GERS	PROCEDIMIENTO PARA CONTROL DE INFORMACIÓN Y SOFTWARE	PR - 107	
		Revisión No: 9	Fecha de aprobación 25 abril 2023

Elaborado por: Douglas López

Douglas López
Auxiliar de Sistemas

Revisado por: _____

Alba Inés Naranjo
Jefe Gestión Humana

Aprobado por: _____

Luis Freyder Posso
Gerente

CONTROL REVISIONES

REVISIÓN	OBSERVACIONES	FECHA DE APROBACIÓN
01	Original	Nov 12 2012
02	Se explicó el formato para guardar información y la forma como se hará el Backup en la oficina de Bogotá	Abril 25 2013
03	Actualizaciones en seguridad y Backup	Enero 19 2016
04	Actualización ítems 5 y 6.1 (Backup y servidor Samba)	Agosto 20 2016
05	Migración Backup de usuarios a Google Drive. Solución Backup automático Bogotá. Replica de Backup de servidores en Google Drive	Enero 12 2017
06	Actualización de usuarios responsables de actualizar los proyectos finalizados	Enero 2018
07	Riesgos o fallas en el servicio	Noviembre 2018
08	Revisión general e inclusión del Backup de servidores nube	Abril 2022
09	Proceso de encriptación y políticas de uso	Abril 2023

1. OBJETIVO

Definir las políticas y métodos para el control de información digital en GERS, de manera quese pueda garantizar la seguridad, disponibilidad y conservación de esta.

2. ALCANCE

Este procedimiento aplica a todas las sedes de GERS en Colombia

3. POLÍTICAS GENERALES

GERS ha definido los siguientes lineamientos y directrices para el manejo de suinformación

No está permitido:

- Dañar o entorpecer el funcionamiento de los servicios de la red de datos.
- Destruir la integridad de la información o hacer mal uso de ella.
- Comprometer material propiedad de la institución.
- Colocar en el servidor cualquier material que esté considerado inapropiado, ofensivo o irrespetuoso.
- Instalar software no licenciado o que sirva para propósitos no aceptables dentro de la empresa.

4. CONTROL DE LA INFORMACIÓN

- Cada usuario de la red de GERS tiene asignado un espacio ilimitado en GoogleDrive para almacenamiento de la información laboral. En cada equipo se configura la ruta **Z:\Google Drive\Mi Unidad**, el usuario debe trabajar directamente sobre esta carpeta con el fin de garantizar que la información se encuentre actualizada, sea trazable y de fácil acceso y recuperación.
- Por seguridad cada usuario tiene acceso al espacio asignado, mediante la cuenta de correo única que tiene en la plataforma Google G Suite For Business.

- El Bacukp se sincroniza automáticamente con los servidores de Google para actualizar la información, siempre y cuando se cuente con conexión a Internet.

- De forma aleatoria se realizan auditorias (3 usuarios por área) para revisar la correcta ejecución de la aplicación, el buen uso del Software autorizado y la integridad de la información.

5. CONTROL Y SEGUIMIENTO DE BACKUP

BACKUP Automáticos	Frecuencia	Seguimiento	Donde
Proyectos (S)	Semanal	Aleatorio C/15 días	Google Drive\Unidades Compartidas

6. ORGANIZACIÓN DE LA INFORMACIÓN DE PROYECTO

En cada área se asigna una persona para que tenga la responsabilidad de crear el directorio de proyectos de su área.

La información del proyecto puede contener entre otros los siguientes archivos.

- Cotización
- Orden de compra
- Pólizas
- Facturas
- Registro de calidad
- Registro de seguridad
- Información de entrada
- Informes
- Memoria de cálculo o protocolos
- Planos
- Correspondencia
- Encuesta de satisfacción
- Actas de inicio y cierre

En este directorio se almacenan todos los proyectos finalizados, de acuerdo con el siguiente modelo de organización:
Ruta: "**Z:\Unidades Compartidas\PROYECTOS FINALIZADOS\A - Z**

<Código de Cliente - Nombre Cliente> / <Proyecto - Año>

Código de Cliente - Nombre Cliente

El nombre del cliente debe coincidir con el nombre registrado en el CRM, se debe anteponer su consecutivo, ej.: E4 - ECOPETROL SA, C131 - CEMENTOS SAN MARCOS SA

Proyecto

<Proyecto>: El código de proyecto sin espacios, al finalizar debe llevar el año de inicio del proyecto, ej.: E10-17 - 2012, C19-30 - 2015, T6-21 – 2016

Ejemplos

Z:\Unidades compartidas\05. P. FINALIZADOS I-J\J1 - JOHNSON Y JOHNSON DECOLOMBIA S A\J1-16 -2018

Z:\Unidades compartidas\05. P. FINALIZADOS I-J\J1 - JOHNSON Y JOHNSON DECOLOMBIA S A\J1-13 - 2016

Historial

Los proyectos anteriores a 2013 se almacenan sin restricción en un directorio llamadoHistorial que será de solo lectura.

