Auditoría Informática

Sistema de Gestión de Seguridad de la Información - SGSI

...

Sistema de Gestión de Seguridad de la Información

Razones para adoptar estándares

- Establecer medidas de seguridad de acuerdo al tipo de negocio
- Mejorar los controles sobre los riesgos de TI y su gestión
- Identificación de peligros y reducir los incidentes de seguridad de la información
- Optimizar los costos mediante medidas de seguridad de TI que preserven la operatividad de la empresa
- Demostrar en el mercado su responsabilidad y compromiso en materia de Seguridad de la Información, logrando competitividad Mejorar la efectividad de los procesos
- Cumplimentar con Mandatos y Leyes
- Satisfacer los requerimientos de los clientes a través de estándares aceptados mundialmente
- Conseguir menores gravámenes potenciales en costos de seguros
- Lograr responsabilidad basada en trabajo de equipo

Sistema de Gestión de Seguridad de la Información

SGSI - ISO 27001

Proceso sistemático, documentado y conocido por toda la organización. Y basado en un enfoque por riesgo de negocio, el SGSI es un modelo para el establecimiento, implementación, operación, control, revisión, mantenimiento y mejora de la seguridad de la información.

Sistema de Gestión de Seguridad de la Información

SGSI - ISO 27001

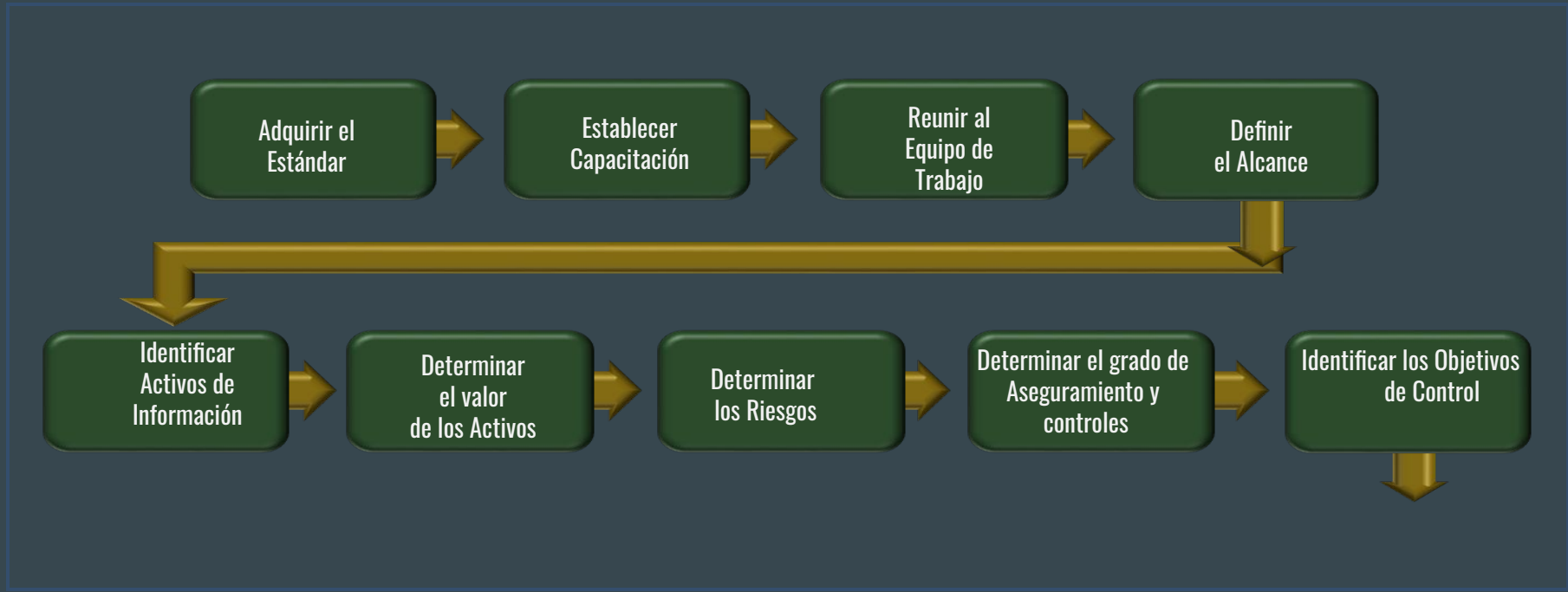
Es un estándar de seguridad genérico reconocido internacionalmente

