off-site without prior authorization.
A.10 Communications and operations management		
A.10.1 Operational procedures and responsibilities Objective: To ensure the correct and secure operation of information processing facilities.		
A.10.1.1	Documented operating procedures	Control Operating procedures shall be documented, maintained, and made available to all users who need them.
A.10.1.2	Change management	Control Changes to information processing facilities and systems shall be controlled.
A.10.1.3	Segregation of duties	Control Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.10.1.4	Separation of development, test and operational facilities	Control Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.
A.10.2 Third party service delivery management Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.		
A.10.2.1	Service delivery	Control It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

A.10.2.2	Monitoring and review of third party services	Control The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
A.10.2.3	Managing changes to third party services	Control Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
A.10.3 System planning and acceptance Objective: To minimize the risk of systems failures.		
A.10.3.1	Capacity management	Control The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
A.10.3.2	System acceptance	Control Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
A.10.4 Protection against malicious and mobile code Objective: To protect the integrity of software and information.		
A.10.4.1	Controls against malicious code	Control Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
A.10.4.2	Controls against mobile code	Control Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
A.10.5 Back-up Objective: To maintain the integrity and availability of information and information processing facilities.		
A.10.5.1	Information back-up	Control Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.
A.10.6 Network security management Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.		
A.10.6.1	Network controls	Control Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including

A.10.6.2	Security of network services	Control Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A.10.7 Media handling Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.		
A.10.7.1	Management of removable media	Control There shall be procedures in place for the management of removable media.
A.10.7.2	Disposal of media	Control Media shall be disposed of securely and safely when no longer required, using formal procedures.
A.10.7.3	Information handling rocedures	Control Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
A.10.7.4	Security of system documentation	Control System documentation shall be protected against unauthorized access.
A.10.8 Exchange of information Objective: To maintain the security of information and software exchanged within an organization and with any external entity.		
A.10.8.1	Information exchange policies and procedures	Control Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
A.10.8.2	Exchange agreements	Control Agreements shall be established for the exchange of information and software between the organization and external parties.
A.10.8.3	Physical media in transit	Control Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.
A.10.8.4	Electronic messaging	Control Information involved in electronic messaging shall be appropriately protected.
A.10.8.5	Business information systems	Control Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

A.10.9 Electronic commerce services Objective: To ensure the security of electronic commerce services, and their secure use.		
A.10.9.1	Electronic commerce	Control Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
A.10.9.2	On-line transactions	Control Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.10.9.3	Publicly available information	Control The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
A.10.10 Monitoring Objective: To detect unauthorized information processing activities.		
A.10.10.1	Audit logging	Control Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
A.10.10.2	Monitoring system use	Control Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
A.10.10.3	Protection of log information	Control Logging facilities and log information shall be protected against tampering and unauthorized access.
A.10.10.4	Administrator and operator logs	Control System administrator and system operator activities shall be logged.
A.10.10.5	Fault logging	Control Faults shall be logged, analyzed, and appropriate action taken.
A.10.10.6	Clock synchronization	Control The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
A.11 Access control		
A.11.1 Business requirement for access control Objective: To control access to information.		
A.11.1.1	Access control policy	Control An access control policy shall be established, documented, and reviewed based on business and security requirements for access.

A.11.2 User access management Objective: To ensure authorized user access and to prevent unauthorized access to information systems.		
A.11.2.1	User registration	Control There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
A.11.2.2	Privilege management	Control The allocation and use of privileges shall be restricted and controlled.
A.11.2.3	User password management	Control The allocation of passwords shall be controlled through a formal management process.
A.11.2.4	Review of user access rights	Control Management shall review users' access rights at regular intervals using a formal process.
A.11.3 User responsibilities Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.		
A.11.3.1	Password use	Control Users shall be required to follow good security practices in the selection and use of passwords.
A.11.3.2	Unattended user equipment	Control Users shall ensure that unattended equipment has appropriate protection.
A.11.3.3	Clear desk and clear screen policy	Control A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.11.4 Network access control Objective: To prevent unauthorized access to networked services.		
A.11.4.1	Policy on use of network services	Control Users shall only be provided with access to the services that they have been specifically authorized to use.
A.11.4.2	User authentication for external connections	Control Appropriate authentication methods shall be used to control access by remote users.
A.11.4.3	Equipment identification in networks	Control Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
A.11.4.4	Remote diagnostic and configuration port protection	Control Physical and logical access to diagnostic and configuration ports shall be controlled.

A.11.4.5	Segregation in networks	Control Groups of information services, users, and information systems shall be segregated on networks.
A.11.4.6	Network connection control	Control For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.
A.11.4.7	Network routing control	Control Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A.11.5 Operating system access control Objective: To prevent unauthorized access to operating systems.		
A.11.5.1	Secure log-on procedures	Control Access to operating systems shall be controlled by a secure log-on procedure.
A.11.5.2	User identification and authentication	Control All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A.11.5.3	Password management system	Control Systems for managing passwords shall be interactive and shall ensure quality passwords.
A.11.5.4	Use of system utilities	Control The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.11.5.5	Session time-out	Control Inactive sessions shall shut down after a defined period of inactivity.
A.11.5.6	Limitation of connection time	Control Restrictions on connection times shall be used to provide additional security for high-risk applications.
A.11.6 Application and information access control Objective: To prevent unauthorized access to information held in application systems.		
A.11.6.1	Information access restriction	Control Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
A.11.6.2	Sensitive system isolation	Control Sensitive systems shall have a dedicated (isolated) computing environment.

A.11.7 Mobile computing and teleworking Objective: To ensure information security when using mobile computing and teleworking facilities.		
A.11.7.1	Mobile computing and communications	Control A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
A.11.7.2	Teleworking	Control A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
A.12 Information systems acquisition, development and maintenance		
A.12.1 Security requirements of information systems Objective: To ensure that security is an integral part of information systems.		
A.12.1.1	Security requirements analysis and specification	Control Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
A.12.2 Correct processing in applications Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.		
A.12.2.1	Input data validation	Control Data input to applications shall be validated to ensure that this data is correct and appropriate.
A.12.2.2	Control of internal processing	Control Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
A.12.2.3	Message integrity	Control Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
A.12.2.4	Output data validation	Control Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A.12.3 Cryptographic controls Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.		
A.12.3.1	Policy on the use of cryptographic controls	Control A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.12.3.2	Key management	Control Key management shall be in place to support the organization's use of cryptographic techniques.

