UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CLASIFICACIÓN DE LA INFORMACIÓN Y CONTROL DE ACCESO PARA UNA PYME

INFORME DE TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

OMAR GARCÍA ARIAS

TUTORA:

M.I. NORMA ELVA CHÁVEZ RODRÍGUEZ

2015

ÍNDICE

CAPÍTULO 1 1

1. INTRODUCCION 1

2. OBJETIVO 1

3. DESCRIPCIÓN DEL PUESTO DE TRABAJO 2

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 2

5. ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN - NORMA ISO/IEC 27001:2005 3

5.1 Descripción 3

5.2 Incorporación del proceso PDCA 3

5.3 Dominios implementados 5

5.3.1 Gestión de activos 5

5.3.1.1 Responsabilidad por los activos 5

5.3.1.2 Inventarios de activos de información 5

5.3.1.3 Propiedad de los activos 5

5.3.1.4 Clasificación de la información 5

5.3.1.5 Lineamientos de clasificación 6

5.3.2 Control de acceso 6

5.3.2.1 Política de control de acceso 6

5.3.2.2 Gestión del acceso del usuario 6

5.3.2.3 Inscripción del usuario 6

5.3.2.4 Gestión de privilegios 6

5.3.2.5 Gestión de la clave del usuario 6

5.3.2.6 Revisión de los derechos de acceso del usuario 6

5.3.2.7 Responsabilidades del usuario 6

5.3.2.8 Uso de utilidades del sistema 6

5.3.2.9 Sesión inactiva 7

5.3.2.10 Limitación de tiempo de conexión 7

5.3.2.11 Restricción al acceso a la información 7

5.3.2.12 Aislamiento del sistema sensible 7

6. DESARROLLO 7

6.1 Administración del proyecto 7

6.2 Fases del proyecto 7

6.2.1 Fase de Iniciación 7

6.2.2 Fase de Planificación 8

6.2.2.1 Reunión de Kickoff……..8
6.2.3 Fase de Ejecución.....9
6.2.3.1 Entrenamiento y concientización 9
6.2.3.2 Elaboración de procedimientos.....9
6.2.3.2.1 Procedimiento de control de accesos lógicos 10
6.2.3.2.2. Procedimiento de clasificación de la información.....16
6.2.3.3 Plataforma de hosteo…….....20
6.2.3.3.1 SharePoint…… 20
6.2.3.3.2 Control de acceso con SharePoint.....20
6.2.3.3.3 Implementación del ambiente 21
6.2.3.3.4 Metamodelo de los sitios de la intranet.....23
6.2.3.3.5 Instructivos para la administración de la intranet 23
6.2.3.3.5.1 Instructivo creación de carpetas y permisos 23
6.2.3.3.5.2 Instructivo copias de seguridad 33
6.2.3.3.5.3 Instructivo creación de subsitios 38
6.2.3.3.5.4 Instructivo creación de plantillas 47
6.2.4 Fase de Seguimiento y control 54
6.2.5 Fase de Cierre.....54
6.2.5.1 Lista maestra de documentos.....55
7. MEJORA CONTINUA 55
7.1 Revisión de las políticas de Seguridad de la Información 55
8. RESULTADOS 56
9. CONCLUSIONES 56
A. Glosario 57
B. BIBLIOGRAFÍA Y MESOGRAFÍA 58

CLASIFICACIÓN DE LA INFORMACIÓN Y CONTROL DE ACCESO PARA UNA PYME

CAPÍTULO 1

1. INTRODUCCION

El dinamismo de las empresas occidentales se crea en medio de un entorno competitivo, motivado por la necesidad del desarrollo continuo. Dicho desarrollo responde a la visión de utilidad de la Dirección General y sus objetivos comerciales, visualizando las posibilidades de crecimiento futuro. Un signo de este desarrollo empresarial fue la creación de un área de seguridad de la información, que pueda brindar respuesta a la necesidad de la organización, la cual es proveer un servicio de consultoría y auditoría de seguridad de la información, bajo el estándar internacional ISO/IEC 27001:2005.

La organización busca ser una empresa mexicana que brinde a las organizaciones servicios especializados de Auditoría y Consultoría en Seguridad de Tecnologías de la Información (TI) y establece dentro de su Manual de Gestión de Seguridad de la Información:

1. Manifestar el compromiso de la Dirección General con la seguridad de la información.
2. Definir el alcance del Sistema de Gestión de Seguridad de la Información y describir claramente la interacción entre los procesos asociados con el cumplimiento de los requerimientos del Sistema de Gestión de Seguridad de la Información.
3. Comunicar la política y objetivos de Seguridad de la Información, sus procedimientos y requisitos del Sistema de Gestión de Seguridad de la Información.
4. Proporcionar las bases documentadas para auditar al Sistema de Gestión de Seguridad de la Información.

Este reporte describe cada una de las actividades asignadas, llevadas a cabo para cumplir con las expectativas mencionadas anteriormente.

2. OBJETIVO

Diseñar, establecer e implementar mecanismos de seguridad de la información que ofrezcan un correcto manejo de la información bajo estándares internacionales, documentados en un Manual de Gestión de Seguridad de la Información que incluya un procedimiento de gestión de accesos lógicos, un procedimiento de clasificación de la información. Adicionalmente, administrar una plataforma de colaboración empresarial donde se provea un servicio de hosteo y administración del repositorio de la organización.

3. DESCRIPCIÓN DEL PUESTO DE TRABAJO

El consultor de Seguridad de la Información debe realizar la documentación e implementación de los controles informáticos y contar con el conocimiento preciso de los requisitos y la metodología de implementación del sistema de gestión de la seguridad de información, ser proactivo en la ejecución de actividades, tener conocimientos claro de los procesos específicos para el alcance de un sistema general en los procesos de la organización y del funcionamiento de la tecnología.

3.1 Funciones principales

1. Participar y contribuir en la definición del plan de trabajo para la Oficina de Seguridad de la Información.

2. Cumplir con las políticas y procedimientos establecidos dentro de la empresa, los Sistemas de Gestión de Calidad y de Seguridad de la información.

3. Participar en la concientización, entrenamiento y formación sobre seguridad de la información a las partes interesadas.

4. Revisar la ejecución de los controles de seguridad de la información.

5. Identificar y realizar revisiones de posibles causas raíz de incidentes relacionados con la seguridad de la información.

6. Apoyar e identificar mejoras a los planes de continuidad del negocio.

7. Informar sobre posibles riesgos que afecten la seguridad de la información.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información ya se encuentra aprobada y autorizada por la Dirección General, asegurando que:

1. Es adecuada al propósito de la empresa.
2. Incluye un compromiso con requisitos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual.
3. Proporciona un marco de referencia para establecer y revisar los objetivos de Seguridad de la Información.
4. Es comunicada por diferentes medios a todo el personal, estos medios incluyen la inducción y seguimiento por parte de los Directores, Gerentes, Administradores de Proyectos, en coordinación con el Representante de la Dirección General.
5. Es revisada para su continua adecuación en períodos definidos, durante la revisión por la Dirección al Sistema de Gestión de Seguridad de la Información.

6. Los temas relacionados con el incumplimiento de los estatutos establecidos por Sistema de Gestión de Seguridad de la Información (SGSI) se encuentran descritos en el Reglamento Interno, del Sistema de Gestión de Calidad, y otros documentos contractuales.

5. ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN - NORMA ISO/IEC 27001:2005

5.1 Descripción

Este estándar internacional fue creado y desarrollado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

Se espera que la implementación de un SGSI se extienda de acuerdo a las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

La definición del enfoque de valuación de riesgos se realiza en función de la seguridad de la información.

5.2 Incorporación del proceso PDCA

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

Tabla 1. Tabla de definición del proceso PDCA.

Planear (establecer el SGSI)	Establecer la política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.

Chequear (monitorear y revisar el SGSI)	Evaluar y, si es posible, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

1. Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.

2. Implementar y operar controles para manejar los riesgos de la seguridad de la información.

3. Monitorear y revisar el desempeño y la efectividad del SGSI.

4. Mejora continuo con base en la medición del objetivo.

Este estándar internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado en términos de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

El SGSI asegura la selección adecuada de controles de seguridad que protejan los activos de información y generen confianza en las partes interesadas.

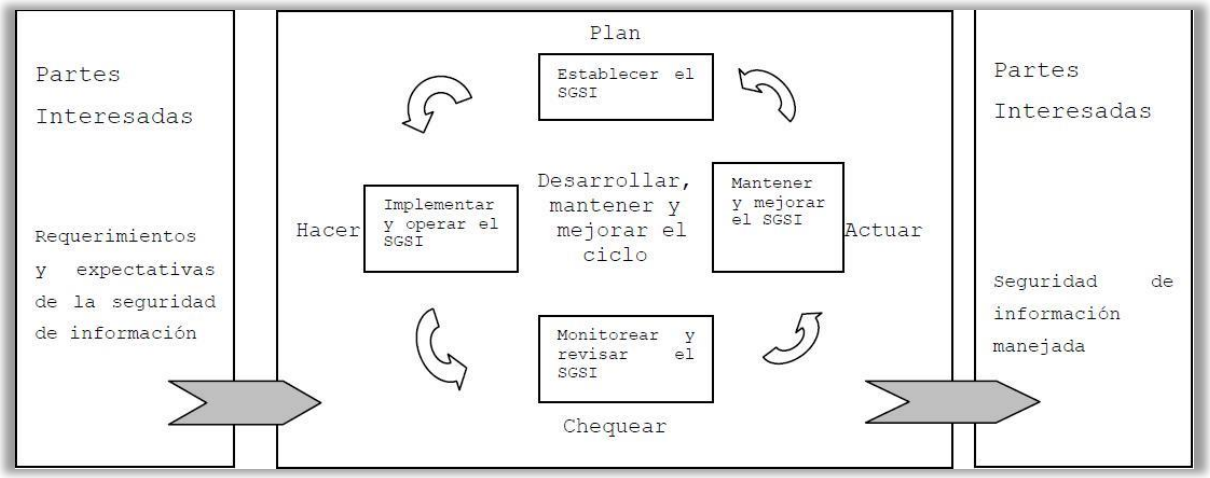


Figura 1. Modelo PDCA.

5.3 Dominios implementados

Este reporte incluye el establecimiento e implementación de dos dominios del estándar ISO/IEC 27001:2005, mismos que fueron solicitados por la Dirección General de la organización, como parte de una primera fase, los cuales son:

1. Gestión de activos - Clasificación de la Información.
2. Control de acceso.

5.3.1 Gestión de activos

5.3.1.1 Responsabilidad por los activos

EL objetivo es proporcionar protección adecuada a los activos de la organización.

5.3.1.2 Inventarios de activos de información

Los activos de información deben de encontrarse identificados; y debe de contarse con un inventario de los activos importantes.

5.3.1.3 Propiedad de los activos

La información debe ser ‘propiedad’ de una parte designada de la organización (Por propiedad se refiere a la responsabilidad gerencial para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos).

5.3.1.4 Clasificación de la información

El objetivo es garantizar que la información reciba un nivel adecuado de protección.

5.3.1.5 Lineamientos de clasificación

La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.

5.3.2 Control de acceso

Tiene como objetivo controlar acceso a la información propiedad la organización y aquella generada o de uso con otros interesados.

5.3.2.1 Política de control de acceso

Debe ser establecida y documentada con base en los requerimientos de seguridad y comerciales de la organización.

5.3.2.2 Gestión del acceso del usuario

El objetivo gestionar el acceso del usuario es garantizar accesos autorizados y evitar accesos no autorizados a los sistemas de información.

5.3.2.3 Inscripción del usuario

Debe existir un procedimiento formal para la inscripción y desinscripción para otorgar acceso a todos los sistemas y servicios de información.

5.3.2.4 Gestión de privilegios

La asignación y uso de privilegios de acceso debe ser controlada por los responsables (propietarios) de la información, a través de la autorización de los perfiles de acceso.

5.3.2.5 Gestión de la clave del usuario

La asignación de claves debe realizarse por medio de un proceso formal.

5.3.2.6 Revisión de los derechos de acceso del usuario

Deben realizarse revisiones a los derechos de acceso de los usuarios planeada y regularmente por medio de un proceso formal.

5.3.2.7 Responsabilidades del usuario

Tiene como objetivo evitar el acceso de usuarios no autorizados. Así como el seguimiento de las buenas prácticas de seguridad en la selección y uso de claves.

5.3.2.8 Uso de utilidades del sistema

Debe controlarse el uso de programas de software que puedan superar al sistema y los controles de aplicación.

5.3.2.9 Sesión inactiva

Deben ser cerradas las sesiones inactivas, en un periodo previamente establecido.

5.3.2.10 Limitación de tiempo de conexión

Deben ser limitados los tiempos de conexión.

5.3.2.11 Restricción al acceso a la información

Debe ser restringido el acceso del personal de soporte al sistema de información, de acuerdo lo establecido por el procedimiento formal correspondiente.

5.3.2.12 Aislamiento del sistema sensible

Los sistemas sensibles deben encontrarse en un ambiente de cómputo aislado.

CAPÍTULO 2

6. DESARROLLO

6.1 Administración del proyecto

La administración de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo. Se logra mediante la aplicación e integración adecuadas de procesos de administración de proyectos, agrupados lógicamente, que conforman las 5 fases de procesos. Estas 5 fases de procesos son:

1. Iniciación
2. Planificación
3. Ejecución
4. Seguimiento y Control
5. Cierre

La administración del proyecto se llevó a cabo bajo la metodología de Administración de Proyectos del PMBOK (Project Management Body of Knowledge) V4.

6.2 Fases del proyecto

6.2.1 Fase de Iniciación

Los requisitos iniciales son presentados y se elabora el acta constitutiva, que es el documento que da inicio formal al proyecto.

6.2.2 Fase de Planificación

En esta fase se realiza la planeación del proyecto, en términos de tiempo y compromisos. Se describen todos los recursos con los que cuenta y requiere el proyecto y se crea un cronograma que describa el ciclo de vida del proyecto y sus actividades así como su duración. También se realiza una reunión de Kickoff con todos los interesados del proyecto donde se presenta la documentación y el análisis elaborado en esta fase. Lo anterior para dar inicio a la siguiente fase, la fase de ejecución.

ACTIVIDADES	TIEMPO						
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio
Fase de iniciación							
Requisitos iniciales							
Fase de Planificación							
Asignación de recursos							
Cronograma							
Reunión de Kickoff							
Fase de Ejecución							
Concientización del personal							
Generación de Procedimiento de Control de Acceso lógico							
Generación de Procedimiento de Clasificación de la información							
Generación de Lista maestra de documentos							
Fase de Seguimiento y Control							
Entregables mensuales							
Fase de Cierre							
Entrega de versiónes finales de procedimientos							
Entrega de Lista maestra de documentos							

Figura 2. Cronograma

6.2.2.1 Reunión de Kickoff

Las reuniones de Kickoff son instancias para reunir a todos y presentar de manera global los objetivos y planes a cumplir o, en el segundo caso, dar inicio al nuevo trabajo que se debe realizar.

El propósito de estas instancias es que los temas que comúnmente se tratan entre los directivos de las empresas lleguen a todos los involucrados, logrando transversalidad y alineamiento de acciones en un fin común. Si se comunican correctamente cuáles son los planes y estrategias anuales, además de dejar claros los objetivos y solicitudes de ese nuevo proyecto, todo podrá ser finalmente aplicado por los colaboradores.

6.2.3 Fase de Ejecución

En esta etapa se lleva a cabo la implementación del proyecto. Esta fase es responsabilidad del líder del proyecto, con la supervisión del cliente, en este caso el grupo directivo de la organización.

6.2.3.1 Entrenamiento y concientización

Uno de los primeros requisitos de la Dirección General es llevar a cabo actividades de concientización para todo el personal que labora en la organización.