Incluye un set de controles basado en las “mejores prácticas” en seguridad de información (complemento: ISO 27002)

El SGSI resultante puede ser auditado y certificado por un Ente de Certificación, añadiendo un valor significativo para la organización y su posicionamiento ante terceros

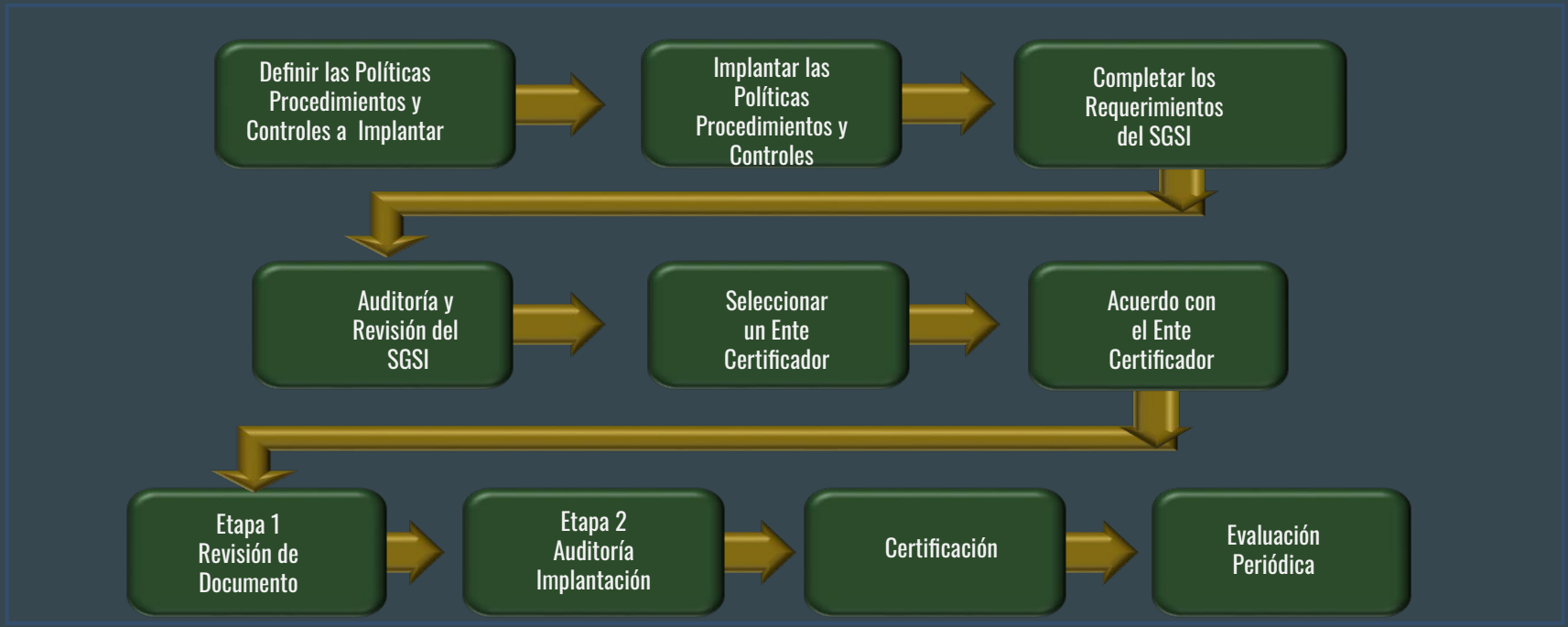
Sistema de Gestión de Seguridad de la Información