A.12.4 Security of system files Objective: To ensure the security of system files.		
A.12.4.1	Control of operational software	Control There shall be procedures in place to control the installation of software on operational systems.
A.12.4.2	Protection of system test data	Control Test data shall be selected carefully, and protected and controlled.
A.12.4.3	Access control to program source code	Control Access to program source code shall be restricted.
A.12.5 Security in development and support processes Objective: To maintain the security of application system software and information.		
A.12.5.1	Change control procedures	Control The implementation of changes shall be controlled by the use of formal change control procedures.
A.12.5.2	Technical review of applications after operating system changes	Control When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.12.5.3	Restrictions on changes to software packages	Control Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
A.12.5.4	Information leakage	Control Opportunities for information leakage shall be prevented.
A.12.5.5	Outsourced software development	Control Outsourced software development shall be supervised and monitored by the organization.
A.12.6 Technical Vulnerability Management Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.		
A.12.6.1	Control of technical vulnerabilities	Control Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
A.13 Information security incident management		
A.13.1 Reporting information security events and weaknesses Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.		
A.13.1.1	Reporting information security events	Control Information security events shall be reported through appropriate management channels as quickly as possible.

A.13.1.2	Reporting security weaknesses	Control All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
A.13.2 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.		
A.13.2.1	Responsibilities and procedures	Control Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A.13.2.2	Learning from information security incidents	Control There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
A.13.2.3	Collection of evidence	Control Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
A.14 Business continuity management		
A.14.1 Information security aspects of business continuity management Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.		
A.14.1.1	Including information security in the business continuity management process	Control A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
A.14.1.2	Business continuity and risk assessment	Control Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
A.14.1.3	Developing and implementing continuity plans including information security	Control Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
A.14.1.4	Business continuity planning framework	Control A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

A.14.1.5	Testing, maintaining and re-assessing business continuity plans	Control Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.
A.15 Compliance		
A.15.1 Compliance with legal requirements Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.		
A.15.1.1	Identification of applicable legislation	Control All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
A.15.1.2	Intellectual property rights (IPR)	Control Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
A.15.1.3	Protection of organizational records	Control Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
A.15.1.4	Data protection and privacy of personal information	Control Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
A.15.1.5	Prevention of misuse of information processing facilities	Control Users shall be deterred from using information processing facilities for unauthorized purposes.
A.15.1.6	Regulation of cryptographic controls	Control Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2 Compliance with security policies and standards, and technical compliance Objective: To ensure compliance of systems with organizational security policies and standards.		
A.15.2.1	Compliance with security policies and standards	Control Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
A.15.2.2	Technical compliance checking	Control Information systems shall be regularly checked for compliance with security implementation standards.

A.15.3 Information systems audit considerations Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.		
A.15.3.1	Information systems audit controls	Control Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
A.15.3.2	Protection of information systems audit tools	Control Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

Controles del Estándar ISO/IEC 27001, Secciones 5 a 15

A continuación, como referencia, se incluye una traducción no oficial de los controles del Estándar ISO/IEC 27001, Secciones 5 a 15.

5. POLÍTICA DE SEGURIDAD

5.1 Política de seguridad de la información.

Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

La gerencia debe establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

5.1.1 Documento de política de seguridad de la información.
La gerencia deber aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.

Esta política Debe distribuirse por toda la organización, llegando hasta a todos los destinatarios en una forma que sea apropiada, entendible y accesible.

5.1.2 Revisión de la política de seguridad de la información.
La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad.

6. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

6.1 Organización interna.

Gestionar la seguridad de la información dentro de la organización.

Debe establecerse una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información dentro de la organización.

Es conveniente organizar foros de gestión adecuados con las gerencias para aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar la implantación de la seguridad en toda la organización.

Si fuera necesario, debe facilitarse el acceso dentro de la organización a un equipo de consultores especializados en seguridad de la información. Deben desarrollarse contactos con especialistas externos en seguridad para mantenerse al día en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como tener un punto de enlace para tratar las incidencias de seguridad. Debe fomentarse un enfoque multidisciplinario de la seguridad de la información.

6.1.1 Compromiso de la gerencia con la información.

La gerencia debe apoyar activamente en la seguridad dentro de la organización a través de direcciones claras demostrando compromiso, asignaciones explicitas y reconocimiento de las responsabilidades de la seguridad de información.

La gerencia debe identificar las necesidades de asesoría especialista ya sea interna o externa, revisando y coordinando los resultados de la esta a través de la organización.

Dependiendo del tamaño de la organización, estas responsabilidades pueden ser manejadas por un forum gerencial dedicado o por un cuerpo gerencial existente, como el consejo directivo.

6.1.2 Coordinación de la seguridad de la información.

La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la organización con roles relevantes y funciones de trabajo.

6.1.3 Asignación de responsabilidades sobre seguridad de la información.

Deben definirse claramente las responsabilidades.

La asignación de responsabilidades sobre seguridad de la información deben hacerse en concordancia con la información de la política de seguridad. Las responsabilidades para la protección de activos individuales y para llevar a cabo procesos de seguridad específicos deben ser claramente identificadas. Esta asignación, debe completarse, dónde sea necesario, con una guía más detallada para ubicaciones, sistemas o servicios específicos. Debe definirse claramente las responsabilidades locales para activos físicos y de información individualizados y los procesos de seguridad como, por ejemplo, el plan de continuidad del negocio.

Los propietarios de los activos de información pueden delegar sus responsabilidades de seguridad en directivos a título individual o en proveedores de servicios. Sin embargo, el propietario sigue manteniendo la responsabilidad última sobre la seguridad del activo y Debe estar capacitado para determinar que cualquier responsabilidad delegada se ha cumplido correctamente.

6.1.4 Proceso de autorización de recursos para el tratamiento de la información.

Debe establecerse un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información.

6.1.5 Acuerdos de confidencialidad.

Requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información deben ser identificadas y revisadas regularmente.

Confidencialidad o acuerdos de no divulgación deben anexar los requerimientos para proteger información confidencial usando términos ejecutables legales.

Basado en los requerimientos de la seguridad de una organización, otros elementos pueden ser necesarios en una acuerdo de confidencialidad o de no-acceso.

Los acuerdos de confidencialidad y de no-acceso deben conformarse con todas las leyes aplicables y las regulaciones para la jurisdicción a la cual aplica (véase el inciso 15.1.1)

Los requerimientos para acuerdos de confidencialidad y de no-acceso deben ser revisados periódicamente y cuando ocurran cambios que influyan en estos requerimientos.

6.1.6 Contacto con autoridades.

Deben ser mantenidos contactos apropiados con autoridades relevantes.

Las organizaciones deben de tener procedimientos instalados que especifiquen cuando y por que autoridades deben ser contactados y como los incidentes identificados en la seguridad de información deben ser reportados de una manera oportuna si se sospecha que las leyes han sido rotas.

Las organizaciones bajo ataque desde el Internet pueden necesitar de terceros (proveedor del servicio de Internet u operadores de telecomunicaciones) para tomar acción contra la fuente de ataque.