La concientización es considerada como uno de los aspectos más importantes dentro de la cultura de seguridad de la información en una organización. Debe realizarse un uso adecuado y responsable de la información; debe ser tratada adecuadamente de acuerdo a los niveles de acceso establecidos por las políticas de seguridad, las cuales, en gran medida, determinan el éxito en la disminución del riesgo y vulnerabilidad de infiltraciones y accesos no autorizados. Por tal motivo, las organizaciones deben orientar sus acciones hacia la protección de la información.

Mediante el manual de Manual de Gestión de continuidad del negocio elaborado por el área de Continuidad del Negocio, se considera el cumplimiento de entrenamiento y concientización hacia el personal realizando lo siguiente:

1. Definir los objetivos de entrenamiento y concientización.
2. Desarrollar y ejecutar programas variados de entrenamiento.
3. Desarrollar programas de concientización.
4. Identificar otras oportunidades de educación.

6.2.3.2 Elaboración de procedimientos

El siguiente paso es la creación de los procedimientos de control de acceso lógico y clasificación de la información.

En esta sección se anexan los procedimientos generados para la oficina de seguridad de la organización.

1. Procedimiento de control de accesos lógicos.
2. Procedimiento de clasificación de la información.

6.2.3.2.1 Procedimiento de control de accesos lógicos

1. OBJETIVO

Establecer los lineamientos para el control de los accesos lógicos en los Sistemas, aplicaciones y Bases de Datos de la organización.

2. ALCANCE

Todos los aplicativos, sistemas y bases de datos que se operan y administran en la organización.

Los lineamientos de control de acceso lógico expresados en este documento aplican para todo el personal que labora para X-Empresa.

3. RESPONSABILIDADES

N°	Rol	Responsabilidad
3.1	Coordinador de Seguridad de la Información (Gestor de Seguridad)	• Genera cuentas de usuario y aplica permisos a los perfiles establecidos de acuerdo a las instrucciones de los Propietarios del Aplicativo o Sistema. • Recibe solicitud de acceso lógico, revisa firmas de personal facultado y ejecuta la instrucción de acceso. • Realiza proceso de validaciones de acceso (re certificación de usuarios) en el aplicativo por lo menos una vez del año. • Realizar mejoras a los procesos de seguridad de control de accesos lógicos. • Único facultado para proporcionar accesos lógicos y gestionar cuentas de usuarios de acuerdo a sus responsabilidades. • Gestionar la habilitación de logs de acceso lógicos en los servidores y/o dispositivos que permita rastrear cualquier operación realizada en los aplicativos y sistemas.

3.2	Propietario del aplicativo o sistema	• Es el único facultado por para autorizar el acceso del usuario al sistema, de acuerdo a sus roles y funciones. • Define y autoriza los privilegios o permisos de acceso a los sistemas de la información, de acuerdo a los roles y funciones del usuario. • En coordinación con el Gestor de Seguridad realizar las recertificaciones de usuarios por lo menos una vez al año.
3.3	Usuario	• Es la persona que requiere, de acuerdo a sus funciones, el acceso a sistema. • Solicita los accesos lógicos a los servicios necesarios para realizar sus labores de acuerdo a sus funciones, recabando las firmas de autorización correspondientes. • Hacer un buen manejo de sus cuentas de acceso, apegándose a los lineamientos de seguridad. • Informar al Gestor de Seguridad cuando la confidencialidad de su contraseña haya sido comprometida.
3.4	Director de área solicitante	• Da visto bueno al requerimiento mediante la herramienta de Centro de Soporte requeridas por su personal, de acuerdo a sus funciones. • Informar los cambios de roles y responsabilidades de su personal para identificar los cambios en los accesos.
3.5	Gerente Administrativa de Recursos Humanos	• Informar al Gestor de Seguridad sobre las altas, cambios de área y bajas del personal. • Aplicar las sanciones definidas en el reglamento interno de trabajo ante un reporte de desapego a los lineamientos de Seguridad.

3.6	Jefe inmediato del usuario	• Solicita el alta/baja de cuenta de accesos específicos para personal, así como el cambio de perfil de acceso de cuenta, al Gestor del Seguridad.

4. FORMATOS DERIVADOS

4.1 N/A

5. DOCUMENTACIÓN DE REFERENCIA

5.1 ISO/IEC 27001:2005 **tecnologías de la información, Control de Accesos.**

5.2 Manual o instructivo de Uso Adecuado de Contraseñas.

5.3 F1-P-AD-12 Solicitud de Servicio

6. DEFINICIONES

6.1 Identificador:

El identificador es un componente de la cuenta de acceso a los sistemas, generalmente conformado con el número de empleado, es a través de este identificador que se rastrean las operaciones realizadas en los sistemas y aplicativos.

6.2 Contraseña

Cadena de caracteres, generalmente cifrados y protegidos, que autentican a un usuario ante el sistema de cómputo.

6.3 Contraseñas temporales

Contraseñas que cuentan con un tiempo de vigencia determinado.

6.4 Cuenta de acceso

Todo usuario, que por sus funciones lo requiera, debe contar con una cuenta para el acceso a los sistemas de información, la cual consta de un identificador y contraseña única e intransferible.

6.5 Logs

Registro manual o automático de todas las actualizaciones a los archivos de datos y/o bases de datos.

7. POLÍTICAS

7.1 Es obligación del usuario cumplir con las políticas de seguridad de control de acceso lógico, establecidas en este documento. Cualquier desapego a estas políticas podrá ser sancionada de acuerdo al reglamento interno de trabajo.

7.2 El acceso a los sistemas solo se otorga al usuario que por sus funciones y roles que dentro de la empresa lo requieran.

7.3 La atención de alta, baja o cambio solo se realizara mediante la herramienta de Centro de Soporte y con autorizado por el Propietario del Aplicativo o Sistema.

7.4 Cualquier mal uso de la cuenta será responsabilidad del usuario al cual se le asignó.

7.5 Cualquier solicitud de baja de cuenta se deshabilitara por 45 días, después de este periodo se eliminara permanentemente con previa notificación.

7.6 Las cuentas con un periodo mayor de 30 días de inactividad se deshabilitaran (baja de cuenta).

8. DESARROLLO

N°	RESPONSABLE	ACTIVIDAD
8.1	**Alta de cuenta de accesos para personal de nuevo ingreso**	
8.1.1	Gerente Administrativa de Recursos Humanos	Solicita alta de usuario, al Gestor del Seguridad, mediante la herramienta de Centro de Soporte debidamente justificada por el Propietario del aplicativo o sistema.
8.1.2	Coordinador de Seguridad de la Información (Gestor de Seguridad)	Genera la cuenta de usuario y aplica los permisos y privilegios.
8.1.3	Coordinador de Seguridad de la Información (Gestor de Seguridad)	Realiza la entrega de cuenta al usuario nuevo.

8.1.4	Usuario	Recibe cuenta y contraseña genérica
8.1.5	Usuario	Ingresa a su cuenta y cambia la contraseña genérica, siguiendo las buenas prácticas.
8.2	**Cambio de perfil de acceso de cuenta**	
8.2.1	Jefe inmediato del usuario	Solicita mediante la herramienta de Centro de Soporte los privilegios al perfil de usuario mediante debidamente justificado por el Propietario del aplicativo o sistema.
8.2.2	Coordinador de Seguridad de la	Aplica cambios de privilegios a la cuenta del perfil de usuario solicitado.

	Información (Gestor de Seguridad)	
8.2.3	Coordinador de Seguridad de la Información (Gestor de Seguridad)	Informa al Jefe inmediato del usuario el requerimiento ha sido atendida.
8.2.4	Director de Área del solicitante	Da visto bueno al requerimiento.
8.3	**Baja de cuenta de acceso de usuario**	
8.3.1	Gerente Administrativa de recursos Humanos Recursos Humanos	Informa por medió de la herramienta de Centro de Soporte sobre la baja de usuarios del personal que causa baja de la empresa.
8.3.2	Gestor de Seguridad	Recibe la baja del personal y deshabilitará la cuenta **Nota:** La cuenta se habilitara solo si es debidamente justificada mediante la herramienta de Centro de Soporte.

9. CONTROL DE CAMBIOS

REVISIÓN	FECHA	MOTIVO
0	**Mayo 2015**	**Inicio en el Sistema de Gestión de Calidad**
1	**Octubre 2015**	**Mejora del Procedimiento**

6.2.3.2.2. Procedimiento de clasificación de la información

	MANUAL DE PROCEDIMIENTOS	**Código: x-xx-xx**
		No. Revisión: 1
		Fecha de Revisión: Junio 2015
	CLASIFICACIÓN DE LA INFORMACIÓN	***Página:*** **16 de 4**

1.- OBJETIVO

Establecer los lineamientos de la clasificación de la información de X-Empresa, con el propósito de establecer las medidas de seguridad que protegen su confidencialidad.

2.- ALCANCE

Los lineamientos d clasificación de la información expresados en este documento aplican para toda la documentación generada en X-Empresa.

3.- RESPONSABILIDADES

3.1 Propietario de la Información

Asigna el nivel de confidencialidad adecuado a los activos de la información que se genera en su proceso, de acuerdo al “Anexo 1: Tabla de niveles de confidencialidad”.

Verifica que toda la información generada en su proceso esté clasificada.

3.2 Consultor de seguridad

Establece el criterio para establecer el nivel de confidencialidad de los activos de la información.

Da Vo.Bo. a la clasificación asignada por el propietario de la información.

3.3 Consultor de Calidad

Actualiza la “Lista maestra de documentos”.

Verifica o valida que toda la documentación generada como parte del manual del SGC esté clasificada de acuerdo al “Anexo 1: Tabla de niveles de confidencialidad”.

4.- FORMATOS DERIVADOS

4.1 Lista maestra de documentos.

5.- DOCUMENTOS DE REFERENCIA

5.1 ISO/IEC 27001:2005 Sistema de Gestión de Seguridad de la Información, Gestión de Activos.

5.3 Minuta.

5.4 Manual de Seguridad de X-Empresa.

5.5 Manual de Gestión de la Calidad.

6.- DEFINICIONES

6.1 Activo de información

Un activo de información se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para X-Empresa. La clasificación general es la siguiente:

Físicos

- Documentos impresos.

Lógicos

- Datos.
- Información.
- Bases de datos.

6.2 Confidencialidad

La información se encuentre solo a disposición de individuos, entidades o procesos autorizados.

Es un atributo de la información o datos y se refiere a que solo el personal autorizado por el propietario de la información y/o datos tiene acceso de lectura, escritura o modificación de la misma, de acuerdo a los criterios establecidos.

7.- POLÍTICAS

7.1 Clasificar toda la información conforme a su criticidad, de acuerdo a lo establecido en el Anexo 11: Tabla de niveles de confidencialidad requerimientos legales, sensibilidad y criticidad a la organización.

7.2 Realizar revisiones semestrales de los activos de información.

7.3 La distribución, transporte y copiado de la documentación confidencial se realizará únicamente con autorización previa del dueño del documento generado.

8.- DESARROLLO

N°	RESPONSABLE	ACTIVIDAD
8.1.1	Propietario de la Información	Clasifica la nueva documentación dada de alta en el Sistema de Gestión de Calidad, por medio de la Solicitud de Modificación de estructura documental, de acuerdo al "Anexo: Tabla de niveles de confidencialidad".
8.1.2	Consultor de Calidad	Notifica al área de Seguridad sobre el alta del documento en el SGC, con el nivel de clasificación definido previamente.
8.1.3	Consultor de seguridad	Se da por enterado del nivel de confidencialidad, asignado a la documentación, generada por el Propietario de la Información.
8.1.4	Consultor de seguridad	Actualiza la lista maestra de documentos.
8.1.5	Consultor de seguridad / Consultor de Calidad	Se genera la "Minuta", en la cual se mencionan los acuerdos establecidos en la entrevista.

9.- CONTROL DE DOCUMENTOS

REVISIÓN	FECHA	MOTIVO
0	Mayo 2015	Inicio en el Sistema de Gestión de Calidad
1	Junio 2015	Mejora del proceso

10. ANEXO

Tabla de niveles de confidencialidad

Nivel	Criticidad	Confidencialidad	Impacto
1	Nula	**Pública**: Toda información cuya divulgación no represente ningún riesgo a la empresa.	No hay impacto.
2	Baja	**Interna**: Toda información emitida para la operación de la empresa y cuya divulgación solo debe realizarse a empleados de la empresa y, si lo requiere, a algunas entidades externas autorizadas. La divulgación no autorizada de este tipo de información no debe representar riesgos financieros para la empresa.	De imagen.
3	Media	**Reservada:** Información conocida por un área y algunos otros empleados de X-Empresa, cuya divulgación o uso no autorizado podrían ocasionar pérdidas, financieras y de imagen, menores a la organización.	Financiero y de imagen.
4	Alta	**Confidencial:** Información conocida por un grupo muy reducido de empleados de la organización, cuya divulgación o uso no autorizado podrían ocasionar pérdidas, financieras y de imagen, graves a la organización.	Financiero y de imagen.

6.2.3.3 Plataforma de hosteo

6.2.3.3.1 SharePoint

La principal herramienta de gestión de perfiles de acceso a la información sensible alojada en el repositorio empresarial utilizada en la organización, intranet, se encuentra diseñada bajo la plataforma empresarial SharePoint.

Plataforma de colaboración empresarial cuyo objetivo es proporcionar espacios de trabajo compartidos y almacenes de información, bajo esquemas de perfiles de acceso. Es un conjunto de herramientas de Microsoft que permiten crear soluciones empresariales de intranet, portales web con gestión de contenidos y la gestión del conocimiento.

El caso de uso de este informe comprende Microsoft SharePoint versión 2010.

6.2.3.3.2 Control de acceso con SharePoint

En la Tabla 2 se describen los niveles de permisos que puede ser asignado a los usuarios y los grupos de SharePoint, y el permiso asignado a los niveles de permisos. Para cada permiso se indica el nivel de permisos asociado de forma predeterminada.

Tabla de Niveles de permiso

Nivel de permisos	Descripción
Control total	Este nivel de permisos contiene todos los permisos. Está asignado al grupo de SharePoint Propietarios de nombre de sitio, de forma predeterminada. No se puede personalizar ni eliminar.
Diseño	Permite crear listas y bibliotecas de documentos, modificar páginas y aplicar temas, bordes y hojas de estilos en el sitio Web. De forma predeterminada no está asignado a ningún grupo de SharePoint.
Colaborar	Permite modificar y eliminar los elementos de las listas y bibliotecas de documentos existentes. De forma predeterminada está asignado al grupo Miembros de nombre de sitio de SharePoint.
Leer	Acceso de sólo lectura al sitio Web. Los usuarios y grupos de SharePoint con este nivel de permisos pueden ver los elementos y páginas, y abrir los elementos y documentos. De forma predeterminada está asignado al grupo Visitantes de nombre de sitio de SharePoint.
Acceso limitado	Está diseñado para combinarse con la personalización avanzada de permisos con el fin de dar a los usuarios acceso a una lista, biblioteca de documentos, elemento o documento específico sin darles acceso a todo el sitio. Sin embargo, para tener acceso a una lista o biblioteca, por

	ejemplo, un usuario debe tener permiso para abrir el sitio Web primario y leer los datos compartidos como las barras de exploración y temas del sitio Web. Este nivel no se puede personalizar ni eliminar.

Tabla 2. Niveles de permisos

6.2.3.3.3 Implementación del ambiente

La instalación y configuración no son parte del alcance de este reporte. Sin embargo, se mencionan de forma general, los elementos que intervienen en la arquitectura de implementación de SharePoint en la organización.