SGSI - ISO 27001



Sistema de Gestión de Seguridad de la Información

SGSI - ISO 27001



Sistema de Gestión de Seguridad de la Información

Ventajas

- Disminución de los riesgos
- Implementación de controles efectivos
- Protección de los activos de la organización y de los clientes
- Continuidad operativa y del negocio
- Prevención y atención inmediata de incidentes
- Cumplimiento de normas y regulaciones
- Concientización sobre el valor de la información de la organización
- Gerenciamiento optimizado ante normas, políticas y procedimiento

Sistema de Gestión de Seguridad de la Información ISO 27001

Consta de: 14 Dominios - 35 Objetivos de Control – 114 Controles de Aplicabilidad

Sistema de Gestión de Seguridad de la Información
Estructura de la Norma ISO 27001

4	Contexto de la organización
4.1	Comprender la organización y su contexto
4.2	Comprender las necesidades y expectativas de las partes interesadas
4.3	Determinar el alcance del sistema de gestión de la seguridad de la información
4.4	Sistema de gestión de la seguridad de la información
5	Liderazgo
5.1	Liderazgo y compromiso
5.2	Política
5.3	Roles organizacionales, responsabilidades y autoridades
6	Planificación
6.1	Acciones para abordar los riesgos y las oportunidades
6.2	Objetivos de seguridad de la información y planificación para lograrlos
7	Apoyo
7.1	Recursos
7.2	Competencias
7.3	Conocimiento
7.4	Comunicación
7.5	Información documentada
8	Operación
8.1	Control y planificación operacional
8.2	Evaluación de riesgo de la seguridad de la información
8.3	Tratamiento de riesgo de la seguridad de la información
9	Evaluación de desempeño
9.1	Monitoreo, medición, análisis y evaluación
9.2	Auditoría interna
9.3	Revisión de gestión
10	Mejora
10.1	No conformidades y acciones correctivas
10.2	Mejora continua

Sistema de Gestión de Seguridad de la Información

A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	*Control* Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de funciones	*Control* Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.
A.6.1.3	Contacto con autoridades	*Control* Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos especiales de interés	*Control* Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.
A.6.1.5	Seguridad de la información en la gestión de proyecto	*Control* Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.
A.6.2 Dispositivos móviles y trabajo remoto		
Objetivo: garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	*Control* Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles.
A.6.2.2	Trabajo remoto	*Control* Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.

Sistema de Gestión de Seguridad de la Información

6.2 Dispositivos móviles y teletrabajo

Objetivo: garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 Política de dispositivos móviles

Control

Se debería adoptar una política y medidas de seguridad de apoyo para administrar los riesgos que se presentan con el uso de dispositivos móviles.

Orientación sobre la implementación

Al utilizar dispositivos móviles, se debería tener cuidado de asegurar que la información comercial no se vea comprometida. La política de dispositivos móviles debería considerar los riesgos de trabajar con dispositivos móviles en entornos sin protección.

La política de dispositivos móviles debería considerar:

a) registro de dispositivos móviles;

b) requisitos para la protección física;

c) restricción de la instalación de software;

d) requisitos para las versiones de software de dispositivos móviles para la aplicación de parches;

e) restricción en la conexión a servicios de información;

f) controles de acceso;

g) técnicas criptográficas;

h) protección contra malware;

i) deshabilitación, borrado o bloqueo remoto;

j) respaldos;

k) uso de servicios web y aplicaciones web.

Se debería ser cuidadoso al utilizar dispositivos móviles en lugares públicos, salas de reuniones y otras áreas sin protección. Se debería contar con protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos, es decir, mediante el uso de técnicas criptográficas (ver cláusula 10) y mediante la obligación del uso de información de autenticación secreta (ver 9.2.4).

Los dispositivos móviles también se deberían proteger físicamente contra el robo, especialmente cuando se dejan, por ejemplo, en automóviles u otros medios de transporte, en habitaciones de hotel, centros de conferencia y lugares de reunión. Se debería establecer un procedimiento específico que considere los requisitos legales, de seguros y otros de seguridad de la organización para casos de robo o pérdida de dispositivos móviles. Los dispositivos que contengan información comercial importante, sensible o crítica no se deberían dejar sin supervisión y, donde sea posible, se deberían guardar con llave o se deberían utilizar bloqueos especiales para proteger a los dispositivos.

