

## 6 - Aspectos Organizativos para la Seguridad

### Resumen Por:

- Edwin Marcelo Guzman Bueso
- Juan Marcos Gutierrez Ramos
- Hernan Payrumani Mamani

### Organización interna

El objetivo es gestionar la seguridad de la información dentro de la organización para lo cual debe establecerse una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información.

### Comité de gestión de seguridad de la información

*Control*, La gerencia debe apoyar activamente en la seguridad a través de direcciones claras demostrando compromiso, asignaciones explícitas y reconocimiento de las responsabilidades.

#### *Guía de implementación*

1. asegurar que las metas de la seguridad de información sean identificadas, relacionarlas con las exigencias organizacionales y que sean integradas en procesos relevantes;
2. formular, revisar y aprobar la política de seguridad de información;
3. revisión de la efectividad en la implementación de la política de información;
4. proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad;
5. proveer los recursos necesarios para la seguridad de información;
6. aprobar asignaciones de roles específicos y responsabilidades para seguridad de información a través de la organización;
7. iniciar planes y programas para mantener la conciencia en seguridad de información;
8. asegurar que la implementación de los controles de la seguridad de información es coordinada a través de la organización

### **Coordinación de la seguridad de la información**

*Control*, La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes.

*Guía de implementación*

1. asegurar que las actividades de seguridad sean ejecutadas en cumplimiento con la política de seguridad;
2. identificar como manejar los no cumplimientos;
3. aprobar metodologías y procesos para seguridad de información, como por ejemplo la evaluación del riesgo y la clasificación de información;
4. identificar cambios significativos de amenazas y exposición de información;
5. evalúa la adecuación y coordina la implantación de los controles de seguridad de la información;
6. promocionar efectivamente educación, entrenamiento y concientizar en seguridad de información, a través de la organización;
7. evaluar información de seguridad recibida de monitorear y revisar los incidentes de seguridad de información y recomendar acciones apropiadas en respuesta para identificar incidentes de seguridad de información.

### **Asignación de responsabilidades sobre seguridad de la información**

*Control*, Deberían definirse claramente las responsabilidades.

*Guía de implementación*

1. deberían identificarse claramente los activos y los procesos de seguridad asociados con cada sistema específico;
2. debería nombrarse al responsable de cada activo o proceso de seguridad, y deberían documentarse los detalles de esta responsabilidad;
3. deberían definirse y documentarse claramente los niveles de autorización.

### **Proceso de autorización de recursos para el tratamiento de la información**

*Control*, Debería establecerse un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información.

*Guía de implementación*

1. los nuevos medios deberían tener la aprobación adecuada de la gerencia de usuario, autorizando su propósito y uso. También debería obtenerse la aprobación del directivo responsable del mantenimiento del entorno de seguridad del sistema de información local, asegurando que cumple con todas las políticas y requisitos de seguridad correspondientes;
2. dónde sea necesario, se debería comprobar que el hardware y el software son compatibles con los demás dispositivos del sistema;
3. debería autorizarse y evaluarse el uso de medios informáticos personales, como laptops o aparatos móviles, para el tratamiento de la información de la organización así como los controles necesarios, ya que pueden introducir nuevas vulnerabilidades.

### **Acuerdos de confidencialidad**

*Control*, Requerimientos de confidencialidad o acuerdos de no divulgación para la protección de información deben ser identificadas y revisadas regularmente.

#### *Guía de implementación*

1. una definición de la información a ser protegida;
2. duración esperada del acuerdo, incluyendo casos donde la confidencialidad pueda necesitar ser mantenida indefinidamente;
3. acciones requeridas cuando un acuerdo sea finalizado;
4. responsabilidades y acciones de los signatarios para evitar acceso desautorizado a la información;
5. propiedad de la información, secretos del comercio y de la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial;
6. la permisión de utilizar información confidencial y los derechos del signatario para usar la información;
7. el derecho de auditar y monitorear actividades que impliquen información confidencial;
8. procesos para notificar y reportar acceso desautorizado a aberturas de información confidencial;
9. términos para que la información sea retornada o destruida en la cesación del acuerdo;  
y
10. acciones prevista que se tomará en caso de una abertura de este acuerdo.

### **Contacto con autoridades**

*Control*, Deben ser mantenidos contactos apropiados con autoridades relevantes.