Para conocer el proceso de instalación y configuración detallado véase - Instalación y configuración:
https://www.microsoft.com/es-mx/download/details.aspx?id=10009

Existen diversas formas de implementar SharePoint, una de ellas es la arquitectura que se encuentra implementada bajo un ambiente virtualizado, como lo es en este caso. Este ambiente consta de los elementos que se describen a continuación:

Host de virtualización Servicio de rol Servicios de Escritorio remoto que se incluye con Windows Server 2008 R2. El Host de virtualización de Escritorio remoto se integra con el rol Hyper-V™ (programa de virtualización basado en un hipervisor para los sistemas de 64-bits1 con los procesadores basados en AMD-V o Tecnología de virtualización Intel) para proporcionar máquinas virtuales que pueden usarse como escritorio virtual personal o grupos de escritorio virtual.

Máquina virtual - Implementación de software de un ambiente de computación en el que se puede instalar y ejecutar un sistema operativo (OS) o programa.

Servidor web IIS - Conjunto de servicios para servidores usando Microsoft Windows. Es especialmente usado en servidores web, actualmente el segundo sistema de servidor web más popular.

Servidor de aplicaciones - Software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negocio y de acceso a los datos de la aplicación. Los principales beneficios de la aplicación de la tecnología de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones.

Windows Server – Sistema Operativo diseñado para el uso de servidores, desarrollado por Microsoft Corporation.

SharePoint Server – Servicio que incluye todas las características de SharePoint Foundation y otras características y funciones, como la administración de contenido empresarial, la inteligencia empresarial, el motor de búsqueda, sitios personales y el suministro de noticias.

VMware vCenter™ Server - Plataforma escalable para una gestión proactiva de la virtualización, que posibilita la máxima visibilidad de la infraestructura virtual. vCenter Server permite gestionar de manera centralizada los entornos VMware vSphere® y simplifica las tareas cotidianas, mejorando notablemente el control administrativo del entorno.

Servidor DNS - Sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Microsoft Exchange - Servidor de comunicación basado en el correo electrónico de colaboración empresarial.

Active Directory - Servicio de directorio de una red Windows server. Este servicio de directorio es un servicio de red que almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se con vierte en un medio de organizar, controlar y administrar centralizadamente el acceso a los recursos de la red.

A continuación se describe la arquitectura de la implementación, cuya administración depende del área de Sistemas Medios de la organización:

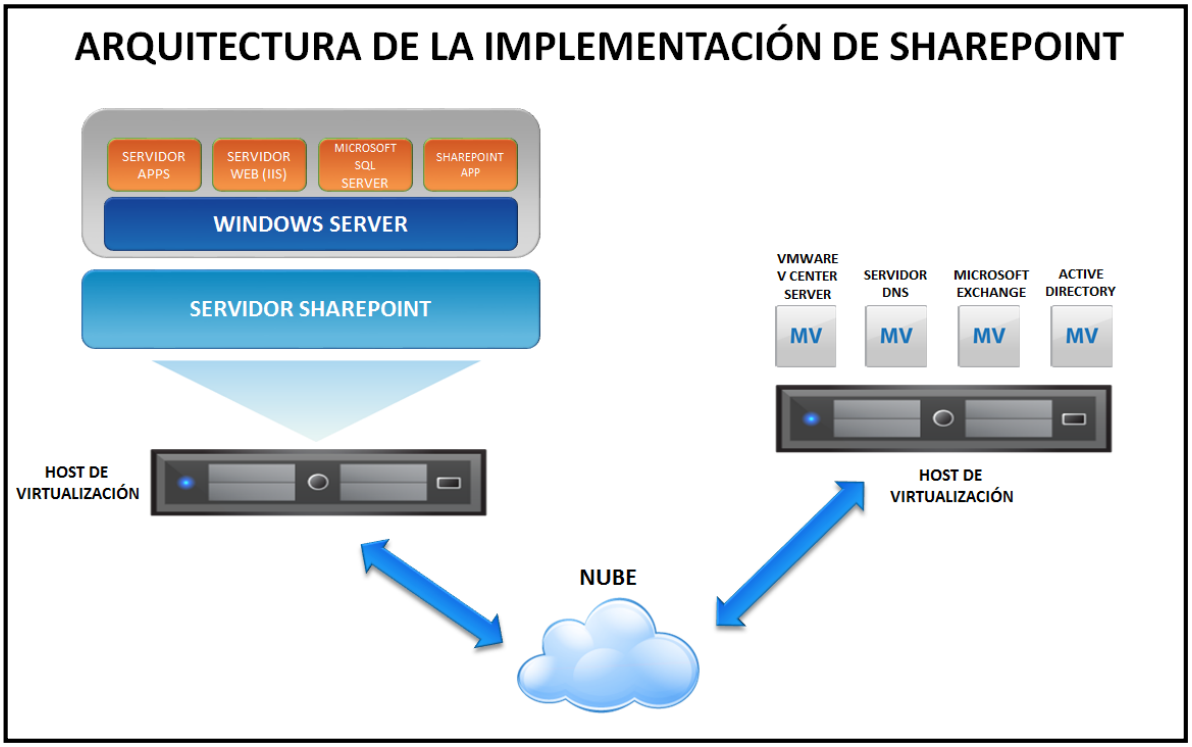


Figura 3 .Diagrama de la arquitectura de SharePoint de la organización.

6.2.3.3.4 Metamodelo de los sitios de la intranet

El metamodelo es un diagrama que describe el mapa de todos y cada uno de los sitios y subsitios que integran espacios de trabajo compartidos y almacenes de información de la organización. Es una herramienta de gran ayuda cuando se requiere conocer la dimensión de los espacios del repositorio empresarial y los perfiles de acceso asociados a cada uno de estos espacios.

El metamodelo es actualizado cada vez que se realiza una modificación a la estructura de los sitios y/o subsitios o cuando se lleva a cabo el proceso de recertificación semestral de perfiles de acceso, en conjunto con los dueños o responsables de cada uno de los sitios.

Por motivos de seguridad, respetando la confidencialidad de la información sensible para la organización, no es posible documentar el metamodelo en este informe.

6.2.3.3.5 Instructivos para la administración de la intranet

Se realizaron cuatro instructivos que describen detalladamente, las actividades más comunes del consultor de seguridad que es responsable del servicio de hosteo y la administración del repositorio, intranet, bajo la plataforma de SharePoint, mismos que se anexan a continuación:

1. Creación de carpetas y permisos.
2. Creación de copias de seguridad.
3. Creación de subsitios.
4. Creación de plantillas

Estos instructivos tienen como objetivo mantener documentada la base de conocimiento de las actividades propias de la administración de la plataforma que brinda el servicio de hosteo y administración del repositorio empresarial.

6.2.3.3.5.1 Instructivo creación de carpetas y permisos

	INSTRUCTIVO DE TRABAJO	**Código:**
		No. Revisión: Julio 2015
		Fecha de Revisión: 0
	CREACIÓN DE CARPETAS Y ASIGNACIÓN DE PERMISOS	***Página:*** **23 de 62**

1.- Objetivo

Proporcionar una guía detallada de creación carpetas, para proporcionar un repositorio empresarial gestionado a través de diferentes perfiles de acceso.

2.- Alcance

Creación de carpetas y asignación de permisos de acceso en Intranet.

3.- Responsabilidades

Coordinación de la Oficina de Seguridad de la Información

- Crear carpetas previamente autorizadas por el dueño del sitio, conforme al procedimiento de solicitud de servicio vigente.
- Proporcionar permisos de acceso a los usuarios, solicitados por los dueños de los sitios.

4.- Formatos Derivados

N/A

5.- Documentos de referencia

N/A

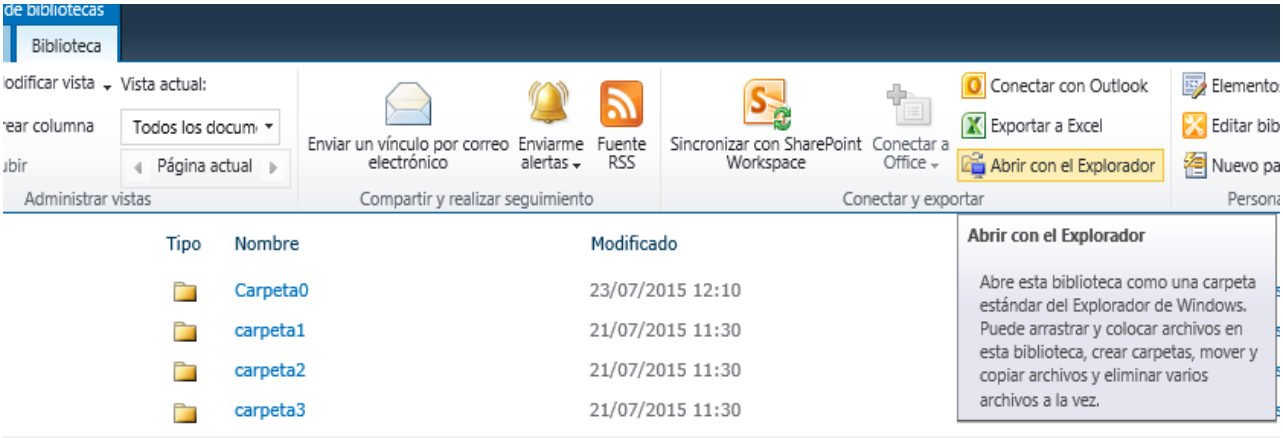
6.- Equipo requerido

N/A

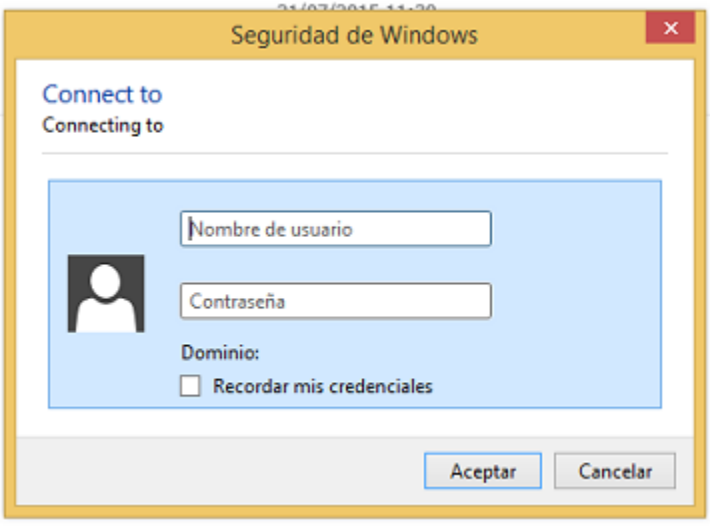
7.- Método

Los pasos para la creación de carpetas son los siguientes:
Existen dos formas de crear una carpeta:

a) **Con IE** - Dentro de la biblioteca de interés, dar clic en la pestaña **Biblioteca** y seleccionar el elemento **Abrir con el explorador**

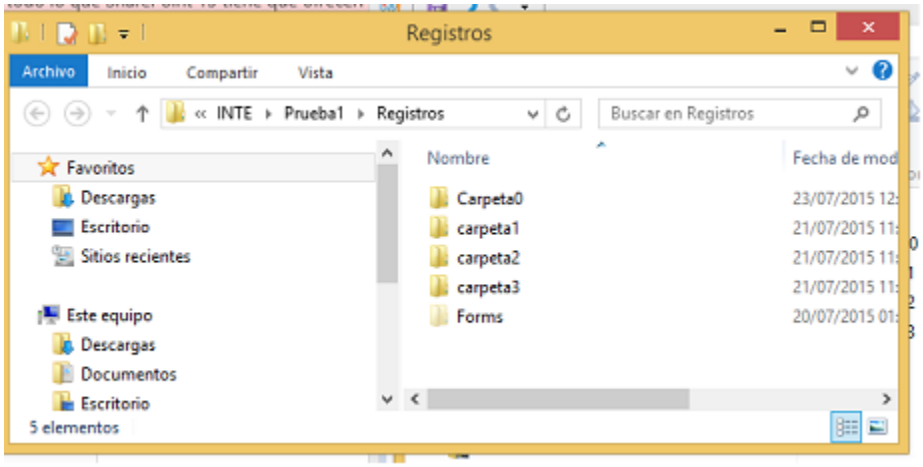


El sistema de seguridad de Windows requiere autenticación del usuario que intenta ingresar a esta opción. Ingresar el mismo **Nombre de usuario** y **Contraseña** de la cuenta de autenticación de Intranet.

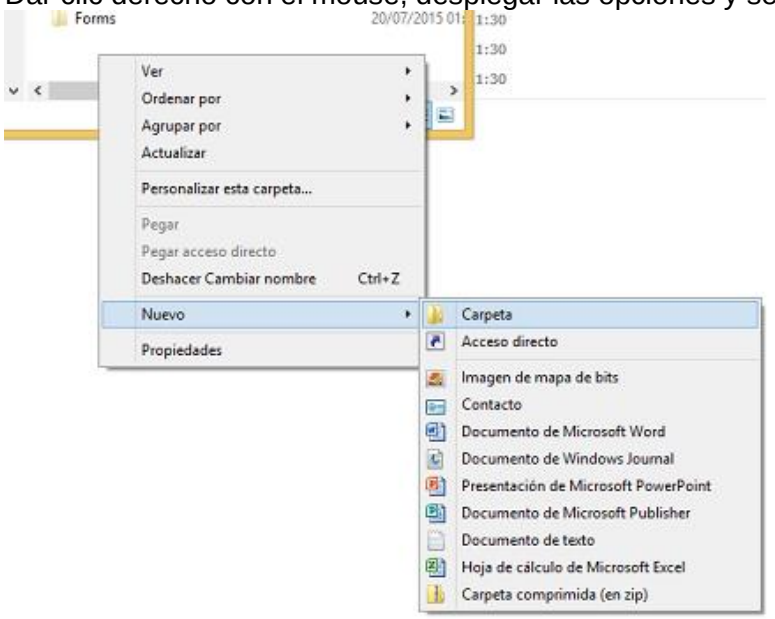


.

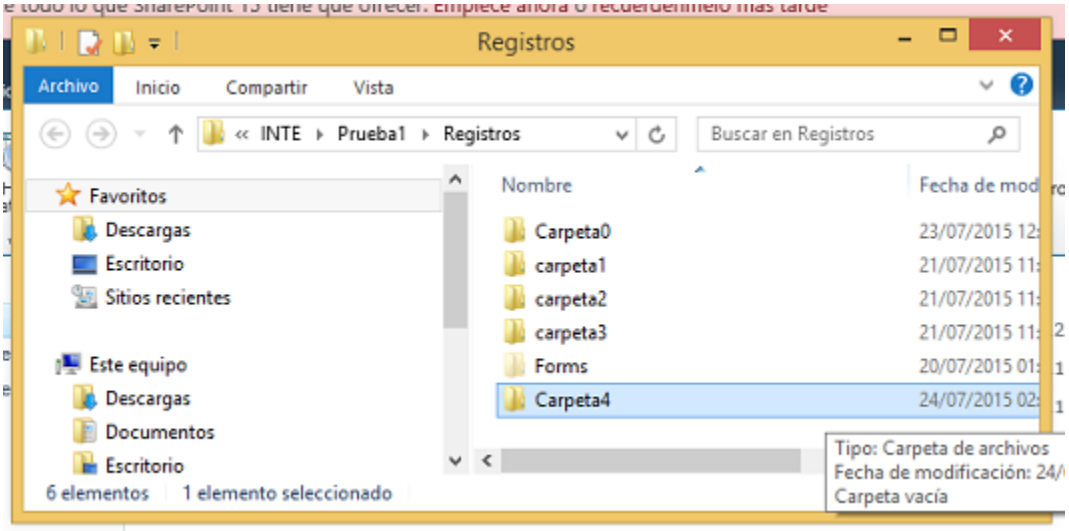
Entonces se abre un explorador de Windows



El procedimiento de creación es exactamente el mismo que se utiliza para crear una carpeta en Windows.
Dar clic derecho con el mouse, desplegar las opciones y seleccionar nueva carpeta.