Se deberían organizar capacitaciones para el personal que utiliza dispositivos móviles y concientizarlos sobre los riesgos adicionales que genera esta forma de trabajo y los controles que se deberían implementar.

Donde la política de dispositivos móviles permita el uso de dispositivos móviles de propiedad privada, la política y las medidas de seguridad relacionadas también deberían considerar:

a) separación del uso privado y comercial de los dispositivos, incluido el uso de software para apoyar dicha separación y proteger los datos comerciales en un dispositivo privado;

b) proporcionar acceso a la información comercial solo después de que los usuarios hayan firmado un acuerdo de usuario final que reconozca sus deberes (protección física, actualización de software, etc.), renunciando a la propiedad de los datos comerciales, permitiendo el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no esté autorizado a utilizar el servicio. Esta política debería considerar la legislación de privacidad.

Otra información

Las conexiones inalámbricas de dispositivos móviles son similares a otros tipos de conexión de redes, pero tienen diferencias importantes que se deberían considerar al identificar los controles. Las diferencias típicas son:

a) algunos protocolos de seguridad inalámbricas son inmaduros y tienen debilidades conocidas;

b) es posible que la información almacenada en dispositivos no se respalde en los dispositivos móviles debido a un ancho de banda limitado o debido a que los dispositivos móviles pueden no estar siempre conectados cuando se han programado los respaldos.

Los dispositivos móviles generalmente comparten funciones comunes, es decir, el funcionamiento en redes, el acceso a internet, correo electrónico y el manejo de archivos con dispositivos de uso fijo. Los controles de seguridad de la información para los dispositivos móviles generalmente constan de aquellos adoptados en dispositivos de uso fijo y aquellos que abordan las amenazas que surgen de su uso fuera de las dependencias de la organización.

Sistema de Gestión de Seguridad de la Información

A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Accesos a las redes y a los servicios de la red	*Control* Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.

Sistema de Gestión de Seguridad de la Información

9.1.2 Acceso a redes y servicios de red

Control

Los usuarios solo deberían tener acceso a la red y a los servicios de red en los que cuentan con autorización específica.

Orientación sobre la implementación

Se debería formular una política en cuanto al uso de redes y servicios de red. Esta política debería cubrir:

a) las redes y los servicios de red a los que se tiene derecho de acceso;

b) procedimientos de autorización para determinar a quién se le permite acceder a qué redes y servicios con redes;

c) controles y procedimientos de administración para proteger el acceso a las conexiones de red y a los servicios de red;

d) los medios que se utilizan para acceder a las redes y a los servicios con redes (es decir, el uso de VPN o red inalámbrica);

e) requisitos de autenticación del usuario para acceder a los distintos servicios de red;

f) monitoreo del uso de servicios de red.

La política sobre el uso de servicios de red debería ser coherente con la política de control de acceso de la organización (ver 9.1.1).