Mantener dichos contactos puede ser un requerimiento para apoyar la gestión de los incidentes de seguridad de la información (sección 13.2) o la continuidad del negocio y la contingencia del planeamiento (sección 14). Contactos con cuerpos regulatorios son también útiles para anticiparse y prepararse a próximos cambios en la ley o en las regulaciones, que deben ser seguidos por la organización. Contactos con otras autoridades incluyen utilidades, servicios de emergencia, seguridad y salud, como por ejemplo los bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (en conexión con la línea de ruta y la disponibilidad), proveedores de agua (en conexión con instalaciones de refrigeración para el equipo).

6.1.7 Contacto con grupos de interés especial.

Deben mantenerse contactos apropiados con grupos de interés especial u otros especialistas en foros de seguridad y asociaciones profesionales.

6.1.8 Revisión independiente de la seguridad de la información.

El alcance de la organización para gestionar la seguridad de información y su implementación (objetivos de control, controles, políticas, procesos y procedimientos para seguridad de información) deben ser revisados independientemente en intervalos planificados o cuando cambios significativos a la puesta en marcha de la seguridad ocurran.

6.2 Entidades externas.

Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

La seguridad de la información de la organización y las instalaciones de procesamiento de la información no deben ser reducidas por la introducción de un servicio o producto externo.

Debe controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización.

Cuando el negocio requiera dicho acceso de terceros, se debe realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control Deben definirse y aceptarse en un contrato: con la tercera parte.

6.2.1 Identificación de riesgos relacionados con entidades externas.

Los riesgos a la información de la organización y a las instalaciones del procesamiento de información desde los procesos del negocio que impliquen a terceros deben ser identificados y se debe implementar controles apropiados antes de conceder el acceso.

6.2.2 Tratamiento de la seguridad cuando se trabaja con clientes.

Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información o a los activos de la organización.

Los requerimientos de seguridad relacionados con el acceso a los activos de la organización de los clientes pueden variar considerablemente dependiendo de las instalaciones del procesamiento de información y la información a la que se accede. Estos requerimientos en la seguridad pueden ser anexados usando acuerdos con los clientes, que contienen todos los riesgos identificados y los requerimientos de seguridad.

Los acuerdos con terceros también pueden implicar a otras partes. Estos acuerdos garantizando acceso a terceros deben incluir permisos para la designación de otras partes y condiciones para su acceso y su inclusión.

6.2.3 Requisitos de seguridad en contratos con terceras personas.

Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, debe cubrir todos los requisitos de seguridad relevantes.

7. GESTIÓN DE ACTIVOS

7.1 Responsabilidad por los activos.

Mantener una protección adecuada sobre los activos de la organización.

Todos los activos deben ser considerados y tener un propietario asignado.

Deben identificarse los propietarios para todos los activos importantes, y se debe asignar la responsabilidad del mantenimiento de los controles apropiados. La responsabilidad de la implantación de controles debe delegarse. Pero la responsabilidad debe mantenerse en el propietario designado del activo.

7.1.1 Inventario de activos.

Todos los activos deben se claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.

7.1.2 Propiedad de los activos.

Toda la información y los activos asociados con el proceso de información deben ser poseídos por una parte designada de la organización.

7.1.3 Uso aceptable de los activos.

Las reglas para un uso aceptable de la información y de los activos asociados con las instalaciones del procesamiento de la información deben ser identificadas, documentados e implementadas.

Reglas específicas o guías deben ser provistas por la gerencia relevante. Empleados, contratistas y usuarios de terceros usando o teniendo acceso a los activos de la organización deben estar al tanto de los limites existentes para el uso de la información de la organización y de los activos asociados con las instalaciones de procesamiento de información y recursos.

Ellos deben ser responsables del uso de cualquier recurso del procesamiento de información y de cualquier otro uso parecido bajo su responsabilidad.

7.2 Clasificación de la información.

Asegurar un nivel de protección adecuado a los activos de información.

La información debe clasificarse para indicar la necesidad, prioridades y grado de protección.

La información tiene grados variables de sensibilidad y criticidad. Algunos elementos de información pueden requerir un nivel adicional de protección o un uso especial. Debe utilizarse un sistema de clasificación de la información para definir un conjunto de niveles de protección adecuados, y comunicar la necesidad de medidas de utilización especial.

7.2.1 Lineamientos de clasificación.

La información debe clasificarse en función de su valor, requisitos legales, sensibilidad y criticidad para la organización.

El nivel de protección puede ser determinado analizando la confidencialidad, integridad y disponibilidad u otro requisito para la información considerada.

7.2.2 Etiquetado y manejo de la información.

Es importante definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización.

El marcado y la manipulación segura de la información clasificada es un requisito clave para acuerdos de información compartida. Las etiquetas físicas son una forma común de marcado.

Sin embargo, algunos activos de información, como documentos electrónicos, no pueden ser físicamente marcados por lo que medios electrónicas para marcar deben ser usadas. Por ejemplo, etiquetas de notificación pueden aparecer en la pantalla. Donde el marcado no se fiable, otras formas de designar la clasificación de la información pueden aparecer.

8. SEGURIDAD EN RECURSOS HUMANOS

8.1 Antes del empleo.

Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y que sean adecuados para los roles para los que han sido considerados, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones.

Las responsabilidades de la seguridad se deben tratar antes del empleo en funciones adecuadas descritas y en términos y condiciones del empleo.

Todos los candidatos para empleo, contratistas y usuarios de terceros deben ser adecuadamente seleccionados, especialmente para trabajos sensibles.

Empleados, contratistas y terceros que utilizan las instalaciones del procesamiento de información deben firmar un acuerdo de confidencialidad.

8.1.1 Roles y responsabilidades.

Las funciones y responsabilidades de los empleados, contratistas y terceros deben ser definidas y documentadas en concordancia con la política de seguridad de la organización.

8.1.2 Selección.

Se debe llevar listas de verificación anteriores de todos los candidatos para empleo, contratistas y terceros en concordancia con las leyes , regulaciones y la ética, al igual que proporcionalmente a los requerimientos del negocio, la clasificación de la información ha ser acezada y los riesgos percibidos.

La organización debe considerar realizar una comprobación mas detallada a largo plazo de la persona cuando acceda por su empleo, en contratación inicial o en promoción, a recursos de tratamiento de la información y en particular trate información sensible, por ejemplo, información financiera o altamente confidencial.

8.1.3 Términos y condiciones de empleo.

Como parte de su obligación contractual, empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de empleo el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

La organización debe asegurarse que los empleados, contratistas y usuarios de terceros acepten los términos y condiciones referentes a la seguridad de información apropiada a la naturaleza y al grado de acceso que tendrán con los activos de la organización asociados a los sistemas y a los servicios de información.