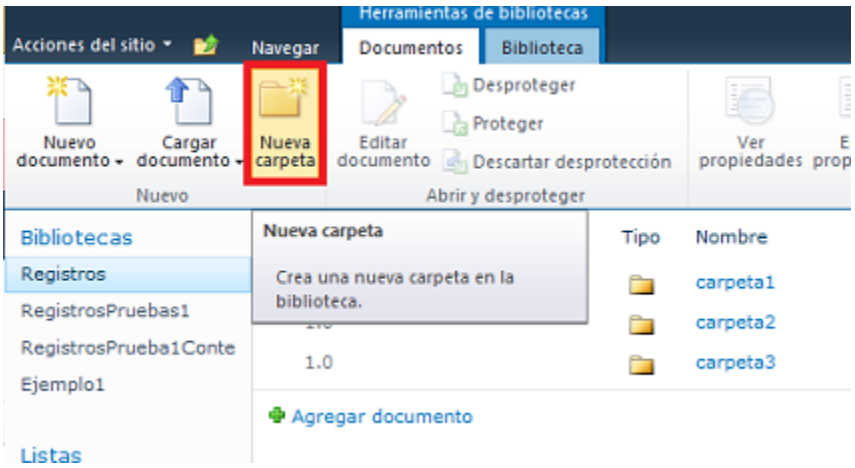


Nombrar la carpeta.

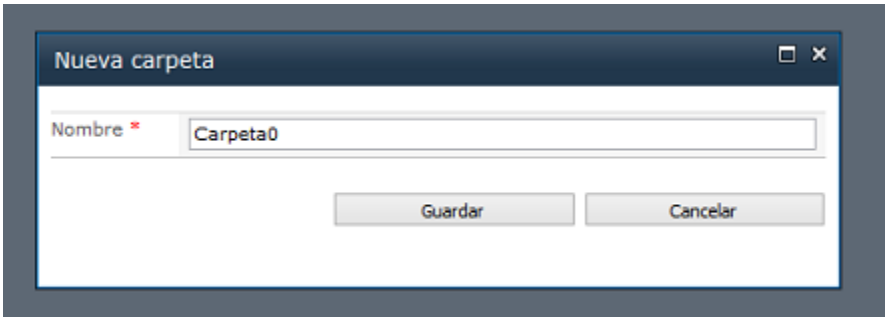


Automáticamente se crea el acceso en el portal de la Intranet, por lo que la carpeta será visible inmediatamente, una vez creada.

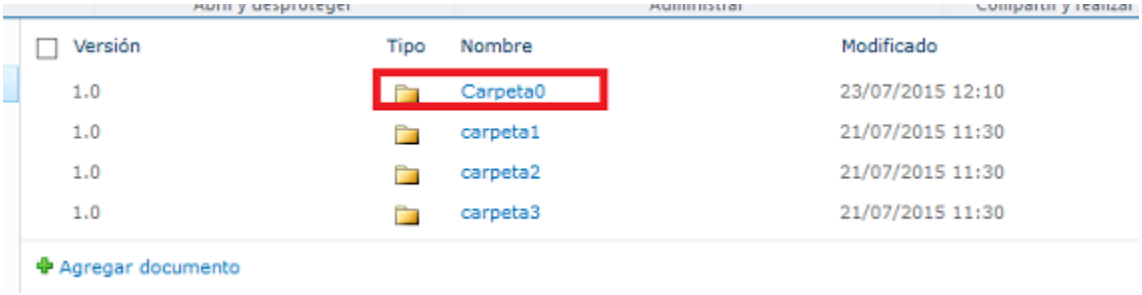
b) **Con Mozilla Firefox** - Es necesario encontrarse en la ubicación en la cual deba estar la carpeta que será creada.
Dar clic en la pestaña **Documentos** para desplegar el menú correspondiente. Dar clic en **Nueva carpeta**.



Nombrar la carpeta y car clic en **Guardar.**

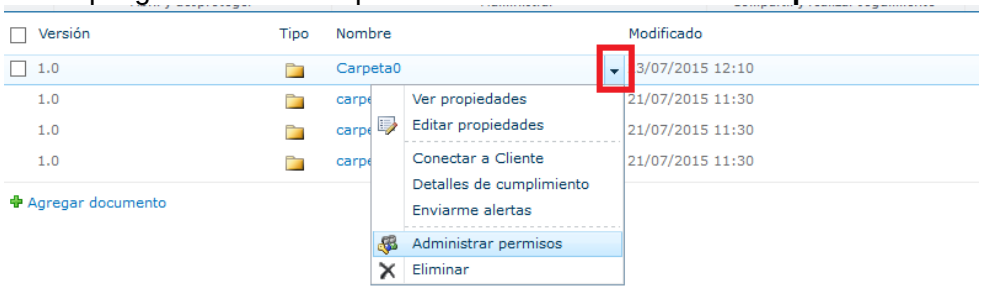


Una vez realizado lo anterior es creada la carpeta, con los datos de última modificación y por quién fue creada.



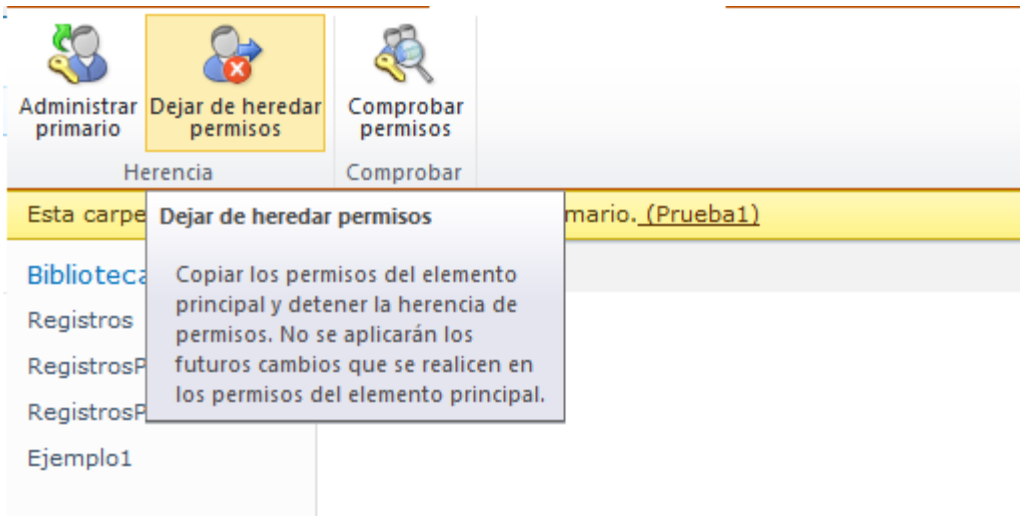
Asignación de privilegios y permisos de acceso.

Existen dos métodos para asignar permisos a los usuarios en una Sub sitio/ carpeta determinado. El primero es colocar el cursor en la carpeta en cuestión para hacer visible un botón que despliega un menú de opciones. Dar clic en **Administrar permisos.**

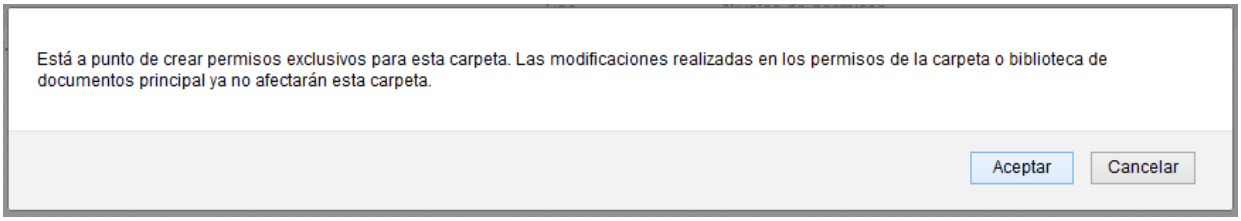


Dentro de **Administrar permisos** se otorgan /modifican/eliminan los permisos de los usuarios
Existen dos posibles escenarios: a) La carpeta hereda permisos de una carpeta padre. B) La carpeta tiene permisos exclusivos.

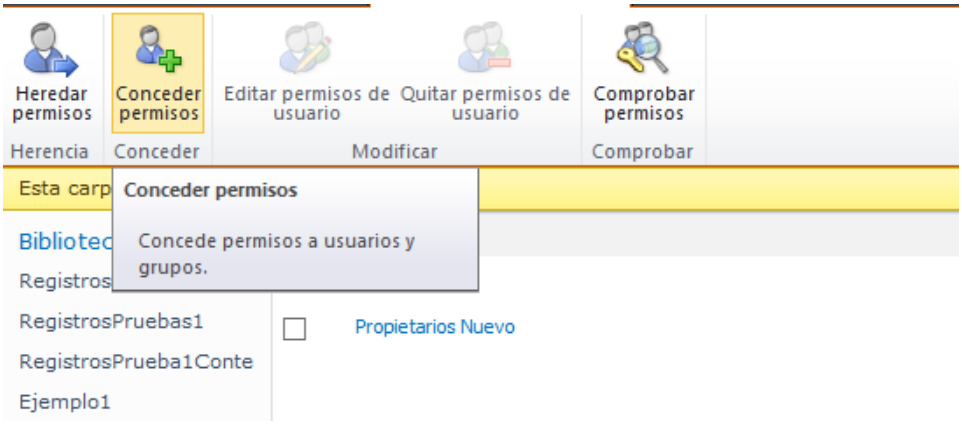
Si la carpeta hereda los permisos y requiere asignar permisos adicionales, dar clic en **Dejar de heredar permisos.**



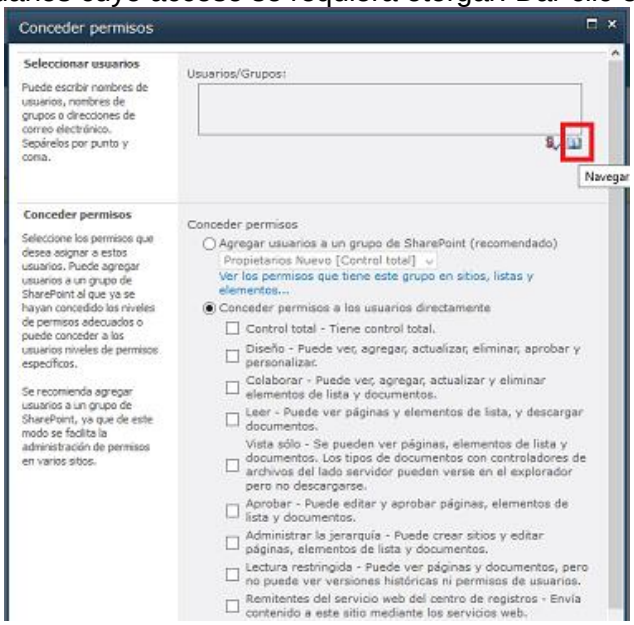
Aparece un recuadro de confirmación. Dar clic en **Aceptar.**



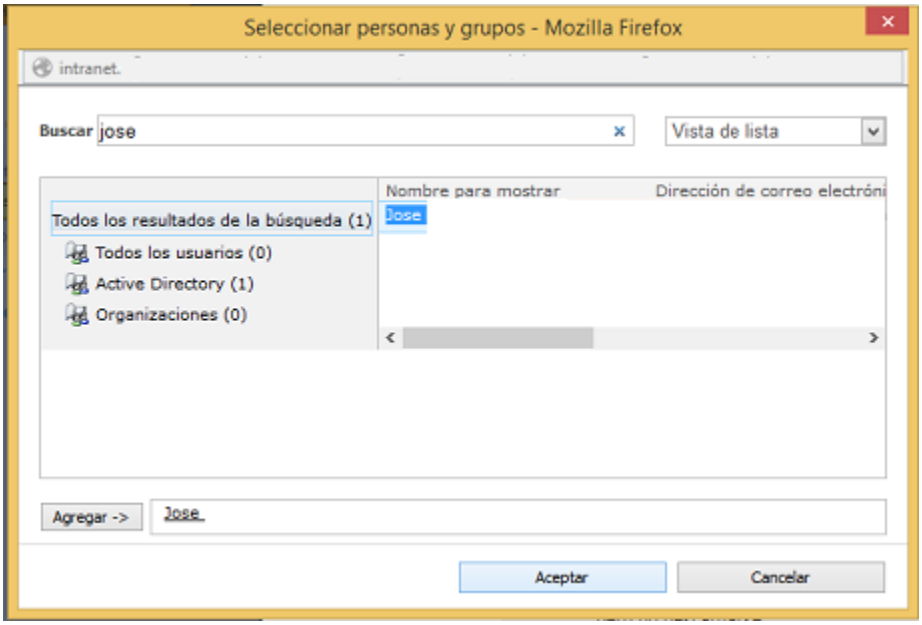
Una vez que la carpeta tiene permisos exclusivos es posible asignar los permisos requeridos.
Dar clic en **Conceder permisos**.



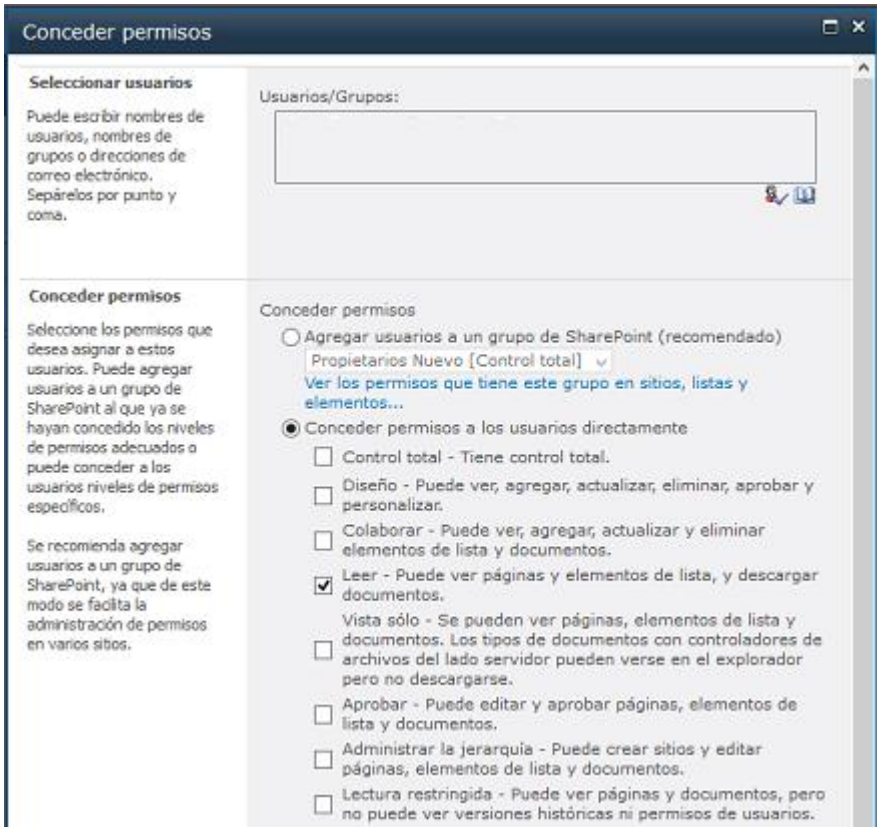
En la siguiente ventana, debajo del recuadro Usuarios/Grupos se encuentran dos íconos para buscar a los usuarios cuyo acceso se requiera otorgar. Dar clic en el ícono  .



En la siguiente pantalla, buscar al(los) usuario(s) requeridos. Dar clic en aceptar.