Otra información

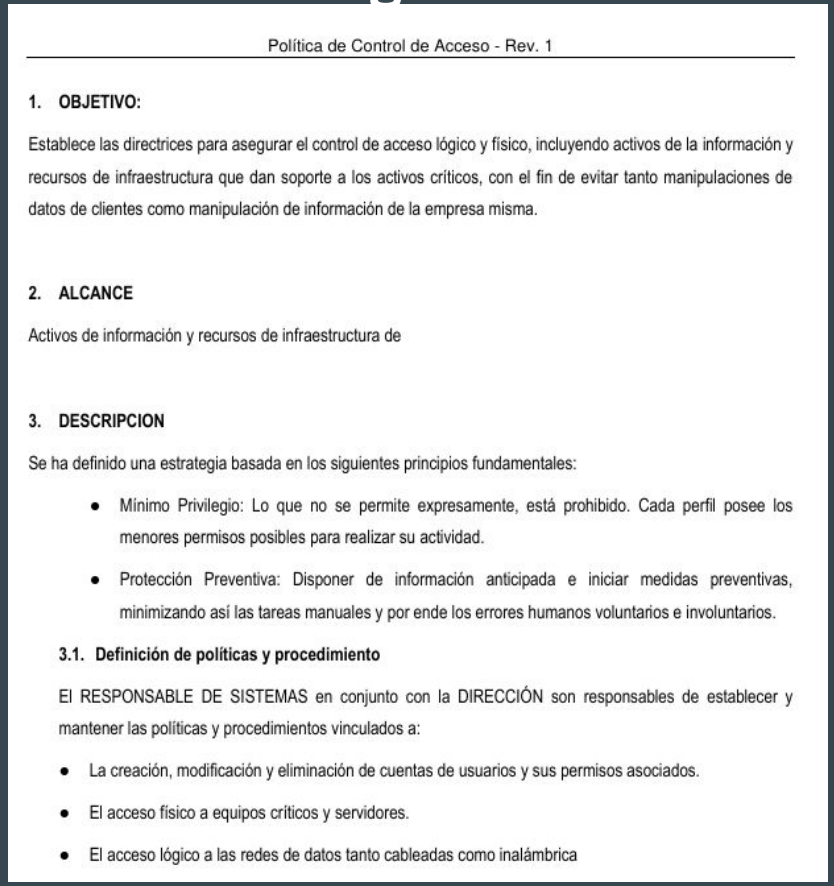
Las conexiones no autorizadas y no seguras a los servicios de red pueden afectar a toda la organización. Este control es de particular importancia para las conexiones de red a aplicaciones comerciales sensibles o críticas o para los usuarios en ubicaciones de alto riesgo, es decir, las áreas públicas o externas que se encuentran fuera de la administración y control de seguridad de la información de la organización.

Sistema de Gestión de Seguridad de la Información

ÍNDICE

1. OBJETIVO: 2
2. ALCANCE 2
3. DESCRIPCION 2
3.1. Definición de políticas y procedimiento 2
3.2. Autorización de accesos sobre activos 2
3.3. Seguridad de acceso lógico 2
3.3.1. Acceso a usuarios: 3
3.3.2. Usuarios Especiales y de Contingencia: 3
3.3.3. Análisis de pistas de auditoría: 3
3.3.4. Accesos Remotos: 3
3.3.5. Accesos a redes de datos: 4
3.3.6. Accesos a bases de datos: 4
3.4. Control de acceso físico 4

Sistema de Gestión de Seguridad de la Información



Política de Control de Acceso - Rev. 1

1. OBJETIVO:

Establece las directrices para asegurar el control de acceso lógico y físico, incluyendo activos de la información y recursos de infraestructura que dan soporte a los activos críticos, con el fin de evitar tanto manipulaciones de datos de clientes como manipulación de información de la empresa misma.

2. ALCANCE

Activos de información y recursos de infraestructura de

3. DESCRIPCION

Se ha definido una estrategia basada en los siguientes principios fundamentales:

- Mínimo Privilegio: Lo que no se permite expresamente, está prohibido. Cada perfil posee los menores permisos posibles para realizar su actividad.
- Protección Preventiva: Disponer de información anticipada e iniciar medidas preventivas, minimizando así las tareas manuales y por ende los errores humanos voluntarios e involuntarios.

3.1. Definición de políticas y procedimiento

El RESPONSABLE DE SISTEMAS en conjunto con la DIRECCIÓN son responsables de establecer y mantener las políticas y procedimientos vinculados a:

- La creación, modificación y eliminación de cuentas de usuarios y sus permisos asociados.
- El acceso físico a equipos críticos y servidores.
- El acceso lógico a las redes de datos tanto cableadas como inalámbrica

Sistema de Gestión de Seguridad de la Información

3.3.4. Accesos Remotos:

Se permitirán accesos remotos a por medio de conexiones Team Viewer bajo las siguientes condiciones

- Team Viewer debe estar siempre desactivado e iniciar el servicio únicamente cuando se requiera una tarea de mantenimiento programada.
- Toda actividad remota debe estar controlada/supervisada por el Responsable/Auxiliar de Sistemas.
- Activar la autenticación de dos factores en Team Viewer
- En la sección Asignación de cuentas configurar para vincular la cuenta de Team Viewer y usar dicha contraseña que debe cumplir la complejidad de contraseñas de cuentas de la organización.
- Team Viewer debe ejecutarse siempre en la última versión disponible.