Donde sea apropiado, las responsabilidades contenidas en los términos y condiciones del empleo deben continuar por un periodo definido después del termino del este (véase también 8.3).

8.2 Durante el empleo.

Asegurar que los empleados, contratistas, y usuarios de terceros estén consientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo y de reducir el riesgo de error humano.

Las responsabilidades de la gerencia deben ser definidas para asegurar que la seguridad sea aplicable a través del empleo de un individuo dentro de la organización.

Un nivel adecuado de conocimiento, educación y entrenamiento en procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información debe ser provista a todos los empleados, contratistas y usuarios de terceros con el fin de minimizar los posibles riesgos de seguridad. Se debe establecer un proceso disciplinario formal para maniobrar aberturas de seguridad.

8.2.1 Gestión de responsabilidades.

La gerencia debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.

8.2.2 Capacitación y educación en la seguridad de información.

Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

El conocimiento sobre seguridad, educación y actividades de entrenamiento deben ser de acuerdo y pertinentes al papel de la persona, las responsabilidades y habilidades deben incluir la información sobre las amenazas conocidas que permitan informar al consejo de seguridad superior a través de los caminos apropiados los eventos relacionados con la seguridad de información (véase el inciso 13.1).

8.2.3 Proceso disciplinario.

Debe existir un proceso formal disciplinario para empleados que han cometido un apertura en la seguridad.

El proceso disciplinario debe ser usado también como un impedimento para prevenir que los empleados, contratistas y usuarios de terceros violen las políticas y procedimientos organizacionales, así como cualquier otra apertura en la seguridad.

8.3 Terminación o cambio del empleo

Asegurar que los empleados, contratistas e usuarios de terceros salgan de la organización o cambien de empleo de una forma ordenada.

Las responsabilidades se establecen con el fin de asegurarse que la salida de la organización de los empleados, contratistas e usuarios de terceros este manejada y que el retorno de todo el equipo y el retiro de todo derecho acceso este completado.

Cambios en la responsabilidad y empleos dentro de la organización deben ser manejados como la terminación de la respectiva responsabilidad o empleo, en línea con esta sección y cualquier nuevo empleo debe ser manejado como se describió en la sección 8.1.

8.3.1 Responsabilidades de terminación.

Las responsabilidades para realizar la finalización de un empleo o el cambio de este deben ser claramente definidas y asignadas.

8.3.2 Devolución de activos.

Todos los empleados, contratistas y terceros deben retornar todos los activos de la organización que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo.

8.3.3 Eliminación de derechos de acceso.

Los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información deben ser removidos hasta la culminación del empleo, contrato o acuerdo, o debe ser ajustada en caso de cambio.

En ciertas circunstancias los derechos de acceso pueden ser asignados en base a la disponibilidad hacia mas personas que el empleado, contratista o usuario de tercero saliente. En estas circunstancias, los individuos salientes deben ser removidos de cualquier lista de grupos de acceso y se deben realizar arreglos para advertir a los demás empleados, contratistas y usuarios de terceros involucrados de no compartir esta información con la persona saliente.

En casos de gerencia terminada, contrariedad con los empleados, contratistas o usuarios de terceros pueden llevar a corromper información deliberadamente o a sabotear las instalaciones del procesamiento de información. En casos de renuncia de personal, estos pueden ser tentados a recolectar información para usos futuros.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1 Áreas seguras.

Evitar accesos no autorizados, daños e interferencias contra los locales y la Información de la organización.

Los recursos para el tratamiento de información crítica o sensible para la organización deben ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se debe dar protección física contra accesos no autorizados, daños e interferencias.

Dicha protección debe ser proporcional a los riesgos identificados.

9.1.1 Perímetro de seguridad física.

Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información e recursos de procesamiento de información.

Un área de seguridad puede ser una oficina cerrada o diversos espacios rodeados por una barrera continua de seguridad interna. Barreras adicionales y perímetros para controlar el acceso físico pueden ser necesarios entre áreas con requisitos de seguridad diferentes dentro del perímetro de seguridad.

Consideraciones especiales hacia la seguridad en el acceso físico deben ser dados a edificios donde existan establecidas organizaciones múltiples.

9.1.2 Controles de entrada físicos.

Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado.

9.1.3 Seguridad de oficinas, habitaciones y medios.

La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada.

9.1.4 Protección contra amenazas externas y ambientales.

Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.

9.1.5 Trabajo en áreas seguras.

Se debe diseñar y aplicar protección física y pautas para trabajar en áreas seguras.

Los arreglos para trabajar en áreas seguras deben incluir controles para los empleados, contratistas y usuarios de terceros que trabajen en dicha área, así como otras actividades de terceros que se lleven acabo ahí.

9.1.6 Áreas de acceso publico, entrega y cargas.

Se deben controlar las áreas de carga y descarga, y si es posible, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.

9.2 Seguridad del equipo.

Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.

El equipo debe estar físicamente protegido de las amenazas.

9.2.1 Ubicación y protección del equipo.

El equipo debe situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.

9.2.2 Servicios públicos.

Se deben proteger los equipos contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo.

Las opciones para lograr continuidad en el suministro de energía incluyen alimentación múltiple con el fin de evitar un punto simple de falla.

9.2.3 Seguridad en el cableado.

Se debe proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.

9.2.4 Mantenimiento de equipo.

Los equipos deben mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.

9.2.5 Seguridad del equipo fuera del local.

Se debe aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización tomando en cuenta los diversos riesgos a los que se esta expuesto.

Sólo la gerencia debe poder autorizar el uso de cualquier equipo para tratamiento de información fuera de los locales de la organización, sea quien sea su propietario.

Los equipos de almacenamiento y procesamiento de información incluyen todas las formas de computadores personales, organizadores, teléfonos celulares, tarjetas inteligentes, papel u otra forma que se utilice para trabajo en el domicilio o que pueda ser transportado fuera del lugar normal de trabajo.

9.2.6 Eliminación seguro o re-uso del equipo.

Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.

Los dispositivos de almacenamiento con información sensible se deben destruir físicamente o la información debe ser destruida, borrada o sobrescrita usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato.

Los dispositivos dañados que contienen data sensible pueden requerir una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.

La información puede ser comprometida a través de dispositivos descuidados o por el re uso del equipo (véase el inciso 10.7.2).

9.2.7 Traslado de propiedad.

El equipo, información o software no debe ser sacado fuera del local sin autorización.