Una vez seleccionado al usuario, otorgar el perfil de acceso requerido.
Dar clic en **Aceptar.**



Una vez realizados los pasos anteriores el nivel de acceso ha sido otorgado satisfactoriamente. En la siguiente pantalla se puede observar el usuario, nivel de permisos y el tipo de usuario.

8.- Control de Cambios

Revisión	Fecha	Motivo
0	Mayo 2015	Inicio en el Sistema de Gestión de Calidad

6.2.3.3.5.2 Instructivo copias de seguridad

	INSTRUCTIVO DE TRABAJO	**Código:**
		No. Revisión: Julio 2015
		Fecha de Revisión: 0
	MANUAL DE COPIAS DE SEGURIDAD DE LA APLICACIÓN WEB DE SHAREPOINT	***Página:*** **33 de 5**

1.- Objetivo

Garantizar la capacidad de recuperación de la información ante posibles pérdidas de información de la aplicación web de SharePoint, a través de una guía para la creación de copias de seguridad de los datos de configuración y contenido de las aplicaciones web de SharePoint.

2.- Alcance

Copias de seguridad a la aplicación web de la Intranet.

3.- Responsabilidades

Coordinación de la Oficina de Seguridad de la Información

- Resguardar, de forma confidencial, la cuenta de administrador del aplicativo SharePoint.
- Realizar las copias de recuperación de la aplicación web de SharePoint de acuerdo a lo especificado dentro del contrato de servicios con el cliente.

4.- Formatos Derivados

N/A

5.- Documentos de referencia

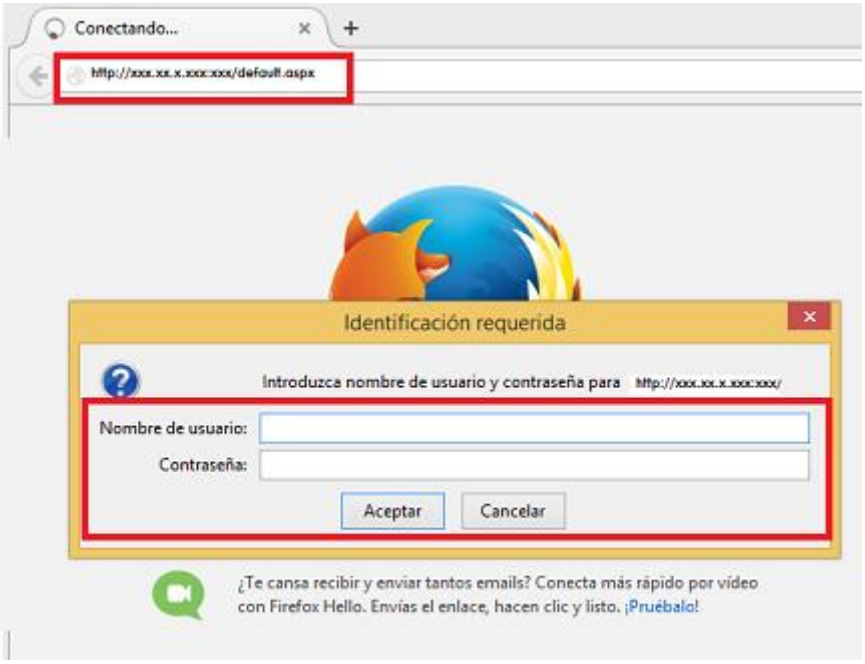
N/A

6.- Equipo requerido

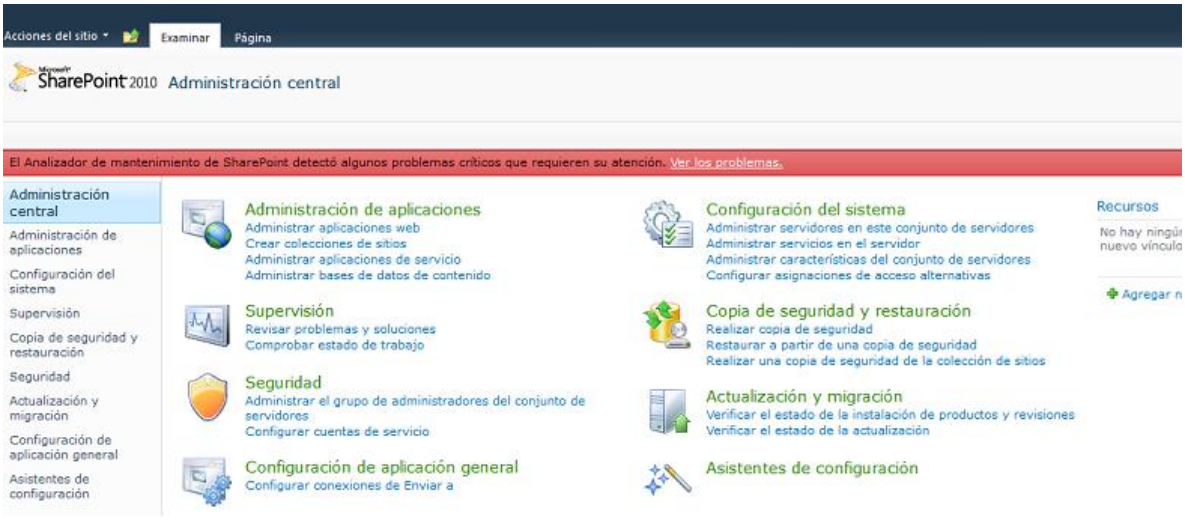
Equipo de cómputo / otros
Conexión a internet
Conexión a la página correspondiente de administración central de SharePoint.
Cuenta de administrador de SharePoint.

7.- Método

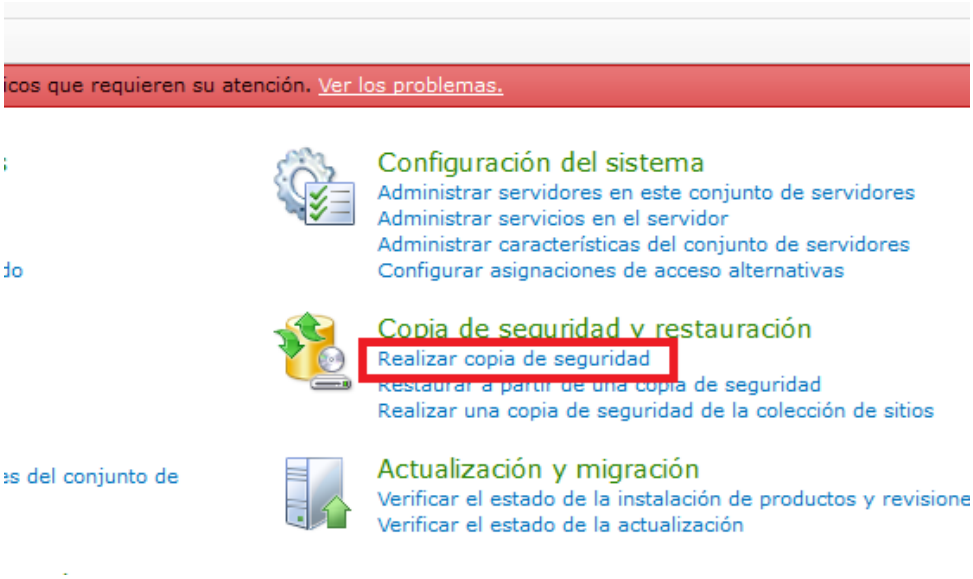
Por medio de un explorador de internet (Internet Explorer o Mozilla Firefox), ingresar la dirección web:
http://xxx.xx.x.xxx:xxx/default.aspx
Ingresar la cuenta de Administrador (Nombre de usuario y contraseña) y dar clic en aceptar.



Si la autenticación es exitosa, aparecerá la página de administración central.

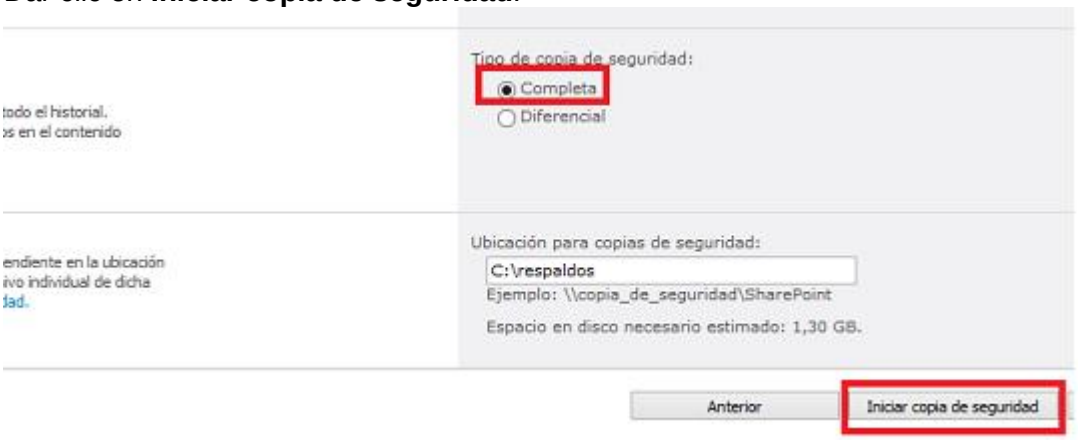


En **Copia de Seguridad y Restauración** dar clic en **Realizar copia de seguridad.**

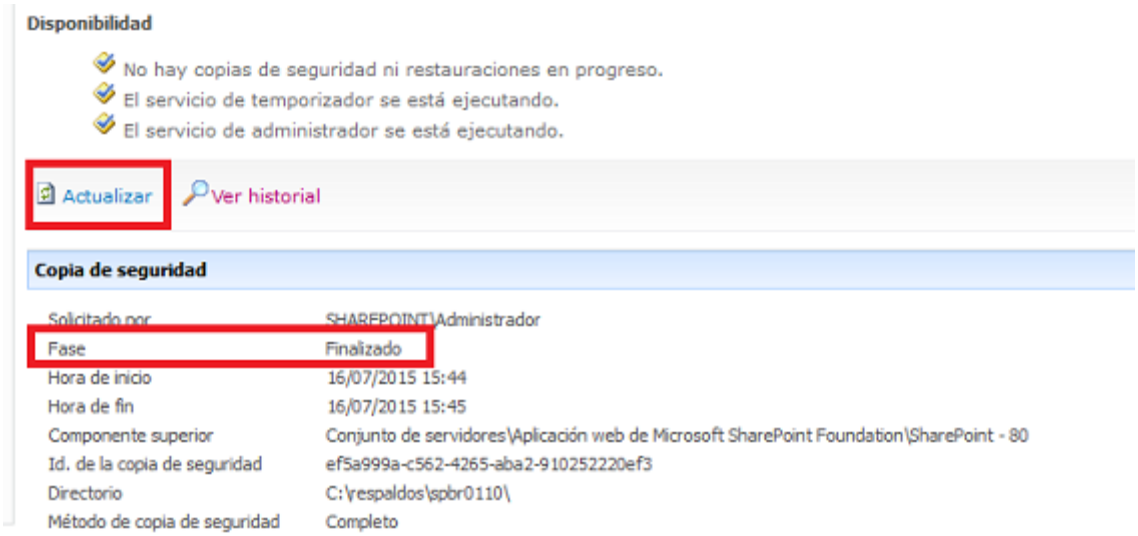


En **Seleccionar el componente para realizar una copia de seguridad** seleccionar el componente de la casilla **SharePoint – 80** y dar clic en **Aceptar**.

En la siguiente pantalla, seleccionar **Tipo de copia completa de seguridad**: **Completa**. Dar clic en **Iniciar copia de seguridad**.



Después de unos minutos el proceso de creación de la copia de seguridad terminará. Dar clic en **Actualizar** para confirmar el estatus del avance del mismo.



8.- Control de Cambios

Revisión	Fecha	Motivo
0	Mayo 2015	Inicio en el Sistema de Gestión de Calidad

6.2.3.3.5.3 Instructivo creación de subsitios

	INSTRUCTIVO DE TRABAJO	**Código:**
		No. Revisión: Julio 2015
		Fecha de Revisión: 0
	MANUAL DE CREACIÓN DE SUB SITIOS Y BIBLIOTECAS DE DOCUMENTOS EN SHAREPOINT	***Página:*** **38 de 9**

1.- Objetivo

Contar con un procedimiento documentado para crear sub sitios y bibliotecas de documentos en SharePoint.

2.- Alcance

Creación de Sub sitios y bibliotecas de documentos en la Intranet de X-Empresa.

3.- Responsabilidades

Coordinación de la Oficina de Seguridad de la Información

Crear los sub sitios y bibliotecas de documentos solicitados por los dueños de los sitios.

4.- Formatos Derivados

N/A

5.- Documentos de referencia

N/A

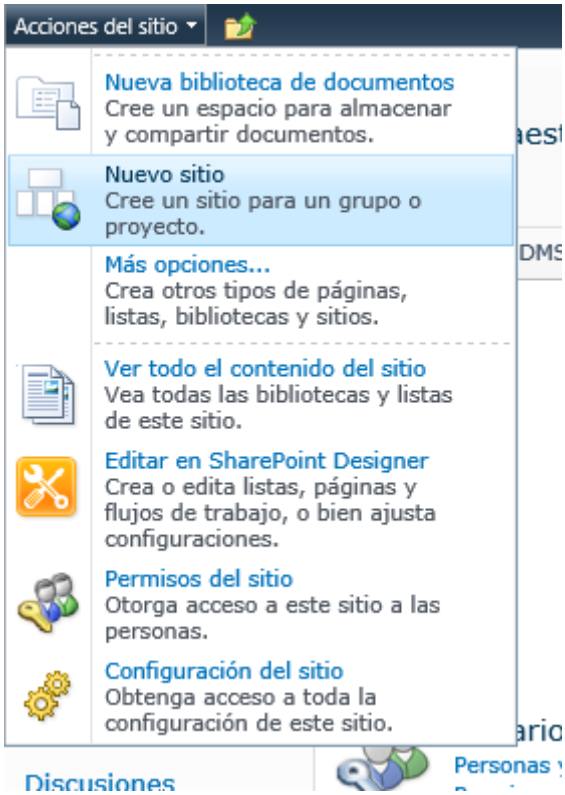
6.- Equipo requerido

Equipo de cómputo con conexión a la intranet de X-Empresa.

7.- Método

Para crear un nuevo sub sitio es necesario seguir los pasos descritos a continuación, recordando que el explorador que debe utilizarse es Internet Explorer:

En **Acciones del sitio** dar clic en **Nuevo sitio.**



En la siguiente página se deben ingresar el Título y descripción, los cuales aparecerán en la sección de sub sitios del sitio correspondiente.