Los accesos remotos deberán solicitarse a través de los procedimientos de gestión de cuentas de usuarios.

Sistema de Gestión de Seguridad de la Información

A.12.3 Respaldo		
Objetivo: Proteger en contra de la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.

Sistema de Gestión de Seguridad de la Información

12.3 Respaldo

Objetivo: brindar protección contra la pérdida de datos.

12.3.1 Respaldo de información

Control

Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada.

Orientación sobre la implementación

Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas.

La política de respaldo debería definir los requisitos de retención y protección.

Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios.

Al asignar un plan de respaldo, se deberían considerar los siguientes elementos:

a) se deberían producir registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;

b) el nivel (es decir, respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización;

c) los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal;

d) la información de respaldo debería tener un nivel de protección física y ambiental adecuada (ver cláusula 11) de acuerdo con las normas que se aplican en la ubicación principal;

e) los medios de respaldo se deberían probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debería combinar con una prueba de los procedimientos de restauración y se debería comprobar contra la restauración según sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y se debería verificar contra el tiempo de restauración necesario. Se deberían realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos;

f) en las situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante el cifrado.

Los procedimientos operacionales deberían monitorear la ejecución de respaldos y abordar las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos.

Se deberían probar regularmente las disposiciones de respaldos para los sistemas individuales a modo de garantizar que cumplen con los requisitos de los planes de continuidad del negocio. En el caso de los sistemas y servicios críticos, las disposiciones de respaldo deberían abarcar la información de todos los sistemas, aplicaciones y datos necesarios para recuperar al sistema completo en el caso de un desastre.

Se debería determinar el período de retención de la información esencial del negocio, considerando cualquier tipo de requisito para archivar copias que se deberían retener de manera permanente.

Sistema de Gestión de Seguridad de la Información

POL-005 Rev. 1 - Política de Backup, restauración y recuperación ante desastres

INDICE AUTOMATICO

1. Objetivo 2
2. Alcance 2
3. Referencias 2
4. Responsables 2
5. Desarrollo: 2
   - 5.1. Información a respaldar 2
   - 5.2. Tipo de backup 3
   - 5.3. Medio utilizado para resguardar la información y protección del mismo 3
   - 5.4. Periodicidad de backups y pruebas 4
     - 5.4.1. Backups 4
     - 5.4.2. Pruebas 5
   - 5.5. Recuperación ante desastres 5
   - 5.6. Tiempo de guarda de copias de respaldo 5
   - 5.7. Control por oposición 5
   - 5.8. Cumplimiento 5

Sistema de Gestión de Seguridad de la Información

1. Objetivo

El presente documento tiene como objetivo definir las políticas de respaldo de la información de ., así como la información respaldada con el fin de mantener la integridad y disponibilidad de la información y proteger los procesos críticos contra los efectos de fallas importantes y/o desastres, asegurando una recuperación oportuna.

2. Alcance

La política propuesta en el presente documento debe ser implementada para aquellos servidores y/o aplicaciones que contengan la información detallada en el punto 5.1 "Información a respaldar". La recuperación ante desastres se enfoca particularmente en recuperar información/servicios críticos para la operatoria diaria de la empresa.

3. Referencias

Norma ISO/IEC 27001:2013

Norma ISO/IEC 27002:2013, A.12.3-Backup

Ley nacional Nº 25326: Protección de los

4. Responsables

La Dirección es responsable de conocer la existencia de la presente política, y asignar las responsabilidades y recursos para su mantenimiento y ejecución. Asimismo, es su responsabilidad la aprobación de la presente política y sus modificaciones y verificar el cumplimiento de la presente política y los procedimientos asociados

5. Desarrollo:

5.1. Información a respaldar

Datos	Fuente	Descripción de la información a respaldar

5.2. Tipo de backup

Cada backup es efectuado de manera completa: se respalda la información en forma completa e histórica.