Unidades Compartidas

Los usuarios de GERS cuentan con un espacio dentro de Google Drive que se llama Unidades Compartidas. La cual permite trabajar información de manera colaborativa entre otros miembros de la organización. El control de acceso a las unidades compartidas solo es permitido por el personal de TI desde la cuenta de administrador para asignar los diferentes perfiles a los diferentes usuarios. No se permite el acceso a los usuarios que no pertenezcan a la organización.

Los tipos de perfiles de las unidades son:

- **Administrador General**: Administra el contenido, los usuarios y configuración.
- **Administrador del Contenido**: Agregar, editar, borrar y compartir contenido.
- **Colaborador:** Agregar y editar archivos
- **Comentarista**.
- **Lector**.

USUARIOS RESPONSABLES DEL BACKUP DE PROYECTOS POR ÁREA

ÁREAS	RESPONSABLE
Estudios	Jesús Ortega, Harold Quintero
Diseños e Interventorías	Ana Piedrahita, Yenny Tafurt
Pruebas, Automatización y Control - PAC	Angelly Mondragón, Rodolfo Valencia

7. RIESGOS

7.1 SERVICIOS NO DISPONIBLES

A la hora de usar Google Drive. Puede que el servicio no esté disponible en algún momento y eso nos impida acceder a contenido importante, ya sea desde la versión web o la aplicación de escritorio

Google será el encargado de restablecer los servicios para el correcto funcionamiento, esto no implica perdida de los datos que se almacenen en Google Drive. El administrador de TI deberá informar a Google para validar los motivos de la caída en el servicio y solicitar un tiempo de respuestas para el restablecimiento del mismo.

7.2 PÉRDIDA DE INFORMACIÓN DE PARTE DEL USUARIO

En caso de que el usuario elimine información de la carpeta en Google Drive, el usuario puede recuperar los elementos desde la papelera de Google Drive el

cual tiene un tiempo máximo de 30 días.

Google G Suite For Business cuenta con una opción de restauración de toda la unidad de Google Drive del usuario no mayor a 25 días estableciendo el periodo de tiempo que se necesite. El tiempo de restauración puede variar según la cantidad de GB que tenga el usuario.

8. SERVIDORES EN LA NUBE

GERS cuenta actualmente cuenta con dos servicios alojados en servidores nubes esto con elfin de garantizar una disponibilidad en el servicio al 100%. Al mismo tiempo lograr conseguir copias completas de toda la máquina y restablecer el servicio logrando conservar los datos para tener el menor impacto posible en cuanto a perdida de información o caída en los servicios.

9. PROCEDIMIENTO DE ENCRIPTACIÓN

9.1. INTRODUCCIÓN

Este documento contiene las normas de seguridad criptográfica aplicables a los sistemas de información.

La seguridad criptográfica especifica normas de uso en relación con la criptografía, e incluye estándares para su implantación en la organización. Algunos de los usos de la criptografía incluyen los mecanismos de autenticación, firma electrónica e irrefutabilidad, confidencialidad o integridad.

10. APLICACIÓN DE SEGURIDAD CRIPTOGRÁFICA

La criptografía es aplicable a toda la información de apoyo a procedimientos y actividades las cuales se vayan a desarrollar por parte de GERS y el cliente, y también a las relaciones por medios electrónicos con terceros que no forman parte de GERS S.A.S.

11. ENCRIPTACIÓN Y CIFRADO: GMAIL, DRIVE Y MEET

GERS usa como cliente de correo y almacenamiento en nube los servicios de Google. Gmail es capaz de cifrar el correo que se envía y se recibe, pero solo cuando el otro proveedor admite el cifrado TLS. El cual es un protocolo de Internet estándar que cifra los correos para proteger su privacidad y entregarlos de manera segura. Con él se evita el acceso no autorizado al correo cuando pasa

por las conexiones a Internet. En Google Workspace, el cifrado del contenido se gestiona en el navegador del cliente antes de transmitir datos o almacenarlos en la nube de Drive. De este modo, los servidores de Google no pueden acceder a tus claves de cifrado ni descifrar tus datos

En el caso de las llamadas 1:1 y de grupo con Google Meet, la encriptación de extremo a extremo implica que los datos de una llamada (su audio y video) se encriptan desde tu dispositivo hasta el de tu contacto. El audio y video encriptados solo se pueden decodificar con una clave secreta compartida.