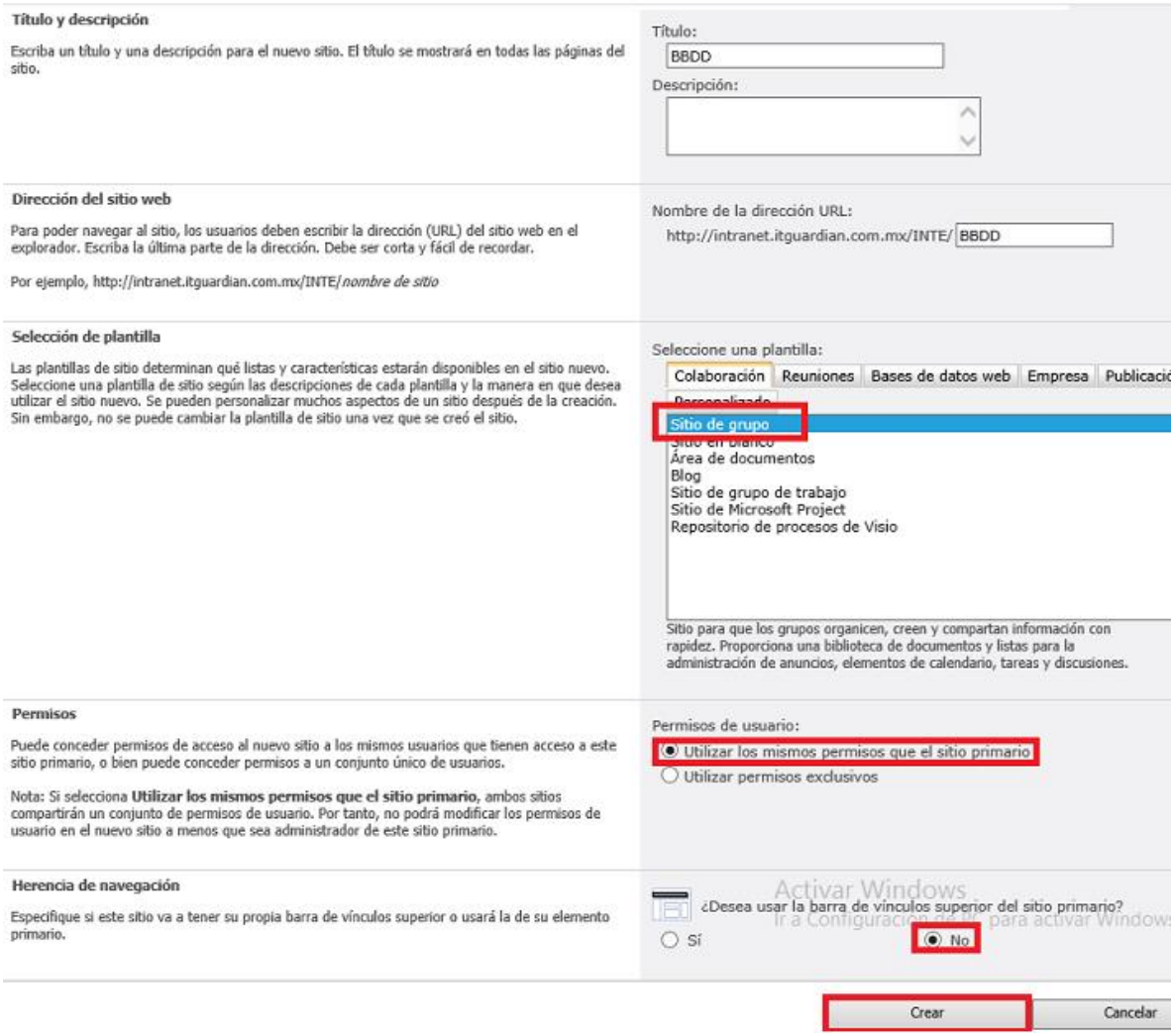
Ingresar el nombre de la dirección URL que se mostrará.

En **Seleccione la plantilla,** en la pestaña **Colaboración** seleccionar **Sitio de grupo.**

En permisos seleccionar **utilizar los mismos permisos del sitio primario.**

En **Herencia de Navegación** seleccionar **no.**

A continuación dar clic en **Crear.**

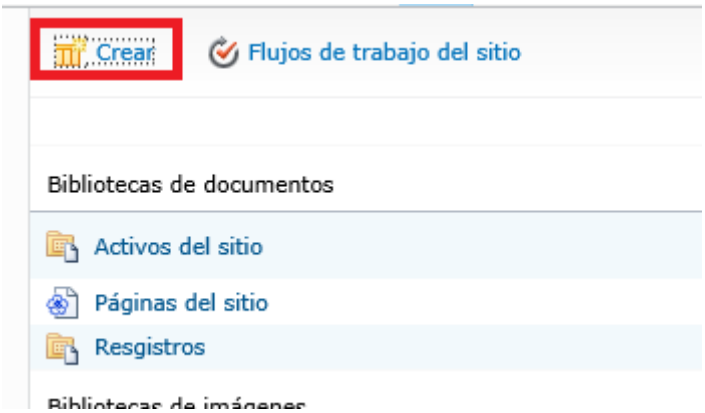

Título y descripción
Escriba un título y una descripción para el nuevo sitio. El título se mostrará en todas las páginas del sitio.
Título:
BBDD
Descripción:
Dirección del sitio web
Para poder navegar al sitio, los usuarios deben escribir la dirección (URL) del sitio web en el explorador. Escriba la última parte de la dirección. Debe ser corta y fácil de recordar.
Por ejemplo, http://intranet.itguardian.com.mx/INTE/nombre de sitio
Nombre de la dirección URL:
http://intranet.itguardian.com.mx/INTE/ BBDD
Selección de plantilla
Las plantillas de sitio determinan qué listas y características estarán disponibles en el sitio nuevo. Seleccione una plantilla de sitio según las descripciones de cada plantilla y la manera en que desea utilizar el sitio nuevo. Se pueden personalizar muchos aspectos de un sitio después de la creación. Sin embargo, no se puede cambiar la plantilla de sitio una vez que se creó el sitio.
Seleccione una plantilla:
Colaboración
Reuniones
Bases de datos web
Empresa
Sitio de grupo
Área de documentos
Blog
Sitio de grupo de trabajo
Sitio de Microsoft Project
Repositorio de procesos de Visio
Sitio para que los grupos organicen, creen y compartan información con rapidez. Proporciona una biblioteca de documentos y listas para la administración de anuncios, elementos de calendario, tareas y discusiones.
Permisos
Puede conceder permisos de acceso al nuevo sitio a los mismos usuarios que tienen acceso a este sitio primario, o bien puede conceder permisos a un conjunto único de usuarios.
Nota: Si selecciona Utilizar los mismos permisos que el sitio primario, ambos sitios compartirán un conjunto de permisos de usuario. Por tanto, no podrá modificar los permisos de usuario en el nuevo sitio a menos que sea administrador de este sitio primario.
Permisos de usuario:
Utilizar los mismos permisos que el sitio primario
Utilizar permisos exclusivos
Herencia de navegación
Especifique si este sitio va a tener su propia barra de vínculos superior o usará la de su elemento primario.
¿Desea usar la barra de vínculos superior del sitio primario?
Sí
No
Activar Windows
Crear
Cancelar

Realizar el diseño al sub sitio. Dar clic en la pestaña editar, representada por el ícono 
.

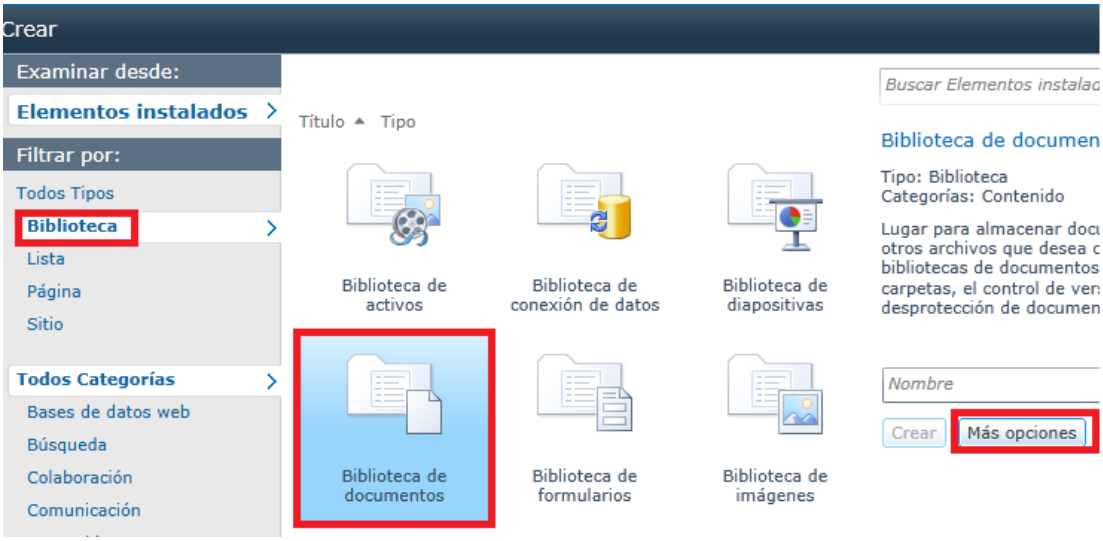
Una vez creado el sub sitio deben agregarse las bibliotecas correspondientes, para lo cual procederemos a realizar los pasos mencionados a continuación.

Creación de Biblioteca Registros

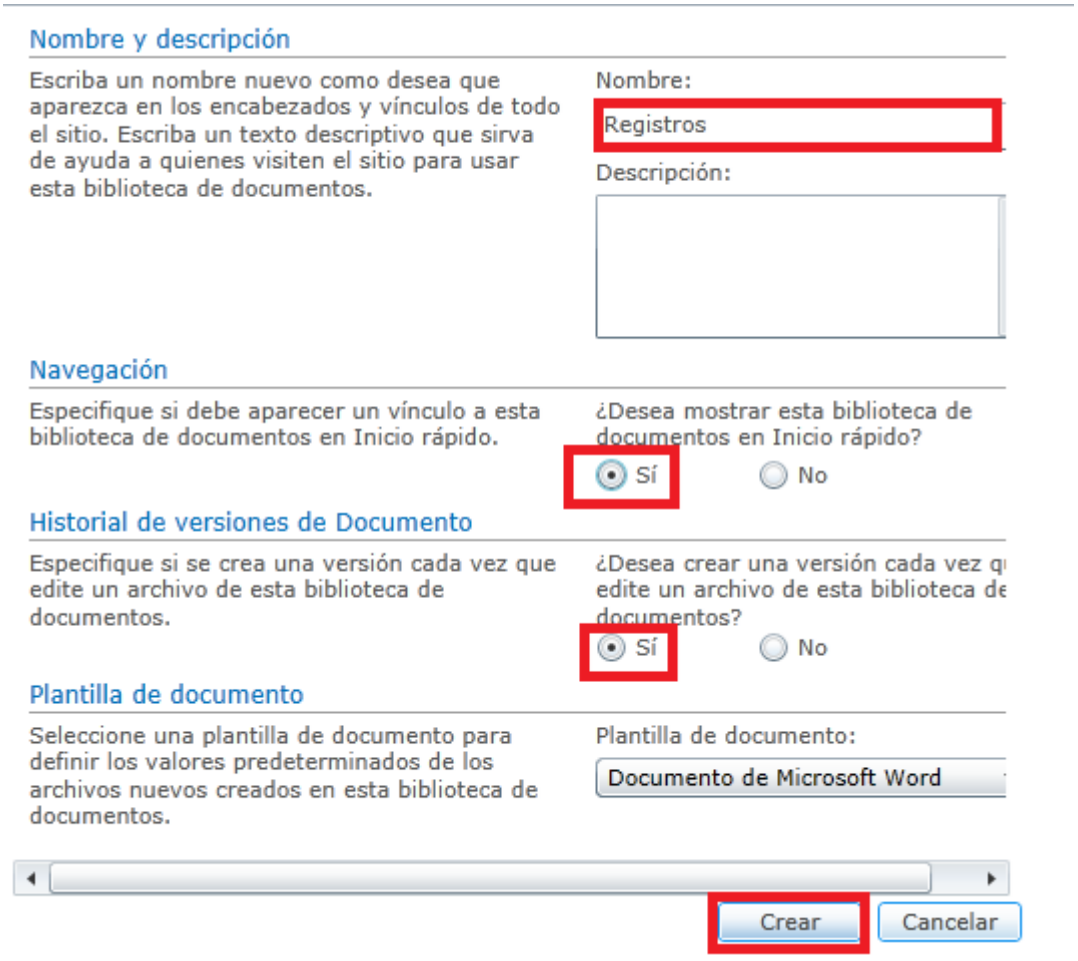
Estando ubicado en el sub sitio, dar clic en **Bibliotecas** o **Todo el contenido del sitio.**
En la siguiente página dar clic en **Crear.**



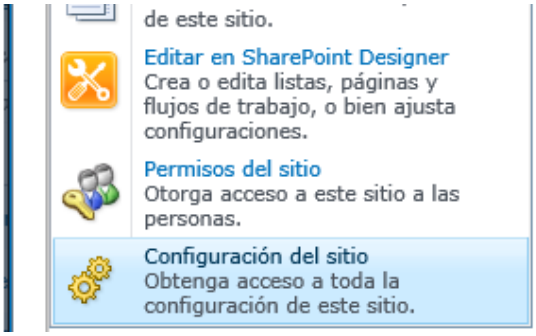
En **filtrar por,** seleccionar **Biblioteca** y el elemento **Biblioteca de documentos.**
Dar clic en **Más opciones.**



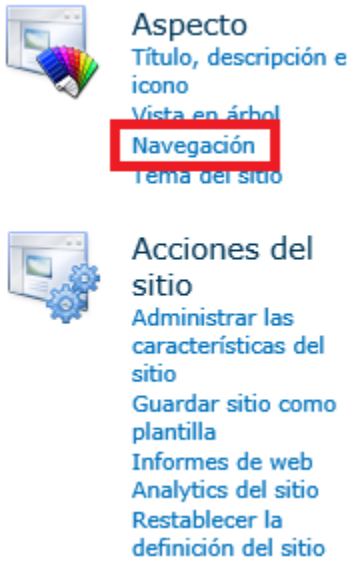
Agregar el nombre y descripción de la biblioteca, en este caso será “Registros**”.**
En **navegación,** dar clic en **Sí** para que se muestren los sitios principales.
En **Historial de versiones del Documento** dar clic en **sí** para guardar una versión cada vez que sea editado un documento de esa biblioteca.



La biblioteca **Registros** ha sido creada, ahora se requiere validar la configuración de navegación; para ello, ingresar a **Configuración de Sitio.**



Dentro de **Configuración de Sitio**, en la sección **Aspecto** dar clic en **Navegación.**

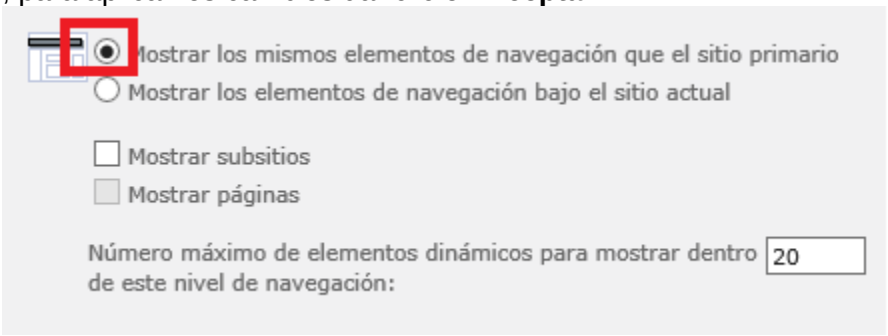


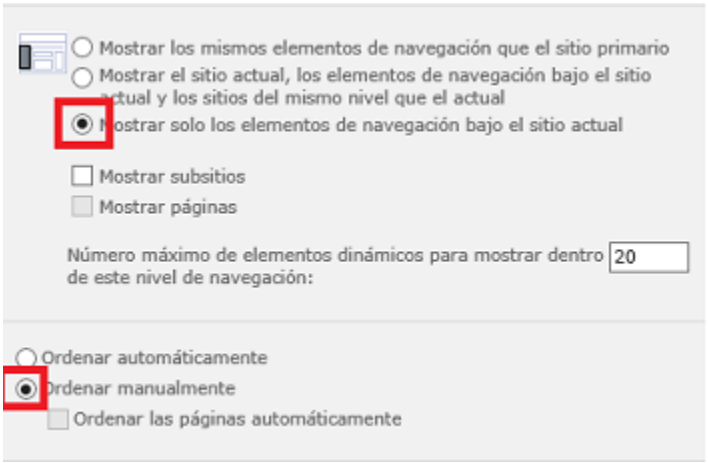
Para configurar la navegación global, seleccionar **Mostrar los mismos elementos de navegación que el sitio primario**, con lo cual tendremos visibilidad de los elementos del sitio primario al cual pertenece el sub sitio que acaba de ser creado, en este caso “Registros”.

