Política de Clasificación de la Información

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en DACTA

Este documento se aplica a todo el alcance del Sistema Integrado de Gestión (SIG).

Los usuarios de este documento son todos los colaboradores de DACTA.

2. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, clausula 5.12.

3. POLÍTICA ESPECÍFICA

3.1. Criterios de Clasificación de la Información

La información se clasificará atendiendo al impacto que podría sufrir la empresa en caso de producirse cualquier incidencia que ponga en peligro la información.
Una vez clasificada la información, sólo el propietario de la misma, o la Gerencia/ Dirección asociada al área de **DACTA S.A.C** puede modificar esta clasificación atendiendo a criterios de:

- Cambios en los procesos implicados, en los planes de la organización, requisitos, etc.
- Desaparición de las causas que originaron la clasificación. Hay información que originariamente puede tener una clasificación de Confidencial que finalmente pase a ser de Uso interno.
- Finaliza el periodo de validez si lo tuviera.

La información de la organización se clasificará en los siguientes grupos:

TIPO	IMPACTO - DEFINICIÓN	DESCRIPCIÓN
PÚBLICA	**Impacto Bajo**. Información sin ninguna necesidad de restringir el acceso. Si se filtrara a terceras partes, no tendría consecuencias relevantes para la organización.	Toda aquella información que, individual o conjuntamente con información de terceros, está destinada a su divulgación pública como consecuencia de la estrategia de comunicación de la empresa, sin perjuicio de que antes de la divulgación le corresponda otro nivel de clasificación. En esta categoría también se incluye la información que está accesible públicamente. Ejemplo: Información en la Página Web, folletos/trípticos publicitarios…
RESTRINGIDA	**Impacto Medio**. Información a la que sólo debe tener acceso el personal de la organización o subcontratistas con necesidad de conocer. Si se filtrara a terceras partes no autorizadas, podría tener consecuencias relevantes para la organización.	Información a la que pueda disponer de acceso el personal de la organización para un adecuado desempeño de sus funciones. Los usuarios podrán acceder a la misma en base a sus necesidades, permisos, y al área en el que desarrollen sus tareas. Si esta información se filtrara a terceras partes, podría tener consecuencias serias para la organización. Se incluye aquella información de uso interno accesible por la totalidad del personal como las políticas o normas de uso. También aquella información, propia o de terceros, destinada a ser

		utilizada en un ámbito concreto o área de la empresa. Ejemplo: Desarrollos, códigos fuente, Información de RRHH, información restringida de proyectos y contratos. En general es información accesible únicamente por personal de la organización específico y expresamente autorizado
CONFIDENCIAL	**Impacto Crítico**. Información a la que sólo las Gerencias dentro de la organización o personal designado por estas gerencias, deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias serias para la organización. En este nivel se incluye, además, la información que contenga datos de carácter personal.	Toda aquella información cuya revelación no autorizada pudiera causar un daño considerable en la reputación de la empresa o bien en la confianza de sus clientes. Las informaciones amparadas por un Acuerdo de Confidencialidad o aquellas que contengan datos personales como contratos deberán ser clasificadas conforme a esta categoría.

La información pública se divide en:

- Web: de acceso público y alojada en proveedor de internet.
- Archivos ofimáticos: por ejemplo, archivos de publicidad de fabricantes que se almacenan en directorios del servidor.
- Documentos en papel: por ejemplo, documentos de publicidad de productos que se guardan en armarios sin llave.

La información restringida/ uso interno se divide en:

- Datos de gestión: Se almacenan en la base de datos de cada área, protegidos mediante la definición de usuarios y contraseñas.
- Archivos ofimáticos: Se almacenan en directorios del servidor y se protege mediante los permisos asignados a cada grupo de usuarios dentro del directorio activo.
- Correo electrónico: sobre el que se aplican las políticas de seguridad del directorio activo.
- Documentos en papel de administración y gestión: Se guardan en armarios dotados de llaves a las que sólo tiene acceso las personas que deben tratar dicha información.
- Normas, políticas, procedimientos e instrucciones de uso interno, necesarias para el desarrollo de las tareas de la organización o para cumplir con los requisitos del Sistema de Gestión.