*Guía de implementación*

1. Las organizaciones deben de tener procedimientos instalados que especifiquen cuando y por que autoridades deben ser contactados.
2. Las organizaciones bajo ataque desde el Internet pueden necesitar de terceros para tomar acción contra la fuente de ataque.

### **Contacto con grupos de interés especial**

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

*Guía de implementación*

1. mejorar el conocimiento sobre mejores practicas y estar actualizado con información relevante de seguridad;
2. asegurar que el entendimiento del ambiente de seguridad de información es actual y completo;
3. recibir alertas de detección temprana, advertencias y parches que para los ataques y a las vulnerabilidades;
4. ganar acceso a consejos especializados de seguridad de información;
5. compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades;
6. proveer puntos de enlaces convenientes cuando se trata con información de incidentes de seguridad

### **Revisión independiente de la seguridad de la información**

*Control*, El alcance de la organización para gestionar la seguridad de información y su implementación deben ser revisados independientemente en intervalos planificados o cuando cambios significativos a la puesta en marcha de la seguridad ocurran.

*Guía de implementación*

1. La revisión independiente debe ser iniciado por la gerencia.
2. Esta revisión debe ser llevado a acabo por individuos independientemente del área bajo revisión.

3. Los resultados de la revisión independiente deben ser registrados y reportados a la gerencia
4. Si la revisión independiente identifica que el alcance de la organización o la implementación de la gestión de seguridad de información es inadecuada o no complaciente con la dirección de seguridad de información establecida en la política, la gerencia debe considerar acciones correctivas.

## Seguridad en los accesos de terceras partes

El objetivo es 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.

### Identificación de riesgos por el acceso de terceros

*Control*, Los riesgos a la información 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.

#### *Guía de implementación*

1. Las instalaciones del procesamiento de la información a la que terceros requieren acceso;
2. El tipo de acceso que terceros tendrán a la información y a las instalaciones del procesamiento de información:
  - (a) acceso físico, por ejemplo oficinas o salas de ordenadores;
  - (b) acceso lógico, por ejemplo la base de datos de la organización o sistemas de información;
  - (c) conectividad de red entre la organización y terceros, por ejemplo la conexión permanente o acceso remoto;
  - (d) si el acceso esta ocurriendo en el sitio o fuera de el;
3. el valor y la sensibilidad de la información implicada, y es critico para operaciones de negocios;
4. los controles necesarios para proteger la información que no debe ser accesible a terceros;
5. el personero externo implicado en maniobrar la información de la organización;
6. como la organización o el personero autorizado para tener acceso puede ser identificado, la autorización verificada y que tan seguido necesita ser reconfirmada;
7. los diferentes significados y controles empleados por terceros cuando guarde, procese, comunique, comparta e intercambia información;

8. el impacto del acceso no disponible a terceros cuando sea requerido, y de terceros ingresando o recibiendo información inexacta o engañosa;
9. practicas y procedimientos para lidiar con incidentes y daños potenciales en la seguridad de información, y los términos y condiciones para continuar con el acceso a terceros en el caso de un incidente en la seguridad de información;
10. requisitos legales y regulatorios u otras obligaciones contractuales relevantes a terceros que deben ser tomadas en cuenta;
11. como los intereses de las partes interesadas pueden ser afectados por los acuerdos.

### **Requisitos de seguridad cuando sea trata con clientes**

*Control*, Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso.

#### *Guía de implementación*

1. protección de activos, incluyendo:
  - (a) procedimientos para proteger los activos de la organización, incluida la información y el software;
  - (b) procedimientos para determinar si ha ocurrido algún incremento del riesgo de los activos, por ejemplo, una pérdida o modificación de datos;
  - (c) medidas de integridad;
  - (d) restricciones en la copia o divulgación de la información;
2. la descripción del servicio o producto disponible;
3. las diferentes razones, requerimientos y beneficios para el acceso del cliente;
4. acuerdos sobre control de accesos, incluyendo:
  - (a) los métodos de acceso permitidos, así como el control y uso de identificadores únicos, como número de identificación ID y contraseñas;
  - (b) el procedimiento de autorización del acceso y privilegios a los usuarios;
  - (c) una declaración de que todo acceso que no esta explícitamente autorizado es prohibido;
  - (d) un proceso para revocar el derecho de acceso o interrumpir la conexión entre sistemas;
5. arreglos para reportar, notificar e investigar inexactitudes de información, incidentes y aberturas en la seguridad de información;

6. una descripción de cada servicio a ser disponible;
7. el nivel de servicio;
8. el derecho para controlar y revocar cualquier actividad relacionado con los activos de la organización;
9. las respectivas responsabilidades de la organización y de los clientes;
10. las responsabilidades en materia de legislación por ejemplo sobre protección de datos personales, teniendo especialmente en cuenta los diferentes sistemas legales nacionales si el contrato implica la cooperación con organizaciones de otros países;
11. los derechos de propiedad intelectual, protección contra copias y protección en tareas de colaboración.