Encriptación de extremo a extremo:

- Es un método de seguridad estándar que protege los datos de las comunicaciones.
- Está integrada en todas las llamadas 1:1 y de grupo. Está activada de forma predeterminada y no se puede desactivar.
- Solo permite que los participantes de una llamada sepan lo que se dice o se muestra.
- Google no puede ver, oír ni guardar el audio ni el video de la llamada.

Clave:

- Es un número que se crea en tu dispositivo y el dispositivo al que llamas. Existe solo en esos dispositivos.
- Desaparece cuando finaliza la llamada.
- No se comparte con:
    - Google
    - Otros usuarios
    - Otros dispositivos

Para garantizar la seguridad y la privacidad de los datos, la app de Google Meet admite las siguientes medidas de encriptación en la nube para las reuniones:

- De forma predeterminada, los datos de las reuniones se encriptan en tránsito entre el cliente y los centros de datos de Google para las

reuniones que se realicen en la app de Google Meet.

- De forma predeterminada, las grabaciones de reuniones que se almacenan en Google Drive se encriptan en reposo.

- La encriptación de las reuniones cumple con lo siguiente:

    - Estándares de seguridad de Internet Engineering Task Force relativas a la seguridad de la capa de transporte para datagramas (DTLS).

    - Protocolo seguro de transporte en tiempo real (SRTP).

Todos los datos que Google almacena se encriptan en la capa de almacenamiento mediante el algoritmo del estándar de encriptación avanzada (AES), AES-256.

12. ¿QUÉ INFORMACIÓN SE DEBE CIFRAR?

Los archivos que el personal de GERS debe de cifrar con todos aquellos que hagan parte de información de proyectos los cuales deben estar presentes en el servicio de Google Drive, por lo que el usuario puede el cual cuenta con métodos de cifrado y encriptación de parte de los servidores de Google los cuales se describen en el punto **#11**.

Solo aquellos que tengan el enlace generado por Drive y cuenten con los permisos de acceso pueden ver los datos.

13. SEGURIDAD INFORMATICA

Todos los empleados, presenciales y tele trabajadores, deben tener un conocimiento importante sobre temas de seguridad de la información y protección de datos, que los lleve a aplicar un pensamiento crítico en la realización de sus tareas diarias.

Hay algunos puntos críticos que no pueden quedar fuera de cualquier programa de capacitación o entrenamiento:

- **Acceso seguro, permisos y contraseñas:**
  La necesidad y la obligatoriedad de crear contraseñas seguras, cambiarlas

de forma periódica, y conceder niveles de acceso de acuerdo con los requerimientos del trabajo

- **Conexiones a Internet públicas:**
  El uso de una red inalámbrica de Internet pública, implica la posibilidad de acceso no permitido con fines delictivos. Los infractores tienen acceso a los datos que circulan por este tipo de redes, lo que incluye correos electrónicos con información sensible.

- **Redes Sociales:**
  Uno de los riesgos que supone el trabajo desde casa es que el empleado alterne sus labores profesionales con su interacción personal en Redes Sociales. Esto implica bajar la defensa y eventualmente compartir información confidencial que permita a los ciber-delincuentes aparecer como una fuente confiable y acceder a bases de datos, cuentas de e-mail e información confidencial.

- **Teletrabajo:**
  Los riesgos para la seguridad de la información y protección de datos aumentarán, pero una forma efectiva de minimizarlos o eliminarlos es formando y concientizando a los empleados.

- **Ataques de phishing:**
  El “spearphishing” es el resultado de la evolución de esta práctica criminal. Mediante ella, los ciber-delincuentes pretenden legitimar un correo electrónico, para un grupo definido de destinatarios. En este correo, aparentemente dirigido desde un supuesto alto cargo u organismo validado, se esconde un archivo de malware.

- **Seguridad móvil:**
  La conexión desde dispositivos móviles aumenta de forma exponencial. Los dispositivos móviles, aún los personales de los empleados, forman parte de la estructura tecnológica de la organización, y se convierten en uno de los puntos más vulnerables para la seguridad de la información.

- **Ransomware Secuestro de Datos:**
  Ransomware es un software malicioso que cifra los datos en un ordenador, impidiendo el acceso del legítimo propietario de la información, hasta que se pague una cantidad exigida de dinero.