5.3. Medio utilizado para resguardar la información y protección del mismo

Los medios utilizados para el respaldo de la información son:

Localmente: en sistema de almacenamiento en red NAS (Network Attached Storage)

Sitio Remoto: un backup en la nube en una cuenta Dropbox corporativa propiedad de

backup de dispositivos móviles en cuenta de Gmail propiedad de

Las copias de backup gozan de los mismos requerimientos de seguridad (confidencialidad, integridad y disponibilidad) que la información original almacenada en los servidores, y en consecuencia deben ser protegidos apropiadamente.

Para esto, los respaldos locales en se encuentran en un sitio privado bajo las mismas condiciones del equipamiento informático con respecto la protección contra acceso no autorizado.

La sincronización al sitio remoto se realiza por canales cifrados SSL/TLS con doble factor de autenticación para el acceso a los mismos.

Sistema de Gestión de Seguridad de la Información

5.4. Periodicidad de backups y pruebas

5.4.1. Backups

El backup de los archivos de las aplicaciones Enaxis, NextLab y Tango será efectuado diariamente de manera automática, iniciando a las 2:00am, en horas donde la utilización de los recursos es considerablemente baja.

El backup de las bases de datos se realizará de la siguiente manera:

LIS (NextLab): Backup automático (dos veces: 11 de la noche y 11 de la mañana)

Tango: Backup automático 1 vez al día

Enaxis: Backup automático 1 vez al día

El backup de los programas se realizará de la siguiente manera, el primer día de cada mes, a las 22hs en Dropbox y a las 23.30hs en el NAS

LIS (Programa NextLab)

ENAXIS (Programa Enaxis)

ENAXIS Installer (Instaladores de Enaxis)

Intepub (Código web de la página de resultados y Enaxis)

El backup en Dropbox se realiza en el mismo que completa el backup de los archivos, una vez creada la copia local automáticamente comienza la copia en dropbox.

El backup de las grabaciones de las cámaras de videovigilancia se realiza diariamente en el NVR. Las grabaciones se almacenan entre 18 y 20 días, de acuerdo a la disponibilidad de almacenamiento que posee el equipo.

El backup de los dispositivos móviles se realizará de manera automática cuando el dispositivo se encuentre bloqueado, conectado a la corriente y a una red Wi-Fi. La configuración del mismo dependerá del sistema operativo del dispositivo, y se configurará para que el respaldo se realice en la cuenta de Gmail de

Los días martes y viernes a las 20hs se realiza un backup completo de todas las bases de datos y la carpeta Documentos en el NAS.

5.4.2. Pruebas

Semestralmente se deberán realizar pruebas de recuperación integrales, desde la restauración de archivos y base de datos de los sistemas instalados de servidor con las mismas caraterísticas técnicas que el servidor productivo o equipo destinado a tal fin, con su posterior comprobación de datos y funcionamiento de los sistemas.

5.5. Recuperación ante desastres

Anualmente se deberán realizar pruebas de recuperación completas del Servidor a un equipo destinado a tal fin, con su posterior recuperación de archivos y base de datos de los sistemas instalados y posterior comprobación de datos y funcionamiento de los sistemas.

5.6. Tiempo de guarda de copias de respaldo

De acuerdo a la Ley N° 25.236 de Protección de Datos Personales, la cual exige mantener los registros de acceso a datos por un tiempo de tres (3) años, se decide proteger las copias de respaldo por un lapso mayor o igual a este período.

5.7. Control por oposición

Anualmente se realizará un control por oposición sobre la realización de las actividades de backup. Este control será realizado la Dirección o personal designado las cuales deben ser personas independientes de la ejecución de las actividades de respaldo. El control consistirá en la revisión de los registros de backup generados durante su realización, así como durante las actividades de seguimiento. Como resultado se deberá obtener un informe de control, dentro del cual en caso de encontrarse fallas en los backups no resueltas por los responsables de backup, o falta de registro de las actividades de control establecidas en el presente procedimiento, se incluirán como incidentes.

5.8. Cumplimiento

Cualquier empleado o tercero contratado que viole la presente política, será sujeto al proceso disciplinario correspondiente, siendo posible la suspensión y/o finalización de un contrato o una relación laboral.