También pueden realizarse notas de salida, emitidos para descubrir si existen salidas desautorizadas de la propiedad, para descubrir dispositivos magnetofónicos desautorizado, armas, etc., y previene su entrada en el lugar. Las notas de salida deben llevarse a cabo siguiendo la legislación pertinente y las regulaciones. Los individuos deben ser conscientes de que estos documentos se emiten solo con la autorización apropiada y los requisitos legales y reguladores.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Procedimientos y responsabilidades operacionales.

Asegurar la operación correcta y segura de los recursos de tratamiento de información.

Se deben establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

10.1.1 Procedimientos de operación documentados.

Se deben documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.

Se deben preparar procedimientos documentados para las actividades de administración del sistema y cualquier cambio que se deba realizar debe ser autorizado por la gerencia. Donde
sea técnicamente viable, los sistemas de información deben ser gestionados consistentemente usando los mismos procedimientos, herramientas y recursos.

10.1.2 Gestión de cambio.

Se deben controlar los cambios en los sistemas y recursos de tratamiento de información.

El control inadecuado de los cambios a los sistemas y recursos de procesamiento de información es una causa común de fallas del sistema o de seguridad. Cambios en el ambiente operacional, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la de operación, pueden impactar en la fidelidad de las aplicaciones (véase el inciso 12.5.1).

Los cambios a los sistemas operacionales deben realizarse solamente cuando existe una razón de negocio valida, como un incremento en el riesgo al sistema. Actualizando los sistemas con
la ultima versión de los sistemas operativos o aplicaciones, no siempre se encuentra en los intereses del negocio además de que puede introducir mayores vulnerabilidades e inestabilidad que la versión actual. También se puede necesitar de un entrenamiento adicional, costos de licencias, apoyo, mantenimiento y administración, y un nuevo hardware especialmente durante la migración.

10.1.3 Segregación de deberes.

Se deben segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional, o el de un mal uso de los activos de la organización.

10.1.4 Separación de los medios de desarrollo y operaciones.

La separación de los recursos para desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

Las actividades de desarrollo y prueba pueden causar serios problemas, por ejemplo, cambios no deseados en los archivos o en el entorno del sistema o fallos del sistema. En este caso es necesario mantener un entorno conocido y estable para poder realizar las pruebas significativas y evitar el acceso inapropiado del personal de desarrollo.

Si el personal de desarrollo y el de prueba tuvieran acceso al sistema de producción y a su información, podrían introducir un código no autorizado o no probado o alterar los datos operacionales. En algunos sistemas esta posibilidad podría utilizarse de forma indebida, para cometer fraudes o para introducir un código no probado o malicioso, lo que podría causar problemas operacionales serios.

10.2 Gestión de la entrega de servicio de terceros.

Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros.

La organización debe verificar la implementación de acuerdos, el monitoreo de la conformidad con los acuerdos y los cambios gestionados con el fin de asegurar que todos los servicios entregados cumplen con todos los requerimientos acordados con terceros.

10.2.1 Entrega de servicio.

Debemos asegurarnos que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluidas en el acuerdo de entrega de servicio externo sean implementados,
operados y mantenidos por la parte externa.

10.2.2 Monitoreo y revisión de los servicios de terceros.

Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorias deben ser llevadas a cabo regularmente.

En caso de outsourcing, la organización necesita estar al tanto que la ultima responsabilidad para el procesamiento de información realizada por un tercero recae en la organización.

10.2.3 Manejar los cambios en los servicios de terceros.

Cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes.

10.3 Planificación y aceptación del sistema.

Minimizar el riesgo de fallos de los sistemas.

Son necesarios una planificación y preparación para asegurar la disponibilidad de capacidad y de recursos adecuados para entregar el sistema de funcionamiento requerido.

Deben realizarse proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema.

Se debe establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los sistemas nuevos.

10.3.1 Gestión de capacidad.

El uso de recursos debe ser monitoreado y las proyecciones hechas de requisitos de capacidades adecuadas futuras para asegurar el sistema de funcionamiento requerido.

Para cada actividad que se este llevando a cabo o para una actividad nueva, los requisitos de capacidad deben ser identificados. Se debe aplicar el monitoreo de los sistemas con el fin de asegurar, y donde sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas. Controles de detección deben ser instalados pata detectar los problemas en un tiempo debido.

Las proyecciones deben tener en cuenta los requisitos de las nuevas actividades y sistemas, así como la tendencia actual y proyectada de tratamiento de la información en la organización.

Se requiere poner particular atención a cualquier recurso con tiempo de llegada largo o con costos altos; por esto, la gerencia debe monitorear la utilización de los recursos claves del sistema. Se deben identificar las tendencias de uso, particularmente relativas a las aplicaciones del negocio o a las herramientas de administración de sistemas de información.

Los administradores deben usar esta información para identificar y evitar los posibles cuellos de botella que puedan representar una amenaza a la seguridad del sistema o a los servicios al usuario, y para planificar la acción correctora apropiada.

10.3.2 Aceptación del sistema

Se deben establecer criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoradas y se deben desarrollar con ellos las pruebas adecuadas antes de su aceptación.

La aceptación puede incluir una certificación formal y un proceso de acreditación para verificar que los requisitos de seguridad han sido apropiadamente anexados.

10.4 Protección contra software malicioso y código móvil.

Proteger la integridad del software y de la información.

Se requieren ciertas precauciones para prevenir y detectar la introducción de software malicioso.

El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, “gusanos de la red”, “caballos de troya” y “bombas lógicas”. Los usuarios Deben conocer los peligros que puede ocasionar el software malicioso o no autorizado y los administradores Deben introducir controles y medidas especiales para detectar o evitar su introducción.

10.4.1 Controles contra software malicioso.

Se deben implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios.

El uso de dos o mas productos de software protegiéndonos contra códigos maliciosos a través del ambiente de procesamiento de información desde diferentes vendedores puede mejorar la efectividad de esta protección.

Los software que protegen contra códigos maliciosos pueden ser instalados para proveer actualizaciones automáticas de archivos de definición y para explorar los motores para asegurar que la protección se encuentre actualizada. En adición, este software puede ser instalado en cualquier escritorio para llevar a cabo verificaciones automáticas.

Se debe tener mucho cuidado al proteger contra la introducción de código malicioso durante el mantenimiento y los procedimientos de emergencia, ya que estos pueden pasar controles normales de protección.

10.4.2 Controles contra códigos móviles.

Donde el uso de código móvil es autorizado, la configuración debe asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y que se debe prevenir que este sea ejecutado.

El código móvil es un código de software que se transfiere desde una computadora a otra y luego ejecuta automáticamente y realiza una función especifica con poco o ninguna interacción del usuario. El código móvil esta asociado con un número de servicios middleware.

En adición para asegurar que los códigos móviles no contienen código malicioso, es esencial controlarlos con el fin de evitar un uso desautorizado o una interrupción del sistema, red o aplicaciones y otras ramas de la seguridad de información.

