

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 1 de 11

01.- ASUNTO: MÓDULO: SEGURIDAD DE LA INFORMACIÓN

02.- FECHA: 22 de septiembre del 2026

03.- INTRODUCCIÓN

La información es uno de los recursos más importantes para GRUNSEG. Durante sus actividades diarias, el personal de Operaciones maneja información relacionada con clientes, puestos de servicio, personal de seguridad, novedades, horarios, contactos, reportes y sistemas tecnológicos.

Por esta razón, **todos los colaboradores son responsables de proteger la información que utilizan.**

La seguridad de la información consiste en aplicar medidas para evitar que la información sea:

- Consultada por personas no autorizadas.
- Modificada o eliminada sin autorización.
- Perdida o divulgada.
- Utilizada para fines diferentes a los establecidos por la empresa.

La seguridad de la información no es responsabilidad únicamente del Departamento de Tecnología. **Cada persona que utiliza información, equipos o sistemas tiene un papel importante en su protección.**



Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 2 de 11

04.- DESARROLLO

4.1. Los tres principios de la Seguridad de la Información

La seguridad de la información se basa principalmente en tres principios:

CONFIDENCIALIDAD

La información debe ser conocida únicamente por las personas que tienen autorización para acceder a ella.

Ejemplos:

- No compartir claves de acceso.
- No enviar información de clientes a personas no autorizadas.
- No publicar fotografías de instalaciones, clientes o procedimientos en redes sociales.
- No dejar documentos con información sensible al alcance de terceros.

Recuerda:

La información que manejas en tu trabajo no debe compartirse fuera de los canales autorizados.



INTEGRIDAD

La información debe mantenerse correcta y completa, evitando modificaciones no autorizadas.

Ejemplos:

- No alterar un reporte o registro sin autorización.
- Registrar correctamente las novedades ocurridas durante un turno.
- No modificar información de un cliente sin autorización.
- Verificar los datos antes de enviar un informe.

Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 3 de 11

Recuerda:

Una información incorrecta puede generar decisiones equivocadas y afectar la operación.



DISPONIBILIDAD

La información y los sistemas deben estar disponibles para las personas autorizadas cuando sean necesarios.

Ejemplos:

- Mantener los equipos en buenas condiciones.
- Reportar oportunamente fallas de computadores, celulares o sistemas.
- No apagar o desconectar equipos críticos sin autorización.
- Informar inmediatamente cuando una plataforma necesaria para la operación presente problemas.

Recuerda:

Si un sistema es necesario para realizar tu trabajo, una falla debe ser reportada oportunamente.



Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 4 de 11

4.2. ¿Qué es una vulnerabilidad?

Una **vulnerabilidad** es una debilidad que puede ser aprovechada para afectar la seguridad de la información.

Algunos ejemplos:

- Utilizar contraseñas fáciles de adivinar.
- Dejar una sesión abierta.
- Dejar documentos con información confidencial sobre un escritorio.
- Utilizar dispositivos USB desconocidos.
- Descargar archivos de sitios no confiables.
- Compartir información mediante canales no autorizados.
- No actualizar los equipos cuando corresponda.

Ejemplo práctico:

Un Agente de seguridad deja el celular corporativo con sesión abierta y se retira de su puesto. Otra persona utiliza el celular.



La sesión abierta es una **vulnerabilidad**.

4.3. ¿Qué es una amenaza?

Una **amenaza** es cualquier situación, persona o acción que puede aprovechar una vulnerabilidad y causar un daño.

Las amenazas pueden ser:

Accidentales

Ocurren sin intención.

Ejemplos:

- Eliminar accidentalmente un archivo.
- Enviar información al destinatario equivocado.
- Derramar líquido sobre un computador.
- Perder un teléfono celular.
- Compartir por error una fotografía.

Intencionales

Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 5 de 11

Son realizadas deliberadamente.

Ejemplos:

- Intentar obtener una contraseña.
- Robar información.
- Acceder a una cuenta sin autorización.
- Instalar software malicioso.
- Copiar información de clientes para utilizarla indebidamente.

Naturales o ambientales

Pueden afectar los equipos y sistemas.

Ejemplos:

- Incendios.
- Inundaciones.
- Descargas eléctricas.
- Terremotos.
- Fallas de energía.
- Temperaturas o humedad excesivas.



Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 6 de 11

4.4. Principales riesgos para el personal de Operaciones

Contraseñas

Las contraseñas permiten proteger el acceso a sistemas y equipos.

Buenas prácticas:

- Mantén tus claves en secreto.
- No las compartas por WhatsApp, correo o llamadas.
- No las escribas en papeles visibles.
- No utilices contraseñas fáciles de adivinar.
- No utilices la misma contraseña para diferentes servicios cuando la política de la empresa indique lo contrario.
- Bloquea tu equipo cuando te retires.

IMPORTANTE:

El personal de GRUNSEG **no debe solicitar ni utilizar las claves de otros colaboradores.**



4.5. Phishing y mensajes sospechosos

El **phishing** es una técnica utilizada para engañar a una persona y conseguir información como contraseñas, datos personales o información empresarial.

Puede llegar mediante:

- Correo electrónico.
- WhatsApp.
- Mensajes de texto.
- Redes sociales.
- Llamadas telefónicas.

Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 7 de 11

- Enlaces enviados por terceros.