### **Requisitos de seguridad en contratos de outsourcing**

*Control*, 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.

#### *Guía de implementación*

1. la política de información de seguridad;
2. los controles que aseguren la protección del activo, incluyendo:
  - (a) procedimientos para proteger los activos organizacionales, incluyendo información, software y hardware;
  - (b) controles cualquiera de protección física requerida y mecanismos;
  - (c) controles para asegurar la protección contra software malicioso;
  - (d) procedimientos para determinar si es que se compromete el activo, como la pérdida o modificación de la información, software y hardware, ha ocurrido;
  - (e) controles que aseguran el retorno o la destrucción de información y activos al final de o de un tiempo acordado durante el acuerdo;
  - (f) confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante de los activos;
  - (g) restricciones para copiar y divulgar información y el uso de acuerdos de confidencialidad;
3. capacitación en los métodos, procedimientos y seguridad para usuario y administrador;

4. asegurar el conocimiento del usuario para temas y responsabilidades de la seguridad de información;
5. disposición para transferir personal, cuando sea apropiado;
6. responsabilidades con respecto a la instalación y el mantenimiento del hardware y software;
7. una clara estructura y formatos de reportes;
8. un claro y especificado proceso de cambio de gestión;
9. política de control de acceso, cubriendo:
  - (a) las diferentes razones, requerimientos y beneficios que hacen el acceso por terceros necesario;
  - (b) métodos permitidos de acceso y el control y uso de identificadores únicos como ID de usuario y contraseñas;
  - (c) un proceso autorizado para acceso de usuarios y los privilegios;
  - (d) un requerimiento para mantener una lista de individuos autorizados a usar el servicio que ha sido disponible y cual son sus derechos y privilegios respecto a su uso;
  - (e) una declaración de que todos los accesos que no son explícitamente autorizados son prohibidos;
10. arreglos para reportar, notificar e investigar incidentes de la seguridad de información y aperturas de seguridad, como violaciones de los requerimientos establecidos en el acuerdo;
11. una descripción del producto o servicio ha ser provisto y una descripción de la información ha ser disponible de acuerdo con su clasificación de seguridad;
12. el objetivo de nivel de servicio y los niveles de no aceptación;
13. la definición del criterio de comprobación del funcionamiento, su control y su reporte;
14. el derecho de controlar y revocar cualquier actividad relacionada con los activos de la organización;
15. el derecho para auditar responsabilidades definidas en el acuerdo, para que dichas auditorias sean llevadas a cabo por terceros y para enumerar los derechos estatutarios de los auditores;
16. el establecimiento de un proceso de escalamiento para resolver problemas;

17. requisitos continuos de servicio, incluyendo medidas para la disponibilidad y la confiabilidad, en concordancia con las prioridades de negocio de la organización;
18. las respectivas responsabilidades de las partes del acuerdo;
19. responsabilidades con respecto a temas legales y como se asegura que los requerimientos legales sean conocidos, como por ejemplo la legislación de protección de datos, considerar especialmente diversos sistemas legislativos nacionales si el acuerdo implica la cooperación con organizaciones de otros países;
20. derechos de propiedad intelectual y de asignación de copyright y protección de cualquier otro trabajo de colaboración;
21. implicancias entre los sub-contratantes y terceros, y los controles de seguridad que estos sub-contratantes necesitan implementar;
22. condiciones para la renegociación/terminación de los acuerdos:
  - (a) un plan de contingencia debe llevarse a cabo en caso de que cualquiera de las partes desee cortar relaciones antes del término de los acuerdos;
  - (b) renegociación de los acuerdos si los requisitos de seguridad de la organización cambian;
  - (c) documentación actual de la lista de activos, licencias, acuerdos o derechos relacionados con ellos.