10.5 Respaldo (back-up).

Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

Se deben establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo (véase el inciso 14.1) haciendo copias de seguridad y ensayando su oportuna recuperación.

10.5.1 Back-up o respaldo de la información.

Se deben hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación.

Las copias de seguridad pueden automatizarse para aliviar el proceso de restauración. Deben probarse tales soluciones automatizadas suficientemente antes de la implementación y a intervalos regulares.

10.6 Gestión de seguridad en redes.

Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.

La gestión de la seguridad de las redes que cruzan las fronteras de la organización requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas.

Controles adicionales pueden ser requeridos también con el fin de proteger información sensible pasando sobre redes publicas.

10.6.1 Controles de red.

Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en transito.

10.6.2 Seguridad en los servicios de red.

Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización.

Los servicios de red incluyen la provisión de conexiones, servicios de red privados y redes de valor agregado así como soluciones manejadas de seguridad de redes como firewalls y sistemas de detección de intrusos. Estos servicios pueden alcanzar desde un simple ancho de bando no manejado hasta ofertas complejas de valor agregado.

10.7 Gestión de medios.

Prevenir acceso no autorizado, modificaciones, evitar daños a los activos e interrupciones de las actividades de la organización.

Los medios deben ser controlados y físicamente protegidos.

Se deben establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema, de daño, modificación, robo y acceso no autorizado.

10.7.1 Gestión de medios removibles.

Debe haber procedimientos para la gestión de los medios informáticos removibles.

10.7.2 Eliminación de medios.

Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales.

10.7.3 Procedimientos de manejo de la información.

Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados.

10.7.4 Seguridad de la documentación de sistema.

Los documentación de sistemas debe ser protegida contra acceso no autorizado.

10.8 Intercambio de información.

Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones

Se deben realizar los intercambios sobre la base de acuerdos formales. Se deben controlar los intercambios de información y software entre organizaciones, que deben cumplir con toda la legislación correspondiente (véase el capítulo 15).

Se deben establecer procedimientos y normas para proteger la información de los medios en tránsito.

10.8.1 Procedimientos y Políticas de información y software.

Se deben establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación.

10.8.2 Acuerdos de Intercambio.

Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y terceros.

10.8.3 Medios físicos en tránsito.

Los medios conteniendo información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización.

10.8.4 Mensajes electrónicos.

La información implicado con la mensajería electrónica debe ser protegida apropiadamente.

10.8.5 Sistemas de Información Comerciales.

Se deben desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información de negocios.

10.9 Servicios de comercio electrónico.

Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

Las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo transacciones en línea y los requisitos para los controles. La integridad y disponibilidad de la información electrónica publicada a través de sistemas disponibles de publicidad deben ser también consideradas.

10.9.1 Comercio Electrónico.

La información envuelta en el comercio electrónico pasando a través de redes publicas, deben ser protegidas de actividad fraudulenta, disputas de contratos y de acceso y modificación no autorizada.

10.9.2 Transacciones en línea.

La información implicada en las transacciones en línea debe ser protegida para prevenir la transmisión incompleta, ruta equivocada, alteración no autorizada de mensajes, acceso no autorizado, duplicado no autorizado del mensaje o reproducción.

10.9.3 Información disponible públicamente.

La integridad de la información que se ha hecho disponible en un sistema público debe ser protegido para prevenir modificaciones no autorizadas.

10.10 Monitoreo.

Detectar las actividades de procesamiento de información no autorizadas.

Los sistemas deben ser monitoreados y los eventos de la seguridad de información deben ser grabadas. El registro de los operadores y el registro de averías debe ser usado para asegurar que los problemas del sistema de información sean identificados.

Una organización debe cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades.

El monitoreo del sistema debe ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad de un acceso a un modelo de política.

10.10.1 Registro de la auditoria.

Los registros de auditoria grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso.

10.10.2 Uso del sistema de monitoreo.

Los procedimientos para el uso del monitoreo de las instalación de procesamiento de información deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente.

10.10.3 Protección de la información del registro.

Las instalaciones de información de registro deben ser protegidas contra acciones forzosas u acceso no autorizado.

10.10.4 Registros de administrador y operador.

Las actividades del administrador y de los operadores del sistema deben ser registradas.

10.10.5 Registro de fallas.

Las averías deben ser registradas, analizadas y se debe tomar acciones apropiadas.

10.10.6 Sincronización de relojes.

Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo.

11. CONTROL DE ACCESO

11.1 Requerimiento comercial para el control de acceso.

Controlar los accesos a la información.

Se debe controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio.

Se deben tener en cuenta para ello las políticas de distribución de la información y de autorizaciones.

11.1.1 Política de control de acceso.

Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requerimientos de seguridad y del negocio.

11.2 Gestión de acceso del usuario.

Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.

Se debe establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Estos procedimientos deben cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se debe prestar especial atención, donde sea apropiado, al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

11.2.1 Inscripción del usuario.

Se debe formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.

11.2.2 Gestión de privilegios.

Debe restringirse y controlarse el uso y asignación de privilegios.

11.2.3 Gestión de la clave del usuario.

Se debe controlar la asignación de contraseñas por medio de un proceso de gestión formal.

11.2.4 Revisión de los derechos de acceso del usuario.

La gerencia debe establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios.

11.3 Responsabilidades del usuario.

Evitar el acceso de usuarios no autorizados y el compromiso o hurto de la información y de las instalaciones del procesamiento de información.

Una protección eficaz necesita la cooperación de los usuarios autorizados.

Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

Un escritorio limpio, así como una política de pantalla clara debe ser implementado con el fin de reducir el riesgo de acceso no autorizado o de daño a los papeles, medios e instalaciones del procesamiento de información.

11.3.1 Uso de clave.

Los usuarios deben seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas.

11.3.2 Equipo de usuario desatendido.

Los usuarios deben asegurar que los equipos informáticos desatendidos estén debidamente protegidos.

11.3.3 Política de pantalla y escritorio limpio.

Se debe adoptar una política de escritorio limpio para papeles y medios removibles de almacenamiento así como una política de pantalla limpia para instalaciones de procesamiento de información.

11.4 Control de acceso a redes.

Prevenir el acceso no autorizado de los servicios de la red.

Debe controlarse el acceso a los servicios a las redes internas y externas.

Hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

a) Interfaces adecuadas entre la red de la organización y las redes públicas o las privadas de otras organizaciones;

b) Mecanismos adecuados de autenticación para los usuarios y los equipos;

c) Control de los accesos de los usuarios a los servicios de información

11.4.1 Política sobre el uso de servicios en red.

Los usuarios sólo deben tener acceso directo a los servicios para los que estén autorizados de una forma específica.