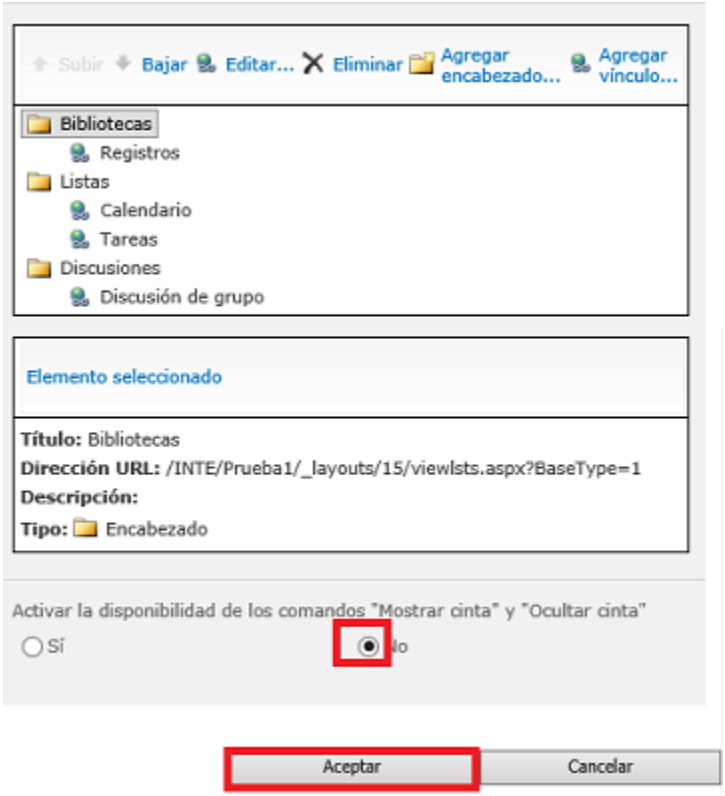
En navegación actual, seleccionar **Mostrar solo los elementos de navegación bajo el sitio actual** para ocultar las demás bibliotecas del sitio principal, una vez que se esté dentro del sub sitio recién creado, en este caso “Registros”.

Y para ocultar la cinta en el menú Acciones del sitio seleccionar **No**.

Finalmente, para aplicar los cambios dar clic en **Aceptar.**







8.- Control de Cambios

Revisión	Fecha	Motivo
0	Mayo 2015	Inicio en el Sistema de Gestión de Calidad

6.2.3.3.5.4 Instructivo creación de plantillas

	INSTRUCTIVO DE TRABAJO	**Código:**
		No. Revisión: Julio 2015
		Fecha de Revisión: 0
	CREACIÓN DE PLANTILLAS	***Página:*** **47 de 62**

1.- Objetivo

Contar con un instructivo detallado de los pasos a seguir para la creación de plantillas de bibliotecas de documentos en los sitios y sub sitios de la intranet.

2.- Alcance

Creación de plantillas de documentos en sitios y sub sitios en la intranet.

3.- Responsabilidades

Coordinación de la Oficina de Seguridad de la Información

Creación de sitios y sub sitios de bibliotecas de documentos en la intranet.

4.- Formatos Derivados

N/A

5.- Documentos de referencia

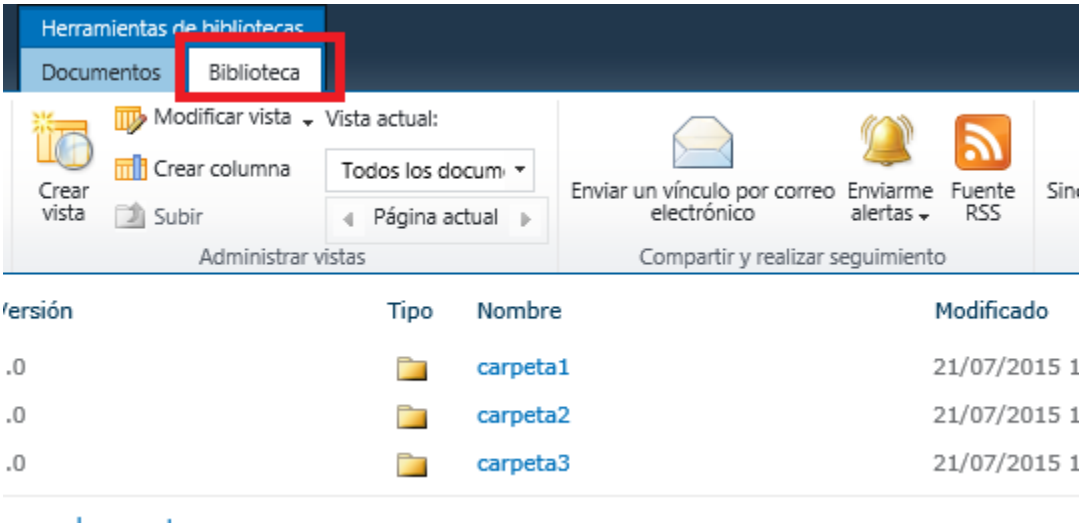
N/A

6.- Equipo requerido

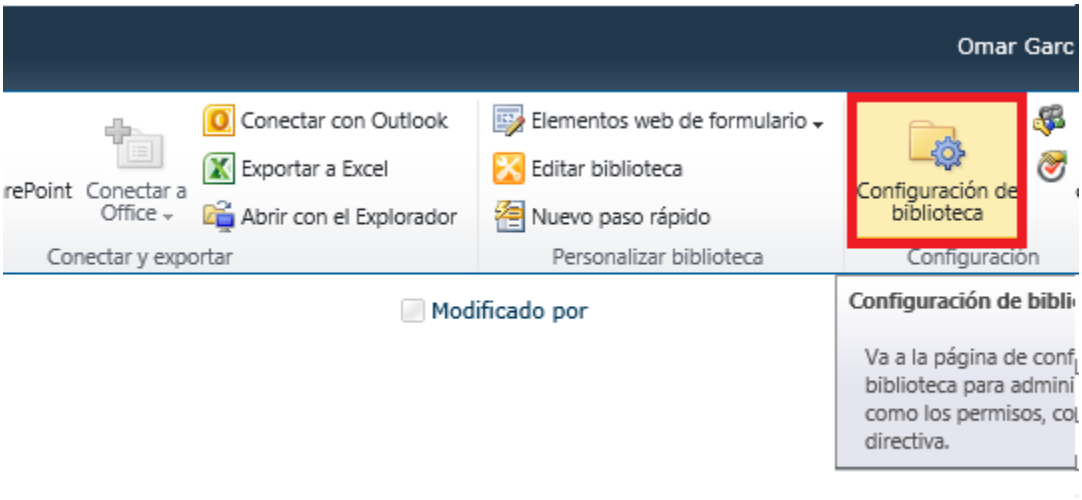
Un equipo de cómputo con conexión a Intranet.

7.- Método

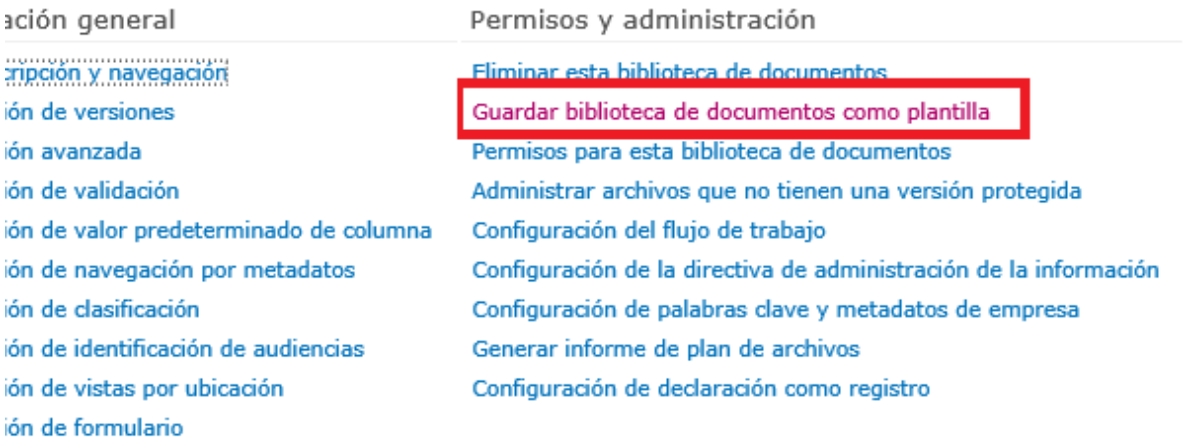
Para crear una plantilla de una biblioteca lo primero que debemos hacer es ubicarnos en la biblioteca que deseemos copiar. Una vez ahí damos clic en la pestaña **Biblioteca;** esto despliega el menú correspondiente.



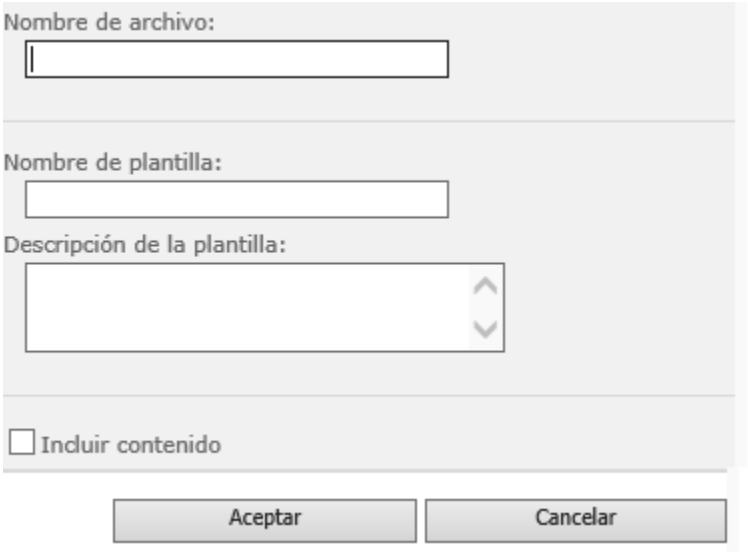
Dar clic en la opción **Configuración de la biblioteca.**



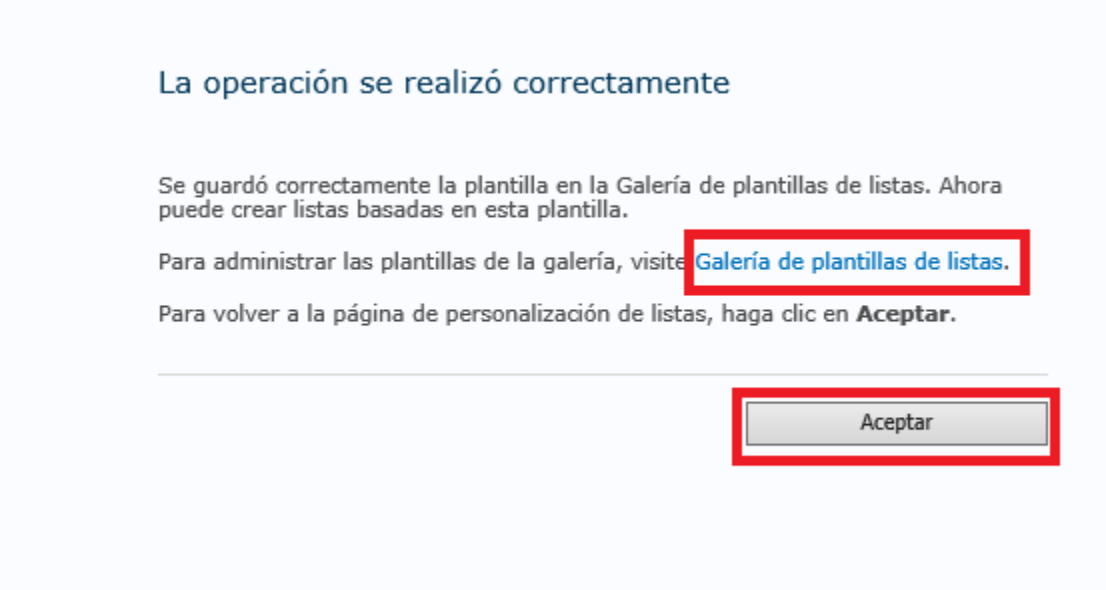
Dentro de **Configuración de la Biblioteca**, en el apartado **Permisos y administración** dar clic en **Guardar biblioteca de documentos como plantilla.**



Se abrirá una pantalla donde debemos ingresar un nombre y título para la plantilla.

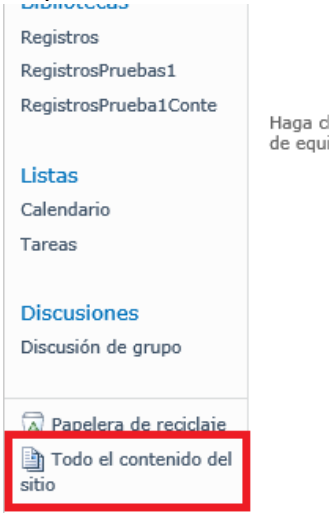


En la siguiente pantalla se muestra un vínculo de la **Galería de plantillas de listas** donde se almacenó la plantilla que acaba de ser creada. Dar clic en **Aceptar.**

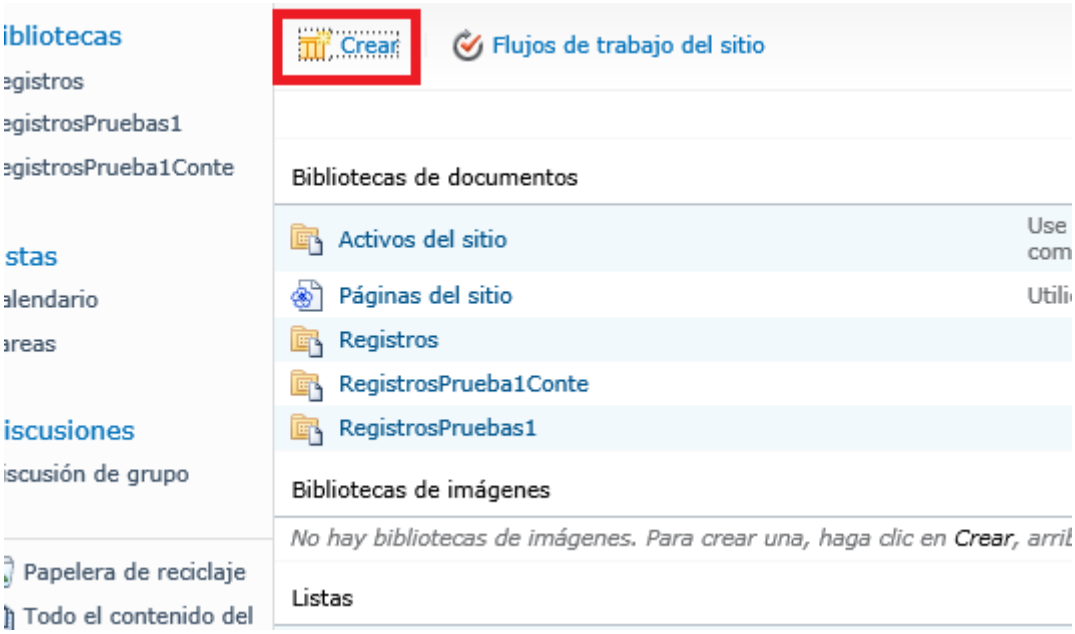


Agregar una plantilla

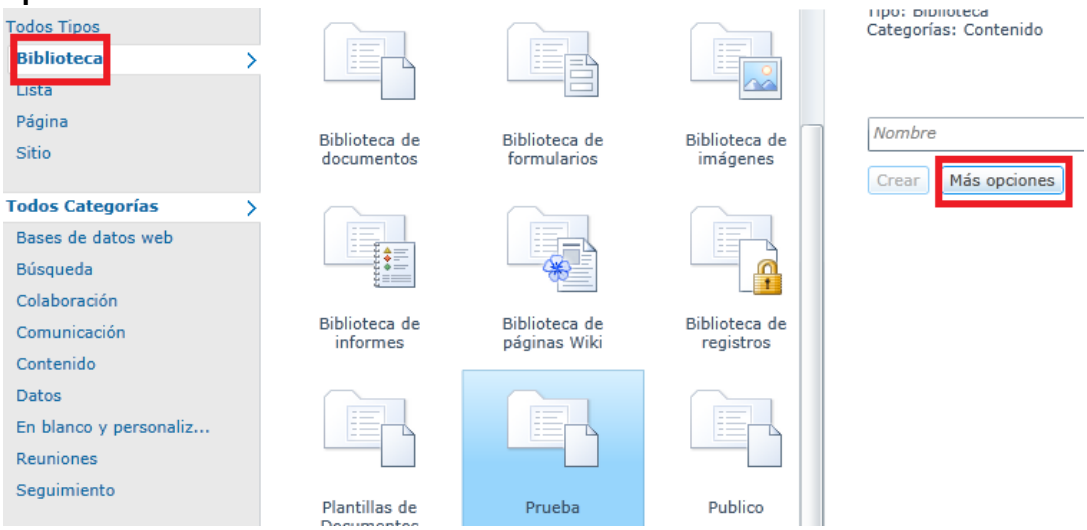
Para crear una biblioteca de documentos en un sitio o sub sitio, a partir de una plantilla, debemos ubicarnos en el sitio o sub sitio donde se desea colocar la biblioteca de documentos y en la parte inferior izquierda, seleccionar **Todo el contenido del sitio**.