La información confidencial se divide en:

- Datos de gestión o de proyectos que contenga datos de carácter personal, en archivos ofimáticos o en papel.
- Toda aquella información que haya sido así categorizado por los clientes de **DACTA S.A.C**, y que requieran un compromiso de confidencialidad sobre la misma.
- Información derivada de proyectos de elevada importancia cuyo conocimiento por personal ajeno sea especialmente crítico.
- Información y datos de configuración, y de la arquitectura de seguridad de los sistemas informáticos
- Información y documentación derivada de la gestión de Recursos Humanos

3.2. Medidas de Seguridad aplicadas a los tipos de información

A cada tipo de información se le aplicarán una serie de medidas de seguridad acordes a su nivel de impacto en caso de incidencia, que pueden variar a lo largo del ciclo de vida de la información.

A menos que se especifique otra cosa, todas las medidas son obligatorias.

3.3. Medidas para el Tratamiento de información Automatizada

	PÚBLICA	USO INTERNO	CONFIDENCIAL
Etiquetado	✓ No aplica	✓ No aplica	✓ Identificador de confidencial
Control de accesos	✓ Lectura: sin restricciones ✓ Escritura: usuarios autorizados	✓ Lectura: usuarios internos y terceras partes autorizadas ✓ Escritura: usuarios autorizados ✓ ID's de usuario únicos ✓ Contraseña de usuario	✓ Lectura: usuarios internos y terceras partes autorizadas ✓ Escritura: usuarios autorizados ✓ Acceso sólo a usuarios y grupos concretos ✓ ID's de usuario únicos ✓ Doble factor de autenticación ✓ Recomendado: Auditoría de accesos
Almacenamiento	✓ Antivirus/ antispyware	✓ Antivirus/antispyware ✓ Almacenamiento en red	✓ Antivirus/antispyware ✓ Almacenamiento en red ✓ Recomendado: Cifrado si está en un equipo portátil u otros soportes.
Transmisión por redes internas	✓ Servicio de correo	✓ Servicio de correo protegido por contraseña. ✓ Aviso de confidencialidad en la firma del e-mail	✓ Servicio de correo protegido por contraseña ✓ Identificador de confidencialidad ✓ Recomendado: Comunicación cifrada, Firma digital
Transmisión por Internet	✓ Servicio de correo protegido por contraseña	✓ Servicio de correo protegido por contraseña ✓ Aviso de confidencialidad en la firma del e-mail ✓ Datos protegidos por contraseña ✓ Eliminación de datos en campos ocultos, metadatos, comentarios, etc. salvo si es pertinente para el receptor ✓ Recomendado: Comunicación cifrada	✓ Servicio de correo protegido por contraseña ✓ Datos adjuntos compactados y protegidos por contraseña ✓ Comunicación cifrada ✓ Recomendado: Firma digital

	PÚBLICA	USO INTERNO	CONFIDENCIAL
Transmisión por soportes	✓ Sin restricciones	✓ Previa autorización ✓ Protegida por contraseña ✓ Registrar entradas y salidas	✓ Previa autorización ✓ Encriptada ✓ Registrar entradas y salidas
Respaldo y recuperación	✓ Respaldo diario de la información ✓ Retención mínima de 30 días	✓ Respaldo diario de la información ✓ Retención mínima de 30 días	✓ Respaldo diario de la información ✓ Retención mínima de 30 días
Destrucción	✓ Borrado convencional	✓ Borrado convencional	✓ Borrado seguro del fichero

3.4. Medidas para el Tratamiento de información en Soporte papel

	PÚBLICA	USO INTERNO	CONFIDENCIAL
Control de accesos	✓ No son necesarios controles de acceso	✓ Acceso a personal interno y subcontratado	✓ Sólo a personal autorizado ✓ Instalaciones con controles de acceso físico
Almacenamiento	✓ No son necesarias medidas especiales	✓ En armarios o estanterías habilitadas para ello	✓ En armarios o estanterías bajo llave ✓ Armario ignífugo
Transporte físico	✓ No son necesarias medidas especiales	✓ Correo ordinario o mensajería ✓ Registrar entradas y salidas	✓ Mensajería con acuse de recibo ✓ Registrar entradas y salidas
Respaldo y recuperación	✓ No son necesarias medidas especiales	✓ No son necesarias medidas especiales	✓ Realizar copia en formato digital
Destrucción	✓ No son necesarias medidas especiales	✓ Destrucción de papel manualmente y desechar. Asegurándose que esta información no quede disponible.	✓ Destrucción de papel manualmente y desechar. Asegurándose que esta información no quede disponible.

4. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
N/A	N/A	N/A	N/A

5. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
2	22/02/2023	Actualización	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
2	22/02/2024	Revisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
Firmas de la versión vigente			 S. Rafaile	 S. Rafaile  A. Morales	 G. Rafaile

Identificación de las modificaciones	
Versión	**Descripción de cambios**
2	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022.