11.4.2 Autenticación de usuario para conexiones externas

Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos.

11.4.3 Identificación del equipo en red.

Las identificaciones automáticas de equipo deben ser consideradas como medios para autentificar conexiones desde locales y equipos específicos.

11.4.4 Protección de puertos de diagnostico remoto.

Se debe controlar el acceso físico y logístico para diagnosticar y configurar puertos.

11.4.5 Segregación en redes.

Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes.

11.4.6 Control de conexión a las redes

Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deben basar en los requisitos de las aplicaciones del negocio (véase el inciso 11.1).

11.4.7 Control de routing de redes.

Se deben implementar controles de enrutamiento que garanticen que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso a las aplicaciones.

11.5 Control de acceso al sistema de operación.

Evitar accesos no autorizados a los computadores.

Las prestaciones de seguridad a nivel de sistema operativo se deben utilizar para restringir el acceso a los recursos del computador. Estos servicios deben ser capaces de:

a) Identificar y verificar la identidad de cada usuario autorizado en concordancia con una política definida de control de acceso.

b) Registrar los accesos satisfactorios y fallidos al sistema.

c) Registrar el uso de privilegios especiales del sistema.

d) Alarmas para cuando la política del sistema de seguridad sea abierta.

e) Suministrar mecanismos, adecuados de autenticación.

f) Cuando proceda, restringir los tiempos de conexión de usuarios.

11.5.1 Procedimientos de registro en el terminal.

El acceso a los servicios de información debe estar disponible mediante un proceso de conexión seguro.

11.5.2 Identificación y autenticación del usuario

Todos los usuarios deben disponer de un identificador único para su uso personal y debe ser escogida una técnica de autentificación adecuada para verificar la identidad de estos.

11.5.3 Sistema de gestión de claves.

Los sistemas de gestión de contraseñas deben proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas.

11.5.4 Uso de utilidades del sistema.

La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado.

11.5.5 Sesión inactiva.

Las sesiones se deben desactivar tras un periodo definido de inactividad.

11.5.6 Limitación de tiempo de conexión

Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo.

11.6 Control de acceso a las aplicaciones e información.

Prevenir el acceso no autorizado a la información contenida en los sistemas.

Se deben usar las facilidades de seguridad lógica dentro de los sistemas de aplicación para restringir el acceso.

Se deben restringir el acceso lógico al software y a la información sólo a los usuarios autorizados. Las aplicaciones deben:

a) Controlar el acceso de los usuarios a la información y las funciones del sistema de aplicación, de acuerdo con la política de control de accesos.

b) Protegerse de accesos no autorizados desde otras facilidades o software de sistemas operativos que sean capaces de eludir los controles del sistema o de las aplicaciones.

c) No comprometer la seguridad de otros sistemas con los que se compartan recursos de información.

11.6.1 Restricción al acceso a la información.

Se debe dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.

11.6.2 Aislamiento del sistema sensible.

Los sistemas sensibles pueden necesitar entornos informáticos dedicados (aislados).

11.7 Computación móvil y teletrabajo

Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

La protección requerida debe ser proporcional a los riesgos que causan estas formas específicas de trabajo. Se deben considerar los riesgos de trabajar en un entorno desprotegido cuando se usa informática móvil y aplicar la protección adecuada. En el caso del teletrabajo la organización debe implantar protección en el lugar del teletrabajo y asegurar que existen los acuerdos adecuados para este tipo de trabajo.

11.7.1 Computación móvil y comunicaciones

Se debe adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática.

11.7.2 Tele-trabajo

Se deben desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

12.1 Requisitos de seguridad de los sistemas.

Asegurar que la seguridad esté imbuida dentro de los sistemas de información.

Esto incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios. El diseño y la implantación de los procesos de negocio que soportan las aplicaciones o el servicio, pueden ser cruciales para la seguridad. Los requisitos de seguridad Deben ser identificados y consensuados antes de desarrollar los sistemas de información.

Todos los requisitos de seguridad deben ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

12.1.1 Análisis y especificación de los requerimientos de seguridad.

Los enunciados de los requisitos de negocio para sistemas nuevos o mejoras a sistemas existentes deben especificar los requisitos de control.

12.2 Procesamiento correcto en las aplicaciones.

Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las Aplicaciones.

Se deben diseñar dentro de las aplicaciones (incluidas las aplicaciones escritas por los usuarios) las medidas de control. Éstos deben incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

Se podrá requerir controles adicionales para sistemas que procesen o tengan impacto en información sensible, con mucho valor o críticas. Estos controles deben ser determinados en base a los requisitos de seguridad y la evaluación de riesgos.

12.2.1 Validación de datos de insumo.

Se deben validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas.

12.2.2 Control del procesamiento interno.

Se deben incorporar a los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados.

12.2.3 Integridad del mensaje.

Se debe identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones y se Deben de identificar e implementar controles apropiados.

12.2.4 Validación del data de output.

Se deben validar los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido correcto y apropiado a las circunstancias.

12.3 Controles criptográficos.

Proteger la confidencialidad, autenticidad o integridad de la información.

Se deben usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

12.3.1 Política de uso de los controles criptográficos.

La organización debe desarrollar e implementar una política de uso de las medidas criptográficas para proteger la información.

12.3.2 Gestión clave.

La gestión de claves debe criptográficas debe apoyar el uso de las técnicas criptográficas en la organización.

12.4 Seguridad de los archivos del sistema.

Asegurar la seguridad de los archivos del sistema.

El acceso a los archivos del sistema debe ser controlado y los proyectos de Tecnología de la Información (TI) y las actividades complementarias deben ser llevadas a cabo de una forma segura. Se debe tener cuidado de evitar la exposición de datos sensibles en ambientes de prueba.

12.4.1 Control del software operacional.

Deben existir procedimientos para controlar la instalación del software en sistemas operacionales.

12.4.2 Protección de la data de prueba del sistema.

Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados.

12.4.3 Control de acceso del código fuente al programa.

El acceso a los códigos de programas fuente debe ser restringido.

12.5 Seguridad en los procesos de desarrollo y soporte.

Mantener la seguridad del software de aplicación y la información.

Se deben controlar estrictamente los entornos del proyecto y de soporte.

Los directivos responsables de los sistemas de aplicaciones también lo deben ser de la seguridad del entorno del proyecto o su soporte. Se deben asegurar de la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo.

12.5.1 Procedimientos de control de cambios.

La implementación de cambios debe ser controlada usando procedimientos formales de cambio.

12.5.2 Revisión técnica de las aplicaciones después de cambios en el sistema operativo.

Se deben revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad.