Señales de alerta

Desconfía cuando un mensaje:

- Solicita tu contraseña.
- Pide información confidencial.
- Contiene enlaces sospechosos.
- Tiene errores o mensajes poco habituales.
- Genera presión o urgencia.
- Solicita instalar un programa.
- Solicita realizar una transferencia o pago sin un procedimiento establecido.

Ante la duda: NO HAGAS CLIC.

Reporta el mensaje al responsable correspondiente.



4.6. Uso seguro de celulares

Los teléfonos celulares utilizados para actividades laborales pueden contener información importante.

Por eso:

- Mantén el equipo protegido mediante PIN, contraseña o método de bloqueo.
- No prestes el equipo sin autorización.
- No instales aplicaciones desconocidas.
- Evita conectar el teléfono a computadores desconocidos.
- No almacenes información empresarial innecesariamente.

Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 8 de 11

- Reporta inmediatamente la pérdida o robo del equipo.
- No compartas fotografías o información de clientes sin autorización.

Recuerda:

Un teléfono celular también es un dispositivo que debe ser protegido.



4.7. Protección de documentos

Los documentos físicos también contienen información que debe ser protegida.

Al finalizar una jornada o cuando abandones tu puesto:

- Guarda los documentos correctamente.
- No dejes reportes sobre escritorios de acceso público.
- No botes documentos con información confidencial directamente en la basura.
- Evita fotografiar documentos sin autorización.
- Verifica los destinatarios antes de entregar documentación.



Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 9 de 11

4.8. Seguridad de los equipos

Los computadores, tablets, celulares y demás equipos utilizados para el trabajo deben ser tratados como herramientas de trabajo y protegidos adecuadamente.

Recuerda:

-  Bloquea tu equipo cuando te retires.
-  No instales programas sin autorización.
-  No desconectes equipos críticos sin autorización.
-  No abras archivos sospechosos.
-  No conectes dispositivos USB desconocidos.
-  Reporta inmediatamente cualquier comportamiento extraño del equipo.

4.10. ¿Qué hacer ante un incidente de seguridad?

Un incidente puede ser cualquier situación que pueda comprometer la información, los equipos o los sistemas.

Por ejemplo:

- Pérdida o robo de un celular.
- Sospecha de robo de una contraseña.
- Correo o mensaje sospechoso.
- Virus o comportamiento extraño del computador.
- Acceso no autorizado.
- Pérdida de información.
- Envío accidental de información a una persona equivocada.
- Daño o pérdida de un equipo.

¿Qué debes hacer?

1. DETÉN LA ACCIÓN

No continúes interactuando con el mensaje, archivo o sistema sospechoso.

2. NO ELIMINES EVIDENCIAS

No borres mensajes, correos, fotografías o archivos relacionados con el incidente.

3. REPORTA

Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 10 de 11

Comunica inmediatamente la situación al responsable correspondiente.

4. SIGUE LAS INSTRUCCIONES

No intentes solucionar por tu cuenta un incidente que pueda comprometer un sistema o información empresarial.



4.11. Regla de oro

Antes de compartir, modificar, descargar o eliminar información, pregúntate:

¿ESTOY AUTORIZADO PARA HACERLO?

¿LA INFORMACIÓN ESTÁ SIENDO ENVIADA POR UN MEDIO SEGURO?

¿LA PERSONA QUE LA RECIBE ESTÁ AUTORIZADA?

¿QUÉ PASARÍA SI ESTA INFORMACIÓN LLEGARA A OTRA PERSONA?

Si tienes dudas, **consulta antes de realizar la acción.**

4.12. Responsabilidad de todos

La seguridad de la información es responsabilidad de todos los colaboradores.

Una contraseña compartida, un documento olvidado, un enlace malicioso o una fotografía publicada sin autorización pueden generar riesgos para la empresa y sus clientes.

PROTEGER LA INFORMACIÓN TAMBIÉN ES PARTE DE PROTEGER A NUESTROS CLIENTES, A NUESTROS COMPAÑEROS Y A GRUNSEG.

Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--

	INFORME GENERAL			
	GVR-10	Rev:01 Fecha de Rev: 9/11/2023	Fecha Elab: 21/08/2017	Página 11 de 11



05.- CONCLUSIÓN

La seguridad de la información no depende únicamente de sistemas tecnológicos o herramientas de seguridad. **También depende de las decisiones que cada colaborador toma diariamente.**

Aplicar buenas prácticas, proteger las contraseñas, verificar la información antes de compartirla, utilizar correctamente los equipos y reportar oportunamente cualquier situación sospechosa permite reducir los riesgos.

Recuerda los tres principios:



CONFIDENCIALIDAD: Solo acceden quienes están autorizados.



INTEGRIDAD: La información se mantiene correcta y sin modificaciones no autorizadas.



DISPONIBILIDAD: La información está disponible cuando la necesitan las personas autorizadas.

SEGURIDAD DE LA INFORMACIÓN = RESPONSABILIDAD DE TODOS

Departamento de Tecnología y Monitoreo Electrónico.

Elaborado por:

Abraham Cruz

Jefe de Tecnología y Monitoreo

GRUNSEG

Elaborado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Revisado: Lcda. Rafaela Grunauer. Gerencia de Calidad	Aprobado: Ing. Ernesto Grunauer Gerencia General
--	---	--