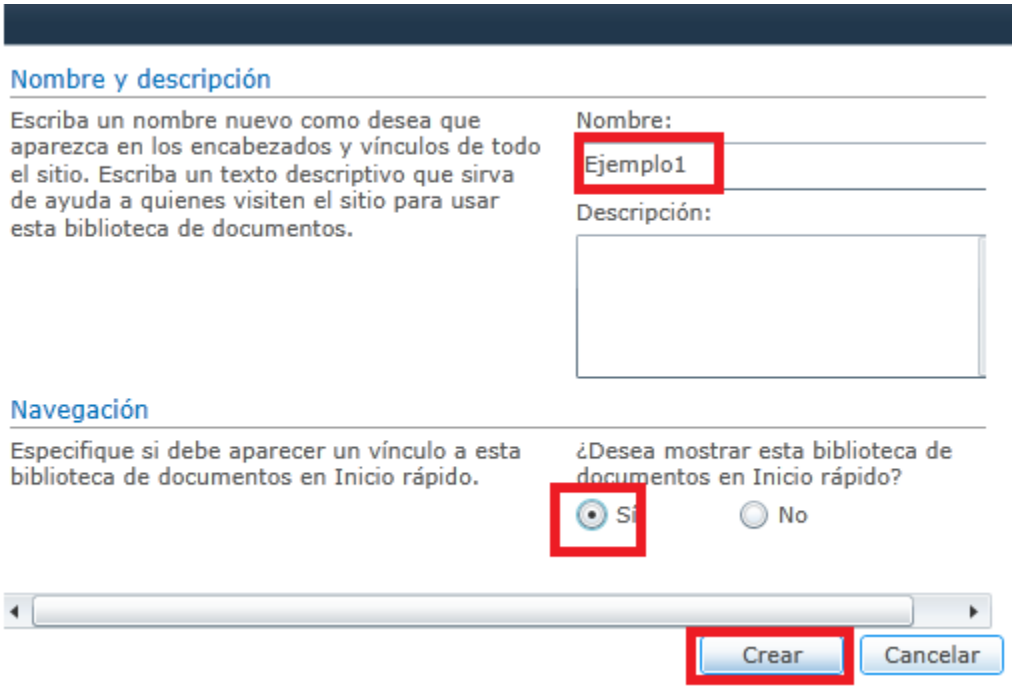
En la siguiente pantalla dar clic en **Crear.**



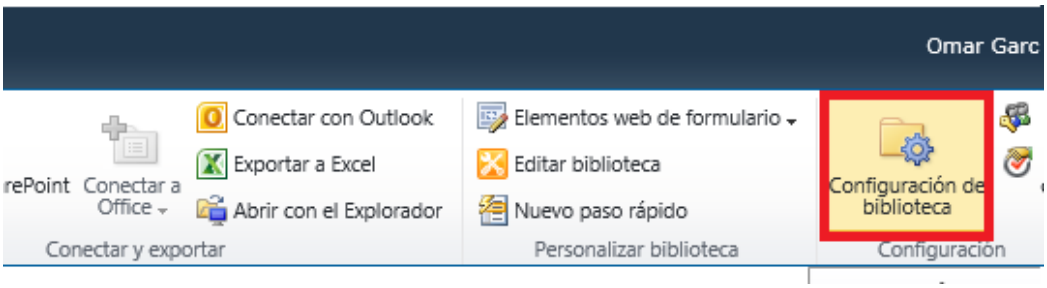
En **Todos Tipos,** dar clic en el tipo **Biblioteca** (para encontrar la plantilla con mayor facilidad) y seleccionar la plantilla que desea agregarse al sitio o sub sitio y dar clic en **Más opciones**.



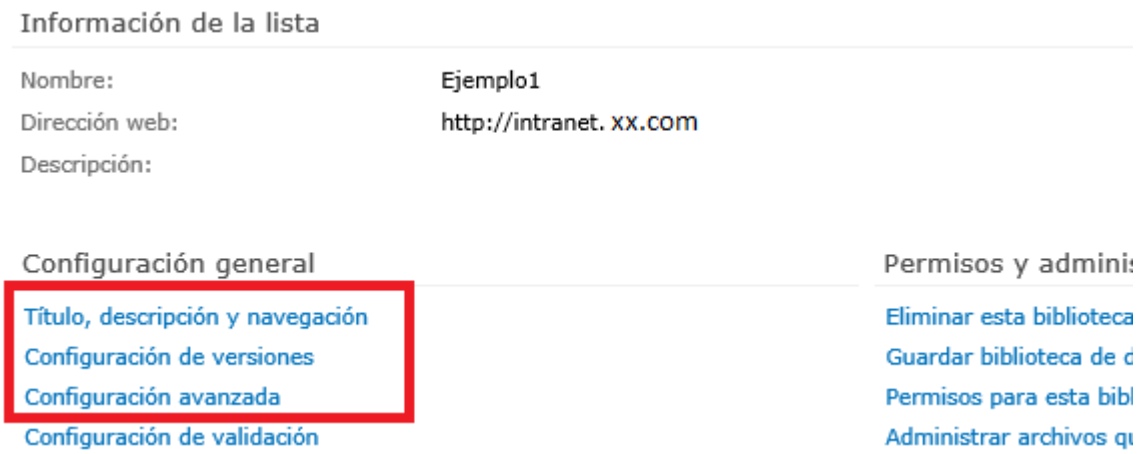
Ingresar el nombre que llevará la biblioteca de documentos dentro del sitio o sub sitio, el cual será visible a todos aquellos que tengan el privilegio de visualizar y acceder al sitio o sub sitio.
Seleccionar, en **Navegación,** si se desea un vínculo en inicio rápido.



Una vez realizado lo anterior podremos iniciar con la personalización de la biblioteca de documentos. Para realizar esto, dar clic en **Configuración de biblioteca,** en la pestaña **Biblioteca.**



Si se requiere una configuración idéntica a las demás Bibliotecas del mismo tipo, modificar los campos que se encuentran dentro de Configuración general: Título, descripción y navegación. Configuración de versiones y Configuración avanzada.



8.- Control de Cambios

Revisión	Fecha	Motivo
0	Mayo 2015	Inicio en el Sistema de Gestión de Calidad

6.2.4 Fase de Seguimiento y control

En esta fase se realiza el monitoreo de la documentación del proyecto y el aseguramiento de calidad, esta fase se desarrolla en todo el ciclo de vida del proyecto, desde la fase de inicio hasta la fase de cierre. Este monitoreo contempla:

La correcta integración de toda la documentación que da inicio formal al proyecto.

El avance del proyecto de acuerdo al cronograma.

La actualización del análisis de riesgos importantes, que en este caso fueron inexistentes.

La revisión de los incidentes de seguridad o polémicas, que en este caso no se presentaron.

La supervisión de la entrega oportuna de las carpetas de entregables al cliente interno, que en este caso es el Director de Infraestructura:

1. Procedimiento de control de accesos lógicos.

2. Procedimiento de clasificación de la información.

3. Instructivo creación de carpetas y permisos.

4. Instructivo copias de seguridad.

5. Instructivo creación de subsitios

6. Instructivo creación de plantillas.

Supervisión en el cierre del proyecto, cuando se firma el acta de cierre del proyecto, previa aceptación y aprobación del grupo directivo (el cliente) y demás interesados del proyecto.

6.2.5 Fase de Cierre

Esta fase contempla la aceptación del entregable final, por parte del Director de Infraestructura, en este caso la “Lista maestra de documentos”, la cual contiene todos los procedimientos y formatos de la organización, perfiles y niveles de acceso, la cual se muestra a continuación en la Tabla 2.

6.2.5.1 Lista maestra de documentos

CÓDIGO	NOMBRE DE DOCUMENTO	NIVEL DE CLASIFICACIÓN	Perfiles
		Confidencialidad	
XX-XX-XX	Manual de uso de la Intranet	2 - Interna	Todo el personal de la empresa
XX-XX-XX	Registro de bajas del personal	3 - Confidencial	Área de Recursos Humanos

Figura 4. Lista maestra de documentos

CAPITULO 3

7. MEJORA CONTINUA

7.1 Revisión de las políticas de Seguridad de la Información

Las políticas de seguridad de la información son revisadas semestralmente (enero y julio) para su adecuación y mejora continua asegurando el alineamiento con los objetivos del negocio.

Para las revisiones se considera la siguiente información:

1. Retroalimentación de las partes interesadas.
2. Resultados de las revisiones previas.
3. Estatus de las acciones preventivas y correctivas.
4. Desempeño de procesos y cumplimiento de la política de seguridad de la información.
5. Cambios que afecten el enfoque de gestión de la seguridad de la información incluyendo cambios en el ambiente organizacional, disponibilidad de recursos, condiciones legales y regulatorias o ambiente técnico.
6. Tendencias de las amenazas y vulnerabilidades.
7. Reportes de incidentes de seguridad de la información.

Los resultados obtenidos de las revisiones pueden incluir acciones de mejora para:

1. El enfoque de gestión de la seguridad de la información.
2. Objetivos y controles.
3. Asignación de recursos y/o responsabilidades.

Los resultados de las revisiones se registran en el Registro de Revisiones de Seguridad de Información.

CAPÍTULO 4

8. RESULTADOS

La creación de la oficina de seguridad y la implementación de los mecanismos de seguridad de la información “Procedimiento de Clasificación de la información” y el “Procedimiento de Accesos Lógicos”, alineados al estándar ISO/IEC 27001:2005, proporcionaron a la organización las políticas que brindan las instrucciones generales y las normas que indican los requisitos técnicos específicos del uso adecuado de la información.

Por otra parte, la inversión de recursos en programas de concientización del personal, como parte vital de la cultura organizacional fortalecieron los mecanismos de seguridad, logrando disminuir uno de los principales riesgos de una organización: La vulnerabilidad que en muchas ocasiones representa el personal interno, desde el del nivel usuario final hasta el administrador de los sistemas de información, pues son todos y cada uno de ellos quienes manejan la información sensible. De esta manera, con ayuda de buenas prácticas y el correcto manejo de los recursos fue posible lograr una implementación efectiva de los mecanismos de seguridad de la información en la organización.

Finalmente, la creación de instructivos de la administración de la plataforma de hosteo y administración del repositorio empresarial generó transparencia en el área, específicamente en temas como segregación de funciones y rotación de personal, ya que al existir actividades documentadas paso a paso se pierde centralización de funciones y por lo tanto, dependencia de personal que podría crear procesos viciados.

9. CONCLUSIONES

La implementación de los mecanismos de seguridad favorece la protección y continuidad de la información de la organización, en función de su nivel de criticidad, privacidad. Estos mecanismos dirigen y distribuyen los recursos para llevar a cabo los objetivos de seguridad de la información que la organización requiere. Estos controles brindan, también, soporte metodológico a la operación de la organización, al ser establecidas bajo los lineamientos de estándares internacionales y de buenas prácticas llevadas a cabo por todos y cada uno de los miembros de la organización.

A. Glosario

Activo de información	Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para una organización. Clasificados en: Físicos: Documentos impresos. Lógicos: Datos, Información, Bases de datos.
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Contraseña	Cadena de caracteres, generalmente cifrados y protegidos, que autentican a un usuario ante el sistema de cómputo.
Contraseñas temporales	Contraseñas que cuentan con un tiempo de vigencia determinado.
Cuenta de acceso	Todo usuario, que por sus funciones lo requiera, debe contar con una cuenta para el acceso a los sistemas de información, la cual consta de un identificador y contraseña única e intransferible.
Hipervisor	Plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos.
Identificador	Componente de la cuenta de acceso a los sistemas, generalmente conformado con el número de empleado, es a través de este identificador que se rastrean las operaciones realizadas en los sistemas y aplicativos.
IEC	International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.
Integridad	Propiedad de la información relativa a su exactitud y completitud.
ISO	Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).
ISO/IEC 27001:2005	Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

Kickoff	Instancias para reunir a todos y presentar de manera global los objetivos y planes a cumplir o, en el segundo caso, dar inicio al nuevo trabajo que se debe realizar.
Logs	Registro manual o automático de todas las actualizaciones a los archivos de datos y/o bases de datos.
PMBOK	Project Management Body of Knowledge. Guía de los fundamentos para la dirección de proyectos.
Plataforma	Sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible
Tecnología	Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico.
TI	Tecnologías de la Información Estudio, diseño, desarrollo, innovación, implementación y gestión de los sistemas informáticos, particularmente usos del software y hardware.
SGSI	Sistema de Gestión de la Seguridad de la Información.
SharePoint	Plataforma de colaboración empresarial cuyo objetivo es proporcionar espacios de trabajo compartidos y almacenes de información, bajo esquemas de perfiles de acceso.

B. BIBLIOGRAFÍA Y MESOGRAFÍA

- ISO/IEC 27001:2005 tecnologías de la información, Control de Accesos, Acceso Lógico.
- ISO/IEC 27001:2005 tecnologías de la información, Gestión de activos, Clasificación de la Información.
- Guía de los Fundamentos Para la Dirección de Proyectos (Guía del PMBOK) = A Guide to the Project Management Body of Knowledge (PMBOK Guide) (Spanish Edition).
- http://www.iso27000.es/iso27000.html
- http://www.iso27000.es/glosario.html#section10c
- https://products.office.com/es-es/sharepoint/collaboration
- https://es.wikipedia.org/wiki/Microsoft_SharePoint

- https://support.office.com/es-es/article/Niveles-de-permisos-y-permisos-49d456eb-d3c8-4402-86b1-deb911224afb

- http://ce.entel.cl/posts/reuniones-kick-off-una-buena-forma-de-alinear-estrategias-en-tu-empresa