12.5.3 Restricciones sobre los cambios en los paquetes de software.

No se recomiendan modificaciones a los paquetes de software. Se debe limitar a cambios necesarios y todos estos deben ser estrictamente controlados.

12.5.4 Filtración de Información.

Las oportunidades de fuga de información deben ser prevenidas.

12.5.5 Desarrollo de outsourced software.

El desarrollo externo del software debe ser supervisado y monitoreado por la organización.

12.6 Gestión de la vulnerabilidad técnica.

Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica debe ser implementada de una manera efectiva, sistemática y respetable con medidas tomadas para confirmar su efectividad. Estas consideraciones deben incluir los sistemas operativos y otras aplicaciones en uso.

12.6.1 Control de las vulnerabilidades técnicas.

Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas información utilizadas. Igualmente, se debe evaluar la exposición de la organización a tales vulnerabilidades y las medidas apropiadas para tratar a los riegos asociados.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

13.1 Reportando eventos y debilidades de la seguridad de información.

Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

El reporte formal de eventos y los procedimientos de escalada deben estar implementados. Todos los empleados, contratistas y terceros deben estar al tanto de los procedimientos para reportar los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales. Se les debe requerir que reporten cualquier evento o debilidad en la seguridad de información, lo más rápido posible, al punto de contacto designado.

13.1.1 Reporte de los eventos en la seguridad de información.

Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada

13.1.2 Reporte de debilidades en la información.

Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.

13.2 Gestión de incidentes y mejoras en la seguridad de la información.

Asegurar un alcance consistente y efectivo aplicado a la gestión de incidentes en la seguridad de información.

Las responsabilidades y procedimientos deben establecerse para maniobrar los eventos y debilidades en la seguridad de información de una manera efectiva una vez que hayan sido reportados. Un proceso de mejora continua debe ser aplicado en respuesta al monitoreo, evaluación y gestión general de los incidentes en la seguridad de información.

Donde se requiera evidencia, esta debe ser recolectada para asegurar el cumplimiento de los requisitos legales.

13.2.1 Responsabilidades y procedimientos.

Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información.

13.2.2 Aprendizaje de los incidentes en la seguridad de información.

Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.

13.2.3 Recolección de evidencia.

Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia
debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.

14. GESTIÓN DE CONTINUIDAD COMERCIAL

14.1 Aspectos de la seguridad de la información en la gestión de continuidad comercial.

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres.

Se debe implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallas de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación. Este proceso debe identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones.

Se deben analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio. Se Deben desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. La seguridad de información debe ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización.

La gestión de la continuidad del negocio debe incluir en adición al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales.

14.1.1 Incluir la seguridad de información en el proceso de gestión de la continuidad comercial.

Se debe instalar en toda la organización un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del negocio a través de la organización que trate los requerimientos en la seguridad de información necesarios para la continuidad del negocio.

14.1.2 Continuidad comercial y evaluación del riesgo.

Los eventos que pueden causar interrupciones a los procesos de negocio deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.

14.1.3 Desarrollar e implementar planes de continuidad incluyendo seguridad de la información.

Se deben desarrollar planes de mantenimiento y recuperación de las operaciones del negocio, para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos.

14.1.4 Marco referencial para la planeación para la continuidad comercial.

Se debe mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.

14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad comercial.

Los planes de continuidad del negocio se deben probar regularmente para asegurarse de su actualización y eficacia.

15. CUMPLIMIENTO

15.1 Cumplimiento con los requisitos legales.

Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

El diseño, operación, uso y gestión de los sistemas de información puede estar sujeto a requisitos estatutarios, regulatorios y contractuales de seguridad.

Se debe buscar el asesoramiento sobre requisitos legales específicos de los asesores legales de la organización, o de profesionales del derecho calificados. Los requisitos legales varían de un país a otro, al igual que en el caso de las transmisiones internacionales de datos (datos creados en un país y transmitidos a otro).

15.1.1 Identificación de la legislación aplicable.

Se deben definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información.

15.1.2 Derechos de propiedad intelectual (IPR).

Se deben implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladores y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario.

15.1.3 Protección de los registros organizacionales.

Se deben proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.

15.1.4 Protección de data y de la privacidad de la información personal.

La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación, las regulaciones y, si es aplicable, en las cláusulas contractuales.

Muchos países han establecido legislación colocando controles y medidas para el tratamiento y transmisión de datos personales (en general la información sobre personas físicas que pueda identificarlas). Dependiendo de la legislación nacional actual, estos controles y medidas suponen ciertas obligaciones a quien recoja, procese, ceda o comunique información personal, y puede restringir la posibilidad de transferir estos datos a otros países.

15.1.5 Prevención de mal uso de medios de procesamiento de información.

El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados.

Muchos países tienen una legislación de protección contra el mal uso de la informática. El uso de un computador con fines no autorizados puede llegar a ser un delito penal.

La legalidad de la supervisión y el control del uso de los recursos, varía de un país a otro y puede requerir que se avise de su existencia a los empleados o que se requiera su consentimiento. Cuando el sistema al que se ingrese sea utilizado como acceso publico (por ejemplo un servidor de red) y este sujeto a monitoreo de seguridad, debe exhibirse un mensaje indicándolo.

15.1.6 Regulación de los controles criptográficos.

Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.

Se debe pedir asesoramiento legal para asegurar el cumplimiento de la legislación del país en la materia, así como antes de trasladar a otro país información cifrada o controles de cifrado.

15.2 Cumplimiento de las políticas y estándares de seguridad, y el cumplimiento técnico.

Asegurar la conformidad de los sistemas con las políticas y normas de seguridad.

Se deben hacer revisiones regulares de la seguridad de los sistemas de información.

Éstas se deben atener a las políticas de seguridad apropiadas y se auditará el cumplimiento de las normas de implantación de la seguridad en los sistemas de información y en los controles de seguridad implementados.

15.2.1 Conformidad con la política de seguridad y los estándares de seguridad.

Los gerentes deben asegurarse que se cumplan correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad cumpliendo las políticas y estándares de seguridad.

15.2.2 Chequeo de cumplimiento técnico.

Se debe comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información.

15.3 Consideraciones de la auditoria de los sistemas de información.

Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema.

Se deben establecer controles para salvaguardar los sistemas operativos y las herramientas de auditoria durante las auditorias del sistema. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoria.

15.3.1 Controles de auditoria de sistemas de información.

Se deben planificar cuidadosamente y acordarse los requisitos y actividades de auditoria que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.

15.3.2 Protección de las herramientas de auditoria de sistemas de información.

Se deben proteger los accesos a las herramientas de auditoria de sistemas con el fin de prever cualquier posible mal uso o daño.